Capítulo 4

Ameaças e Vulnerabilidades em Open RAN: Desafios e Soluções

Diogo Menezes Ferrazani Mattos (UFF), Dianne Scherly Varela de Medeiros (UFF), Rodrigo de Souza Couto (UFRJ), Pedro Henrique Cruz Caminha (UFRJ), Lucas Airam Castro de Souza (UFRJ), Felipe Gomes Táparo (UFRJ), Guilherme Araujo Thomaz (UFRJ), João Vitor Valle (UFF), Franciele Batista de Oliveira (UFF), Miguel Elias Mitre Campista (UFRJ), Luís Henrique Maciel Kosmalski Costa (UFRJ), Igor Monteiro Moraes (UFF)

Resumo

A experiência com as redes de acesso via rádio atuais demonstra que o uso de arquiteturas monolíticas e de código fechado não favorece a customização de serviços nem a interoperabilidade dos componentes da rede. Tais obstáculos trazem concentração de mercado, dificuldade de inovação e maior custo de operação. Nesse sentido, a Rede de Acesso via Rádio Aberta (Open Radio Access Network – Open RAN) traz um modelo totalmente disruptivo que abre as interfaces de software e hardware para a desagregação de componentes, permitindo a entrada de novos participantes e serviços. As interfaces abertas permitem a "softwarização" da rede e a introdução de gerenciamento e controle baseado em inteligência artificial. A abertura, porém, tem um custo em segurança, tendo em vista a expansão da superfície de ataque da RAN. Este capítulo discute as ameaças e vulnerabilidades relativos à Open RAN e os desafios e oportunidades de pesquisa para o desenvolvimento de soluções de segurança em redes móveis de próxima geração.

4.1. Introdução

Estimativas do mercado global relacionado às redes 5G apontam uma taxa de crescimento anual de 21,1% e um volume de capital de aproximadamente 57 bilhões de dólares até 2030 [Research e Markets, 2022]. Esses números demonstram a importância das redes de acesso móvel, tanto pelos serviços de interconexão prestados quanto pelo ponto de vista econômico que mantém grandes empresas no setor de telecomunicações. Dessa forma, a concentração do mercado fornecedor de tecnologia de acesso sem fio móvel em poucos participantes, com o uso de soluções fechadas e monolíticas, não é conveniente em um ambiente altamente disputado e estratégico. Esse entendimento leva à tendência

de abertura das soluções empregadas nas redes de acesso móvel ao longo das gerações. Tais ações culminam na abertura de interfaces, que tem por objetivo promover a interoperabilidade de *hardware* e de *software* de múltiplos fabricantes, além de possibilitar a criação e inserção de novas funções à rede.

As Redes de Acesso via Rádio (*Radio Access Networks* – RANs) são compostas por um conjunto de componentes que interagem entre si para possibilitar a comunicação entre o equipamento do usuário (*User Equipment* – UE) e a rede de núcleo do sistema de comunicação móvel celular [Couto et al., 2023b, de Oliveira et al., 2023, Lopez et al., 2022]. Essa interação é intermediada pela Estação Rádio-Base (*Radio Base Station* – RBS) [Couto et al., 2023b], principal afetada pela abertura de interfaces de *hardware* e *software*. As condições necessárias para abertura de interfaces podem ser percebidas ao longo das diferentes gerações das redes móveis. Nas primeiras gerações, a RBS era implementada como um componente monolítico que acumulava funções de múltiplas camadas. Na terceira geração, houve a separação das funções de comunicação via rádio em funções de transmissão e recepção, executadas por uma nova RBS, chamada de NodeB, e em funções de gerenciamento de recursos de rádio e processamento relacionado aos usuários, executadas pelo Controlador da Rede via Rádio (*Radio Network Controller* – RNC) [Arnaz et al., 2022]. A quarta geração agregou funcionalidades do RNC à nova RBS, chamada de *Evolved Node B* (eNB), extinguindo a entidade de controle separada. Tanto a terceira quanto a quarta geração desagregaram as funções da RBS em Unidade de Rádio Remota (*Remote Radio Head* – RRH), que executava as funções de rádio, e em Unidade de Banda Base (*BaseBand Unit* – BBU), que realizava o processamento de sinal em banda base. Tal desagregação permitiu que a BBU e a RRH fossem fisicamente separadas, sendo a RRH mantida mais próxima da RBS. Essa arquitetura introduz a RAN distribuída (*Distributed RAN* – D-RAN) [Brik et al., 2022] utilizada nas gerações atuais.

A quinta geração das redes celulares deu um passo a mais na direção da desagregação de funcionalidades, propondo a separação da RNB, eNB do 4G que evoluiu para gNB (*Next Generation Node* B), em três unidades: central (*Central Unit* -– CU), distribuída (*Distributed Unit* -– DU) e de rádio (*Radio Unit* – RU) [Polese et al., 2023]. As funcionalidades das camadas física, de enlace e de rede são então divididas entre essas três unidades, que ainda mantêm um projeto composto por componentes monolíticos com interfaces fechadas. Tal característica ainda favorece a concentração do mercado em poucos fabricantes, criando obstáculos tecnológicos tanto para customização da rede quanto para interoperabilidade das unidades. A arquitetura desagregada da rede e os entraves das soluções fechadas, portanto, motivaram o movimento atual em direção ao uso de interfaces abertas. Nesse sentido, a *O-RAN Alliance*[1] lidera a proposta de uma arquitetura e um conjunto de interfaces que concretizem a RAN aberta (*Open* RAN) [O-RAN Working Group 1, 2023]. A arquitetura O-RAN para a RAN aberta segue os seguintes princípios fundamentais: desagregação dos componentes da RAN, controle inteligente, virtualização e interfaces abertas [Polese et al., 2023]. A arquitetura O-RAN define um novo padrão industrial para redes móveis de quinta geração e além (*Beyond 5G* - B5G). As interfaces abertas e padronizadas permitem a interoperabilidade entre equipamentos de diferentes fornecedores, oferecendo flexibilidade de rede a um custo reduzido

[1]Disponível em `https://www.o-ran.org/`.

de capital e operação. A arquitetura O-RAN combina os benefícios da execução de funções de rede em *software* e inteligência artificial para tornar a operação de dispositivos e da rede de acesso mais eficiente e segura.

A arquitetura O-RAN introduz componentes, interfaces e tecnologias que possibilitam a participação de novos atores e viabilizam novos modelos de negócios. A abertura das interfaces e desagregação dos componente trazem benefícios para a segurança da rede. Enquanto as interfaces abertas O-RAN introduzem transparência à implementação dos componentes, tornando mais viável o alinhamento com os padrões de segurança e as melhores práticas, a desagregação dos componentes aumenta a agilidade e a adaptabilidade. Além disso, a O-RAN suporta o uso de microsserviços hospedados em nuvens, permitindo empregar mecanismos de segurança nativos da nuvem, como isolamento de recursos de *hardware*, reconfiguração automática e automação de testes de segurança, que reforçam o gerenciamento de vulnerabilidades de código aberto e a configuração de segurança. No entanto, novas tecnologias implicam aumento da superfície de ataque, trazendo desafios de segurança e riscos associados às novas interfaces e componentes específicos da O-RAN, às técnicas de virtualização e conteinerização, ao suporte a código-fonte aberto e ao suporte de modelos de aprendizado de máquina de terceiros. O *software* de código-fonte aberto aumenta a necessidade de práticas de desenvolvimento seguras nas comunidades de código aberto. A incorporação de Inteligência Artificial (IA) na RAN apresenta riscos como a falta de transparência e explicabilidade dos modelos de IA, que pode levar a ações imprevisíveis na RAN [de Oliveira et al., 2023]. O acesso não-autenticado e não-autorizado aos componentes da arquitetura pode ser alcançado através de diferentes interfaces. Tal acesso depende do projeto de *hardware* e *software* da O-RAN e de como as diferentes funções são desacopladas dentro da própria arquitetura. Assim, interfaces de gerenciamento devem seguir as melhores práticas de segurança do setor, incluindo criptografia forte, autenticação mútua, controle de acesso, registro robusto e validação de entrada.

Os componentes da O-RAN podem estar vulneráveis caso estejam desatualizados por falta de gerenciamento de remendos (*patches*), tenham um projeto de arquitetura deficiente em termos de segurança, não tenham proteção apropriada, usem uma função ou protocolo que não sejam seguros ou que não sejam mais necessários. Nesse caso, um atacante pode tanto injetar *malwares* e manipular *software* existente, quanto manipular parâmetros ou reconfigurar os componentes O-RAN para reduzir seu desempenho e desativar os recursos de segurança. Esse último com o objetivo de espionar ou interceptar planos de controle e de dados, atingir interfaces externas, atacar uma rede para disparar um ataque de negação de serviço mais amplo ou roubar chaves privadas desprotegidas, certificados e valores de *hash*. Ademais, os componentes O-RAN podem ser componentes de *software* que fornecem funções de rede, sendo possivelmente vulneráveis a falhas como, por exemplo, o estouro de *buffer* para execução de comandos arbitrários. A fim de aumentar a segurança da O-RAN, microsserviços integrados aos Controladores Inteligentes da RAN (RAN *Intelligent Controllers* – RICs) podem empregar dados e análises em tempo real, avaliando a integridade da RAN e reforçando os recursos de segurança e gerenciamento. Para tanto a plataforma de *software* O-RAN segue as referências de segurança do setor de telecomunicações e os requisitos de garantia de segurança do 3GPP. Contudo, é importante destacar que a implementação de controles de segurança requer

atenção devido às rigorosas demandas de latência [NIS Cooperation Group, 2022] das redes móveis de quinta geração e além.

Este capítulo aborda os desafios de segurança da Open RAN, incluindo seus conceitos básicos e soluções. O objetivo é apresentar as principais ameaças, vulnerabilidades e vetores de ataque, e discutir os desafios de pesquisa para prover segurança a essas redes. Inicialmente, apresenta-se a arquitetura de referência O-RAN e os requisitos de segurança especificados pela O-RAN Alliance. Em seguida, as principais ameaças e vulnerabilidades da O-RAN são explicadas. Este capítulo ainda introduz as principais técnicas e estratégias para defesa e mitigação de ataques às RANs. Discute-se também os principais ataques baseados em aprendizado de máquina para RANs. Por fim, os desafios e oportunidades de pesquisa para o desenvolvimento de mecanismos de segurança e preservação da privacidade em redes móveis de próxima geração são elencados.

4.2. A Arquitetura de Referência O-RAN e os Requisitos de Segurança

A arquitetura O-RAN é proposta pela *O-RAN Alliance* para a RAN aberta com o objetivo de oferecer maior flexibilidade na implantação das RANs e facilidade para gerenciamento e orquestração dos diversos serviços e componentes da rede. A arquitetura O-RAN permite às operadoras de telecomunicações independência de soluções monolíticas de um único fornecedor, devido ao suporte à desagregação, virtualização e "softwarização" de componentes que são conectados através de interfaces abertas padronizadas. Essa padronização permite a interoperabilidade entre equipamentos de fornecedores distintos e possibilita às operadoras utilizarem *hardware* não proprietário. Ademais, a arquitetura O-RAN permite aproveitar os princípios das soluções nativas em nuvem e integrar inteligência no controle da RAN [Polese et al., 2023]. Para tanto, a arquitetura segue a desagregação das três unidades funcionais da gNodeB proposta pelo 3GPP. Essas unidades se interconectam e estão conectadas a outros componentes da arquitetura O-RAN por meio de interfaces abertas.As três unidades definidas são nós lógicos, denominados Unidade Central O-RAN (O-RAN *Central Unit* – O-CU), Unidade Distribuída O-RAN (O-RAN *Distributed Unit* – O-DU) e Unidade de Rádio O-RAN (O-RAN *Radio Unit* – O-RU).

A inovação da arquitetura O-RAN em relação à RAN tradicional são os Controladores Inteligentes da RAN (*RAN Intelligent Controllers* – RICs). Os RICs introduzem componentes programáveis que podem executar rotinas de otimização com um laço de controle fechado e orquestrar serviços na RAN de forma eficiente, possuindo uma visão abstrata e centralizada da rede. Para isso, os RICs acessam informações de medidas de desempenho e contexto provenientes da RAN e de fontes externas à RAN, que podem ser utilizadas para produzir modelos de aprendizado de máquina com o objetivo de criar políticas e ações de controle sobre a RAN [O-RAN Working Group 1, 2023]. Dessa forma, é possível automatizar procedimentos de otimização da rede com foco no fatiamento dos recursos, balanceamento de carga e mudança de células (*handovers*) [Polese et al., 2023]. As especificações da O-RAN Alliance [O-RAN Working Group 3, 2023a, O-RAN Working Group 2, 2021] descrevem requisitos e funcionalidades de diferentes componentes dos RICs para que as implementações, em conformidade com o padrão, forneçam os mesmos conjuntos de serviços e sejam interoperáveis.

Apesar de trazer benefícios para as RANs, a nova arquitetura sofre com vulnerabilidades que precisam ser tratadas. Por um lado, a desagregação da arquitetura facilita a atualização e a introdução de funções de rede por utilizar redes definidas por *software* (*Software Defined Networking* – SDN) e virtualização de funções de rede (*Network Function Virtualization* – NFV). Por outro lado, a "softwarização" da RAN traz desafios de segurança relacionados a arquiteturas virtualizadas, englobando riscos de segurança em nuvem e contêineres. A desagregação também aumenta a superfície de ataque da RAN devido aos novos componentes criados [Soltani et al., 2023]. A separação da O-DU e da O-RU, por exemplo, expõe uma das interfaces abertas padronizadas, a Open Fronthaul [Dik e Berger, 2023]. O uso de *software* de código-fonte aberto aumenta a dependência de práticas de desenvolvimento seguro, ficando exposto a vulnerabilidades de "dia zero" (*zero-day*). Além disso, com a introdução dos RICs e a consequente dependência de fluxos de aprendizado de máquina e inteligência artificial (*Machine Learning/Artificial Intelligence* – ML/AI) levam a vulnerabilidades não mapeadas inicialmente. A possibilidade de diversas entidades poderem desenvolver aplicações que operam nos RICs, consumindo dados da RAN, é um fator crítico, visto que essas aplicações podem inserir vulnerabilidades. Existe, ainda, o aumento da superfície de ataque devido ao crescimento exacerbado de dispositivos conectados, exigindo que a RAN seja protegida contra dispositivos que foram violados. É importante destacar que nem todos os problemas citados são exclusivos da RAN aberta, mas se tornam mais significativos devido à adição de novos componentes não existentes nas RANs contemporâneas, de novas interfaces abertas e ao uso da opção de divisão 7.2x [O-RAN Working Group 11, 2023c]. Nesse contexto, a O-RAN Alliance especifica requisitos de segurança e pilhas de protocolos para configuração e criptografia que devem ser usados nas interfaces O-RAN para garantir confidencialidade, autenticidade, integridade, autorização e proteção contra ataques de repetição [O-RAN Working Group 11, 2023c]. O objetivo é adequar a RAN aberta ao padrão de qualidade e segurança que os sistemas de telecomunicações exigem, de forma que o risco à segurança seja mitigado na implantação da RAN aberta pelos Provedores de Serviços de Comunicação (*Communication Service Providers* – CSPs).

Esta seção apresenta primeiramente uma visão geral da arquitetura de referência O-RAN proposta pela O-RAN Alliance, destacando em seguida os requisitos de segurança especificados pela aliança.

4.2.1. Arquitetura O-RAN

A desagregação da gNodeB tem como base a Opção de Divisão 7.2x (*Split Option* 7.2x) definida no conjunto de especificações 3GPP *New Radio* (3GPP NR), que separa as funcionalidades de camada física para serem implementadas em duas unidades distintas. Os componentes desagregados estão representados na Figura 4.1. A O-RU passa a ser responsável apenas pelo processamento de sinais de radiofrequência e pelas funcionalidades de camada física inferior (*Low*-PHY), como transformada rápida de Fourier direta e inversa, remoção e adição de prefixo cíclico e conformação de feixe (*beamforming*). A O-DU é responsável pelas funcionalidades de camada física superior (*High*-PHY), como embaralhamento, modulação, mapeamento de camada e mapeamento de elementos de recursos. Dessa forma, a O-RU torna-se uma unidade de baixo custo e de fácil implantação, reduzindo a largura de banda necessária para comunicação no *fronthaul* e o atraso.

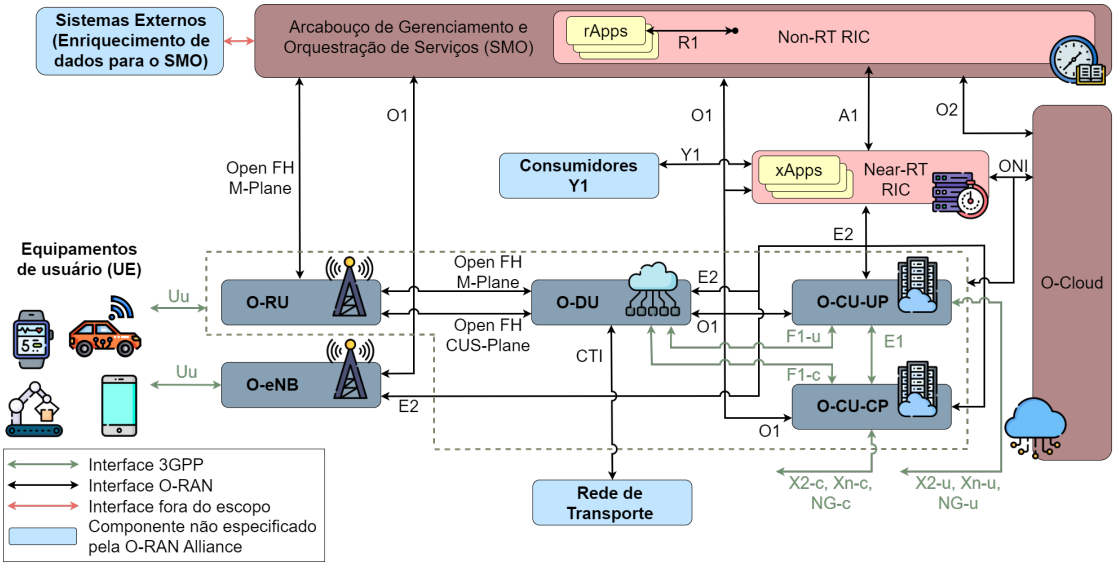

Figura 4.1. Componentes da arquitetura O-RAN. A arquitetura divide as funcionalidades da estação rádio base em três componentes, O-CU, O-DU e O-RU, além de definir o SMO, os RICs e a O-Cloud. Os componentes da arquitetura interagem por meio de interfaces especificadas pela O-RAN Alliance (em preto) e pelo 3GPP (em verde). Adaptado de [O-RAN Working Group 1, 2023], com ícones de Freepik (flaticon.com).

A O-DU também é responsável pelas funcionalidades de camada de enlace, implementando a subcamada de Controle de Acesso ao Meio (*Medium Access Control* – MAC) e a subcamada de Controle de Enlace de Rádio (*Radio Link Control* – RLC). As operações realizadas pela camada física superior e pelas subcamadas MAC e RLC devem ser fortemente sincronizadas, porque a subcamada MAC gera Blocos de Transporte (*Transport Blocks* – TBs) para serem enviados pela camada física usando dados que são enfileirados pela subcamada RLC. A O-CU é responsável por funcionalidades como controle de mobilidade, compartilhamento da RAN, gerenciamento de sessão e transferência de dados do usuário. Para isso, a O-CU implementa a camada de Controle de Recursos de Rádio (*Radio Resource Control* – RRC), que gerencia o ciclo de vida das conexões; a camada de Protocolo de Adaptação de Serviços de Dados (*Service Data Adaptation Protocol* – SDAP), que gerencia a qualidade de serviço dos fluxos de tráfego; e a camada de Protocolo de Convergência de Pacotes de Dados (*Packet Data Convergence Protocol* – PDCP), responsável pela reordenação de pacotes, tratamento de pacotes duplicados, criptografia dos dados para a interface aérea, dentre outras funções [Arnaz et al., 2022]. A O-CU é formada por um componente lógico para o plano de controle (O-CU *Control Plane* – O-CU-CP) e outro para o plano de usuário (O-CU *User Plane* – O-CU-UP) para permitir a implementação de funcionalidades distintas em diferentes locais da rede e plataformas de *hardware* [O-RAN Working Group 1, 2023].

A O-RAN Alliance especifica o RIC não tempo-real (*Non-Real-Time* RIC – Non-RT RIC) e o RIC quase tempo-real (*Near-Real-Time* RIC – Near-RT RIC) [O-RAN Working Group 1, 2023], apresentados na Figura 4.1. Enquanto o Non-RT RIC fornece operação inteligente e otimização da RAN em uma escala de tempo maior do que 1 segundo, o Near-RT RIC opera em escala de tempo entre 10 milissegundos e 1 segundo. Para operar nessa escala de tempo, o Near-RT RIC é implan-

tado na borda da rede, estando conectado às O-DUS, O-CUs e O-eNBs. Uma O-eNB é uma eNB ou *Next-Generation* eNB (gNodeB) que suporta as interfaces E2 e O1 [O-RAN Working Group 1, 2023].

O Non-RT RIC suporta a execução de rApps, aplicações de terceiros que fornecem serviços de valor agregado para facilitar ou aprimorar as operações da RAN [Polese et al., 2023, Arnaz et al., 2022]. Por sua vez, o Near-RT RIC suporta a execução de xApps, que são microsserviços usados para gerenciar recursos de rádio através de interfaces padronizadas e modelos de serviços [Polese et al., 2023, Arnaz et al., 2022], que também podem ser fornecidas por terceiros. Por meio das xApps e rApps, é possível realizar o controle inteligente da RAN. Enquanto as xApps implementam uma lógica personalizada que pode utilizar informações de telemetria da RAN e enviar ações de controle para serem executadas por elementos da RAN, as rApps permitem a implantação de serviços de valor agregado a fim de suportar e facilitar a otimização e operação da RAN, oferecendo serviços de orientação de políticas, enriquecimento de informação, gerenciamento de configuração e análise de dados [Polese et al., 2023].

Outro componente fundamental da arquitetura O-RAN, responsável pelo gerenciamento do domínio da RAN, é o componente de Orquestração e Gerenciamento de Serviços (*Service Management and Orchestration* – SMO). O SMO fornece uma interface com as funções de rede O-RAN, seguindo o modelo FCAPS (*Fault, Configuration, Accounting, Performance, Security*). O SMO é composto pelo Non-RT RIC e por um conjunto de funções e serviços para gerenciamento, orquestração e automação da RAN, tendo um papel semelhante à entidade de Gerenciamento e Orquestração (*Management and Orchestration* – MANO) definida na arquitetura NFV [Thiruvasagam et al., 2023].

O Near-RT RIC é formado por [O-RAN Working Group 3, 2023a]:

- terminações de interfaces (O1, A1, Y1, E2), que permitem a comunicação por meio das interfaces conectadas ao Near-RT RIC;
- APIs do Near-RT RIC para as xApps, um conjunto de APIs que fornecem serviços à plataforma Near-RT RIC, definindo explicitamente os possíveis tipos de fluxos de informação e modelos de dados. São definidas APIs relacionadas às interfaces A1 e E2, APIs de gerenciamento, APIs para a camada de compartilhamento de dados e as APIs de ativação;
- infraestrutura de mensagens internas, responsável por interconectar os componentes internos do Near-RT RIC;
- componente para mitigação de conflitos, que lida com possíveis conflitos entre requisições de configurações geradas por diferentes xApps;
- gerenciador de assinaturas de xApps, que permite que as xApps se conectem a funções expostas pela interface E2, controlando também o acesso individual das xApps às mensagens nessa interface;
- componente de funções de gerenciamento, fornece funções de gerenciamento de falha, configuração e desempenho, registro e rastreio, coleta de métricas para capturar, monitorar e obter o estado dos componentes internos do Near-RT RIC;

- componente de segurança, responsável por prevenir a exploração abusiva de informações por xApps e o controle de funções da RAN com intenção maliciosa;
- suporte ao fluxo de trabalho de AI/ML, que oferece treinamento de modelos nas xApps e preparação dos dados para consumo pelas xApps;
- função de repositório de xApps, permite a seleção de xApps para roteamento de mensagens da interface A1 com base nas políticas adotadas, e controle de acesso das xApps ao serviço de enriquecimento de informação com base nas políticas da operadora;
- Base de Informações de Rede (*Network Information Base* – NIB) e camada de compartilhamento de dados, que permitem às xApps e ao Near-RT RIC modificarem informações armazenadas no banco de dados e obterem informações sobre os componentes conectados à interface E2 e sobre os UEs; e
- API de ativação, que suporta a operação da API do Near-RT RIC, como registro, autenticação, descoberta de APIs, dentre outras operações.

O Non-RT RIC implementa um subconjunto de funcionalidades do arcabouço SMO com o objetivo de realizar a otimização inteligente da RAN por meio de orientação baseada em políticas, gerenciamento de modelos de aprendizado de máquina e enriquecimento de informação para o Near-RT RIC. Dessa forma, o Non-RT RIC é responsável pelos procedimentos de orquestração, gerenciamento e automação usados para monitorar e controlar os componentes da RAN. A comunicação entre os componentes do SMO e do Non-RT RIC é feita por meio de uma infraestrutura de mensagens interna. O Non-RT RIC oferece dois serviços de gerenciamento e orquestração de alto nível, permitindo que a arquitetura O-RAN seja suficientemente flexível para que o comportamento de cada componente da rede e funcionalidade possa ser ajustado em tempo real, atendendo aos objetivos e intenções das operadoras. O primeiro serviço é o gerenciamento de rede baseado em intenção, que permite às operadoras especificarem intenções utilizando uma linguagem de alto nível. A intenção é automaticamente analisada pelo Non-RT RIC que determina a política e o conjunto de rApps e xApps que devem ser implantadas e executadas para satisfazer as políticas. O segundo serviço é a orquestração inteligente, que permite coordenar e orquestrar as diferentes xApps e rApps que executam em diferentes RICs e locais da rede. Assim, o Non-RT RIC é responsável pela orquestração da inteligência da rede para garantir que as aplicações selecionadas sejam adequadas para satisfazer as intenções da operadora e atender aos requisitos impostos. Além disso, o Non-RT RIC deve garantir que as aplicações sejam instanciadas no local apropriado para garantir o controle sobre os elementos da RAN especificados na intenção, sejam alimentadas com dados relevantes, e sejam robustas o suficiente para não gerarem conflitos por condição de corrida entre as aplicações [Polese et al., 2023]. As rApps devem ser capazes de se comunicarem por meio da interface R1, interna ao Non-RT RIC, para que o arcabouço Non-RT RIC possa oferecer serviços às rApps [O-RAN Working Group 1, 2023].

Além das rApps, o Non-RT RIC é composto pelo arcabouço Non-RT RIC, formado por funções ancoradas e não ancoradas no arcabouço. Dentre as não ancoradas estão [O-RAN Working Group 2, 2023]:

- as funções de gerenciamento e exposição de serviços da interface R1, que permitem registrar e descobrir serviços, enviar notificações sobre serviços, autenticar e autorizar acessos, dentre outras funções;
- a função de gerenciamento de rApp, responsável pelo gerenciamento das rApps no contexto do arcabouço, permitindo a configuração das aplicações, acesso a informações de desempenho e falha, dentre outras funções;
- as funções relacionadas à interface A1, que fornecem acesso às funcionalidades oferecidas pela interface A1 como descoberta de políticas suportadas pela interface e criação, atualização e remoção de políticas, e suporte ao enriquecimento de informação;
- as funções de gerenciamento e exposição de dados, que permitem consumir dados do arcabouço Non-RT RIC e do SMO;
- as funções do fluxo de trabalho AI/ML, que permitem acessar serviços como treinamento de modelos de acordo com pré-requisitos estabelecidos, registro e descoberta de modelos, atualização e armazenamento de modelos, monitoramento do desempenho de modelos implantados; e
- as terminações externas, que permitem ao SMO e ao arcabouço Non-RT RIC trocarem mensagens com entidades externas por meio de interfaces que estejam fora do escopo da arquitetura O-RAN.

As funções ancoradas no arcabouço Non-RT RIC são [O-RAN Working Group 2, 2023]:

- a terminação da interface R1, que possibilita a troca de mensagens entre o arcabouço Non-RT RIC e as rApps para acessar os serviços da interface R1;
- a terminação da interface A1, que permite a troca de mensagens entre o Non-RT RIC e o Near-RT RIC pela interface A1; e
- outras funções do Non-RT RIC, como funções específicas da RAN para gerenciamento de fatias de rede.

A O-Cloud combina nós físicos, componentes de *software* e funcionalidades de gerenciamento e orquestração com o intuito de desacoplar componentes de *hardware* e *software*. A O-Cloud permite o compartilhamento de *hardware* entre diferentes inquilinos e automatiza a implantação e instanciação de funcionalidades da RAN, como Funções Virtuais de Rede (*Virtual Network Functions* – VNFs) encontradas na O-CU e as rApps do Non-RT RIC [Arnaz et al., 2022, Polese et al., 2023]. A Tabela 4.1 resume as funções dos componentes definidos pela O-RAN Alliance na arquitetura O-RAN.

O objetivo das interfaces abertas especificadas pela O-RAN Alliance é padronizar e flexibilizar o acesso aos componentes da RAN, permitindo a conexão entre os diversos componentes da arquitetura de forma interoperável [Arnaz et al., 2022]. A arquitetura O-RAN utiliza as interfaces A1, E2, *Open FrontHaul* (Open FH), O1, O2, R1, ONI (*O-Cloud*

Tabela 4.1. Resumo das funções dos componentes da arquitetura O-RAN.

Componentes	Descrição
SMO	Hospeda o Non-RT RIC e é responsável pelo monitoramento e orquestração da RAN
Non-RT RIC	Suporta rApps, atua em laços de controle maiores que 1 s
Near-RT RIC	Suporta xApps, atua em laços de controle entre 10 ms e 1 s
O-CU	Implementa as camadas superiores da pilha 3GPP: RRC, SDAP, PDCP
O-CU-CP	Componente lógico do plano de controle da O-CU
O-CU-UP	Componente lógico do plano de usuário da O-CU
O-DU	Implementa funções da High-PHY e subcamadas MAC e RLC
O-RU	Implementa funções da Low-PHY e de processamento de sinais de radiofrequência
O-eNB	Estação rádio base 4G/LTE compatível com O-RAN
O-Cloud	Plataforma de computação em nuvem híbrida formada por um conjunto de recursos computacionais e infraestrutura virtualizados reunidos em um ou mais centros de dados

Notification Interface), Y1 e CTI (*Cooperative Transport Interface*) padronizadas pela O-RAN Alliance, e as interfaces E1, F1, X2, Xn, NG e UU, padronizadas pelo 3GPP. Em conjunto com a interface Open FH, as interfaces 3GPP permitem desagregar a gNodeB. Por meio das interfaces padronizadas pela O-RAN Alliance, os RICs obtêm informações sobre a RAN usadas para definir as ações de controle e automação a serem executadas na RAN [Polese et al., 2023]. A Tabela 4.2 resume as interfaces da arquitetura O-RAN e suas terminações.

A interface O1 conecta o SMO aos RICs, à O-eNB, à O-CU e à O-DU, permitindo o gerenciamento e orquestração das funcionalidades de rede [O-RAN Working Group 10, 2023]. A interface A1 é usada para comunicação entre o Non-RT RIC e o Near-RT RIC, permitindo que o Non-RT RIC envie para o Near-RT RIC orientações baseadas em políticas, gerencie modelos de aprendizado de máquina e envie informações para o Near-RT RIC com o objetivo de otimizar a RAN. Os modelos de aprendizado implantados no Near-RT RIC para otimizar a RAN podem ser refinados com informações enriquecidas fornecidas pelo Non-RT RIC ao Near-RT RIC. A comunicação é feita por meio de mecanismos padronizados baseados em uma sintaxe específica que pode expressar intenções de alto nível e políticas. Dessa forma, permite-se a implementação do controle de não tempo-real e de políticas e modelos inteligen-

Tabela 4.2. Resumo das interfaces O-RAN e 3GPP presentes na RAN aberta.

Interface	Terminação	Tipo
O1	Non-RT RIC, O-eNB, Near-RT RIC, O-CU-CP , O-CU-UP, O-DU e O-RU	O-RAN
A1	Non-RT RIC e Near-RT RIC	O-RAN
E2	Near-RT RC e Nós E2	O-RAN
Open FH	O-DU e O-RU	O-RAN
O2	SMO e O-Cloud	O-RAN
ONI	O-Cloud, Near-RT RIC, O-RU, O-DU e O-CU	O-RAN
Y1	Near-RT RIC e consumidor Y1	O-RAN
CTI	O-DU e nó da rede de transporte	O-RAN
R1	rApp e arcabouço Non-RT RIC	O-RAN
E1	O-CU-CP e O-CU-UP	3GPP
F1	O-CU-CP, O-CU-UP e O-DU	3GPP
X2, Xn, NG	O-CU-CP, O-CU-UP e funções 3GPP	3GPP
Uu	UE, O-eNB, O-RU, O-DU e O-CU	3GPP

tes no Near-RT RIC [Polese et al., 2023]. O Near-RT RIC usa a interface A1 com o Non-RT RIC também para descoberta, requisição e entrega de informações enriquecidas, além de descoberta de informações de enriquecimento provenientes de fontes externas [Polese et al., 2023]. A interface E2 permite a comunicação entre o Near-RT RIC e os componentes lógicos denominados Nós E2, isto é, os componentes que são pontos de terminação para essa interface. Assim, a O-CU, a O-DU e a O-eNB compõem os Nós E2. Por meio da interface E2 são transmitidos dados de telemetria da RAN e as respostas de controle do Near-RT RIC [Polese et al., 2023]. O Near-RT RIC pode executar ações sobre os Nós E2, como monitoramento, suspensão, parada e controle do comportamento do nó [O-RAN Working Group 3, 2023b].

A interface Open FH possibilita a interação entre O-RUs e O-DUs, permitindo o controle das operações da O-RU a partir da O-DU e a distribuição das funcionalidades de camada física entre a O-DU e a O-RU. Como deve existir forte sincronização entre as duas unidades, a interface Open FH oferece uma referência de relógio compartilhada [Polese et al., 2023]. Para ofertar esses serviços, a interface Open FH inclui quatro planos: controle (C-Plane), usuário (U-Plane), gerenciamento (M-Plane) e sincronização (S-Plane). A interface O2 conecta o SMO à O-Cloud para suportar as funcionalidades que executam na nuvem. Essa interface oferece funções tanto para gerenciar a infraestrutura em nuvem quanto para gerenciar implantações na infraestrutura [O-RAN Working Group 6, 2023]. A O-RAN Alliance considera adotar para a interface O2 padrões e soluções abertas, como os padrões da *European Telecommunications Standards Institute* (ETSI) para *Network Function Virtualization* (NFV), interfaces baseadas em serviços do 3GPP e os projetos Kubernetes, OpenStack e ONAP/OSM [Polese et al., 2023]. A ONI permite que componentes da arquitetura implantados na O-Cloud recebam notificações com informações críticas de eventos e estado da O-Cloud que outrora seriam conhecidos apenas pela infraestrutura de nuvem. A interface CTI permite a comunicação com nós da rede de transporte para controle dinâmico da alocação de largura de banda quando se utiliza uma rede de transporte ponto-a-multiponto. A interface Y1 permite o consumo de informações de análise (*analytics*) do Near-RT RIC por entidades que estão dentro ou fora de um domínio de confiança PLMN (*Public Land Mobile Network*), denominadas consumidores Y1.

As interfaces E1, F1, X2, Xn, NG e Uu possibilitam a interoperabilidade entre componentes da RAN aberta e componentes herdados de outras gerações da RAN. A interface E1 permite realizar a conexão entre O-CU-CP e O-CU-UP. A interface F1 conecta elementos da O-DU e O-CU para troca de informação sobre o compartilhamento de recursos de rádio e sobre outros estados da rede. As interfaces X2 e Xn ajudam com a interoperabilidade entre nós de diferentes gerações. A interface NG conecta nós 5G à rede de núcleo quando está operando no modo *standalone*. Por fim, a interface Uu permite a conexão dos UEs às O-eNBs e às O-RUs [O-RAN Working Group 1, 2023].

4.2.2. Requisitos de Segurança

As especificações de segurança da O-RAN Alliance buscam alcançar os objetivos de uma arquitetura de "confiança zero" (*Zero-Trust Architecture* – ZTA) [O-RAN Working Group 1, 2023]. A confiança zero (*Zero Trust* – ZT) é um paradigma de cibersegurança focado na proteção de recursos e tem como premissa nunca

confiar em nenhum dispositivo ou usuário, sejam eles internos ou externos ao perímetro de segurança definido. Assim, todos os dispositivos e usuários devem ser avaliados antes de terem acesso a qualquer recurso [Rose et al., 2020]. Portanto, no paradigma ZT, mesmo que um usuário ou dispositivo esteja autenticado em um sistema, não há garantia de que terá autorização a acessar os recursos daquele sistema. Cada solicitação de acesso a um recurso é autorizada e monitorada individualmente durante o período de acesso para verificar a conformidade com as regras da política de segurança, autenticação e autorização iniciais [Ramezanpour e Jagannath, 2022]. Assim, ao aplicar ZT à RAN, não há confiança implícita de um usuário ou recurso, mesmo levando em consideração a localização física, localização de rede ou posse do recurso.

A ZTA é uma arquitetura baseada no paradigma ZT, permitindo aplicar a confiança zero no sistema de forma fim-a-fim, ou seja, abrangendo identidade (humana e não-humana), credenciais, acesso de gerenciamento, operação, pontos de terminação (*endpoints*), ambientes de hospedagem e interconexões de infraestrutura. Tanto as ameaças internas quanto as externas devem ser consideradas na ZTA e, dessa forma, seu uso na RAN aberta reduz os riscos associados à superfície de ataque aumentada [O-RAN Working Group 1, 2023]. A ZTA é definida na especificação NIST 800-27 e deve incluir suporte para uma Infraestrutura de Chave Pública (*Public Key Infrastructure* – PKI) com autenticação mútua baseada em certificados. A especificação também prevê a utilização de ZTA em infraestrutura de rede, com um controlador capaz de configurar e reconfigurar a rede de acordo com a concessão de acesso a um usuário ou dispositivo [Rose et al., 2020].

A arquitetura O-RAN segue os princípios de segurança do 3GPP e as melhores práticas da indústria, trabalhando em direção ao ZT como princípio orientador para que a RAN aberta ofereça o nível de segurança esperado pelos operadores e usuários das redes móveis celulares. A O-RAN Alliance especifica requisitos de segurança para cada componente e interface, com a intenção de proteger ativos críticos. A segurança na arquitetura é fundamentada em criptografia, certificados X.509v3 e IKEv2 (*Internet Key Exchange version 2*) e nos protocolos mTLS (*mutual Transport Layer Security*), TLS, IPsec (*Internet Protocol Security*), SSH (*Secure Shell*), DTLS (*Datagram Transport Layer Security*) e CMPv2(*Certificate Management Protocol version 2*). Os requisitos de segurança são agrupados em três categorias: (i) funções de rede e aplicações, (ii) interfaces abertas e (iii) requisitos transversais [O-RAN Working Group 11, 2023c], discutidas a seguir.

4.2.2.1. Funções de Rede e Aplicações

Na primeira categoria incluem-se todos os componentes da arquitetura O-RAN e as aplicações que executam nos RICs. De forma geral, exige-se que esses componentes e aplicações suportem a autenticação e a autorização de funções internas e de sistemas externos e sejam capazes de se recuperarem de ataques DDoS (*Distributed Denial of Service*) massivos que cheguem por uma interface interna ou externa. As comunicações internas e externas devem suportar autenticação mútua, confidencialidade, integridade e proteção contra reprodução. A Tabela 4.3 apresenta uma lista não exaustiva dos requisitos de segurança especificados para os componentes da O-RAN, exceto O-CU, O-DU, O-RU e O-eNB [O-RAN Working Group 11, 2023c, O-RAN Working Group 11, 2023b,

Abdalla e Marojevic, 2023]. Esses quatro componentes devem suportar os mesmos requisitos de segurança especificados para CU, DU, RU e O-eNB definidos pelo 3GPP nas especificações TS 33.501 e TS 33.401. A Tabela 4.4 mostra os protocolos utilizados para suportar os requisitos.

Tabela 4.3. Requisitos de segurança para componentes da arquitetura O-RAN.

Requisito	Near-RT RIC	xApp	Non-RT RIC	rApp	SMO	O-Cloud
Armazenamento seguro						✓
Atualização segura					✓	✓
Autenticação multifator					✓	✓
Autenticação mútua	✓	✓	✓	✓	✓	✓
Auto-configuração segura	✓		✓	✓		✓
Autorização	✓		✓	✓	✓	✓
Boot seguro	✓		✓	✓		✓
Capacidade de recuperação e *backup*	✓	✓	✓	✓	✓	✓
Computação em nuvem segura	✓	✓	✓	✓		
Comunicação confiável						✓
Confidencialidade	✓					✓
Confidencialidade de registros					✓	✓
Controle de acesso		✓	✓	✓	✓	✓
Criptografia	✓	✓	✓		✓	✓
Gerenciamento de chaves		✓	✓	✓		✓
Gerenciamento de segurança de software de código aberto	✓		✓			
Integridade de registros					✓	
Isolamento robusto	✓	✓		✓		✓
Monitoramento contínuo	✓			✓	✓	✓
PKI		✓	✓	✓		
Privacidade	✓		✓	✓	✓	✓
Proteção contra reprodução						✓
Recuperação contra ataques DDoS	✓		✓	✓	✓	
Registro contínuo	✓			✓	✓	✓
Transferência segura de registros					✓	
Tratamento de vulnerabilidades contínuo	✓			✓	✓	✓
Virtualização segura	✓	✓	✓	✓		✓

Tabela 4.4. Protocolos de segurança recomendados pela O-RAN Alliance para componentes da arquitetura O-RAN. (MFA: *Multi-Factor Authentication*)

Requisito	Near-RT RIC	Non-RT RIC	SMO	O-Cloud	O-DU	O-RU	rApps	xApps
Autenticação	TLS, mTLS, X.509v3, IPsec, IKEv2		mTLS, X.509v3, TLS, PSK	TLS, mTLS, X.509v3, MFA	802.1X	802.1X		TLS, mTLS, X.509v3, IPsec, IKEv2
Confidencialidade	TLS, IPsec		TLS	TLS, Criptografia⋆				
Integridade	TLS, IPsec		TLS	TLS, X.509v3				
Autorização	OAuth 2.0	OAuth 2.0	OAuth 2.0	OAuth 2.0			OAuth 2.0	OAuth 2.0
Proteção contra reprodução				TLS, Resumo criptográfico⋆				
Exportação de registros			FTPES, TLS, SSH, mTLS, X.509v3					

⋆Conforme algoritmos especificados em [O-RAN Working Group 11, 2023b].

Os requisitos de segurança para a O-Cloud protegem os pacotes de aplicações e funções virtualizadas na camada de aplicação, isto é, xApps, rApps, O-CU, O-DU e Near-RT RIC; da camada de infraestrutura. A proteção da camada de infraestrutura ainda não está completamente especificada. Em relação à camada de aplicação, a O-Cloud deve suportar autenticação e autorização de usuários, recomendando-se o uso de autenticação por múltiplos fatores. As aplicações e funções que se comunicam entre si devem estar mutuamente autenticadas e autorizadas. A autenticidade e integridade das imagens das aplicações e funções que executam na O-Cloud devem ser garantida e, para tal, utilizam-se resumos criptográficos e assinaturas com a chave privada do fornecedor daquela aplicação ou função. As imagens armazenadas no repositório de imagens da O-Cloud devem ser protegidas em relação à confidencialidade e integridade, e podem ser acessadas apenas por entidades autorizadas. Os pacotes devem ser testados pelos fornecedores em relação a vulnerabilidades conhecidas antes de serem instanciados na O-Cloud. As informações sensíveis existentes nesses elementos devem estar criptografadas, de forma que a arquitetura deve suportar criptografia simétrica ou assimétrica. Deve existir registro contínuo de modificações realizadas em cada aplicação ou função entre versões e monitoramento contínuo do repositório para verificar se modificações, exclusões ou adições não autorizadas foram realizadas no repositório. É importante prover um isolamento robusto dos dados em trânsito, usados e armazenados, e controle de acesso aos recursos da infraestrutura. Em relação à camada de infraestrutura, são especificados requisitos e controle para prover atualização segura. As imagens dos pacotes devem estar sempre atualizadas e antes de serem atualizadas devem ser assinadas pelo fornecedor para assegurar a autenticidade e integridade. Deve haver capacidade da O-Cloud de se recuperar de incidentes na atualização ou instalação de pacotes [O-RAN Working Group 11, 2023c].

O Non-RT RIC deve suportar autorização e ser capaz de se recuperar de ataques DDoS massivos provenientes das interfaces A1 e R1. A autorização ocorre via OAuth2.0.

As rApps também devem ser capazes de suportar autorização e se recuperarem de ataques DDoS, porém provenientes da interface R1. O Near-RT RIC deve oferecer serviço de autenticação e autorização, de forma que apenas xApps autenticadas e autorizadas possam acessar a NIB. As xApps devem ser autenticadas com a assinatura do fornecedor antes de serem instanciadas e devem ter sua integridade verificada ao serem registradas no Near-RT RIC, usando assinaturas tanto do provedor de serviço quanto do fornecedor da xApp. As APIs do Near-RT RIC devem suportar autenticação mútua para que as xApps possam ser autenticadas. As APIs também devem suportar autorização, para que apenas xApps autorizadas segundo as políticas da operadora possam acessá-las. Ademais, o Near-RT RIC deve ser capaz de se recuperar de ataques DDoS massivos provenientes da interface A1. A autenticação mútua é realizada por meio do protocolo mTLS com certificados X.509v3. Atualmente as APIs relacionadas aos nós E2 são especificadas para executarem sobre SCTP (*Stream Control Transmission Protocol*) com Protobuf como protocolo de codificação. Essas APIs são consideradas de tempo crítico e não são suportadas pelo protocolo TLS. A autenticação de APIs relacionadas aos nós E2 é baseada em IPsec com certificado IKEv2. A autorização é feita por meio de OAuth2.0. A confidencialidade e a integridade são suportadas por TLS, exceto para APIs relacionadas aos nós E2, que utilizam IPsec nesse caso [O-RAN Working Group 11, 2023c].

O SMO deve suportar autenticação e autorização de funções internas e sistemas externos, além de confidencialidade, integridade, autenticação mútua e proteção contra reprodução para comunicações internas e externas. A comunicação externa deve adicionalmente ser autorizada. O SMO deve ser capaz de se recuperar de ataques DDoS massivos tanto internos quanto externos, seguindo o princípio de ZT. A autorização é feita por meio de OAuth 2.0 (*Open Authorization* 2.0), enquanto a autenticação é suportada por mTLS com certificados X.509v3. Opcionalmente, o SMO também pode suportar autenticação usando TLS com chave pré-compartilhada (*Pre-Shared Key* – PSK). A segurança dos registros de segurança produzidos pelo SMO também é destacada pela O-RAN Alliance. Os registros devem ser acessados apenas por agentes autorizados, autenticados mutuamente, e deve-se garantir a confidencialidade e integridade do conteúdo. Os registros de segurança gerados pelo SMO podem ser armazenados tanto local quanto remotamente. No caso de armazenamento remoto, deve haver suporte à escolha de servidores para transferência segura. Os registros de segurança devem ser armazenados separadamente dos registros do sistema. Além de mTLS e X.509v3, a segurança dos registros de segurança deve suportar FTPES (*File Transfer Protocol over explicit transport layer security*) e pode suportar o uso de PSK (*Pre-Shared Key*), sendo também sugerido o suporte a SSH e SFTP (*Secure File Transfer Protocol*), para transferência segura de arquivos [O-RAN Working Group 11, 2023c].

4.2.2.2. Interfaces Abertas

Na segunda categoria de requisitos estão as interfaces abertas, que de forma geral, devem suportar autenticação, autorização, confidencialidade, integridade e proteção contra reprodução. As interfaces devem também suportar o uso de NACM (*Network Configuration Access Control Model*) quando o NETCONF (*Network Configuration Protocol*) for usado pelas operadoras da rede para gerenciar as funções O-RAN. O NACM

fornece os meios para restringir o acesso dos usuários a um subconjunto pré-configurado de todas as operações e conteúdos disponíveis do NETCONF. O NACM também permite que as operadoras integrem autenticação e autorização com uma plataforma centralizada de gerenciamento de acesso, protejam a configuração em execução contra modificação e exclusão não autorizadas, e ofereçam suporte a procedimentos de gerenciamento de mudanças para atualizar as configurações das funções de rede e as alterações na instância do NACM em uma função de rede [O-RAN Working Group 11, 2023c]. A Tabela 4.5 resume os requisitos das interfaces e a Tabela 4.6 mostra os protocolos usados para suportar os requisitos.

Tabela 4.5. Requisitos de segurança para as interfaces especificadas pela O-RAN Alliance.

Requisito	A1	O1	O2	E2	R1	Open FH			
						U-Plane	M-Plane	C-Plane	S-Plane
Autenticidade		✓							
Autenticação	✓		✓	✓	✓		✓	✓	✓
Confidencialidade	✓	✓	✓	✓	✓	✓	✓		
Integridade	✓	✓	✓	✓	✓	✓	✓		
Autorização	✓	✓		✓	✓			✓	✓
Proteção contra reprodução	✓		✓	✓	✓				
Proteção contra *spoofing* de relógio mestre									✓
Proteção contra homem no meio									✓
Proteção contra remoção									✓

Tabela 4.6. Protocolos de segurança recomendados pela O-RAN Alliance para as interfaces abertas.

Requisito	A1	O1	O2	E2	R1	Open FH			
						U-Plane	M-Plane	C-Plane	S-Plane
Autenticidade		TLS							
Autenticação	TLS, mTLS		TLS, mTLS, X.509v3	IPsec	TLS, mTLS	802.1X, TLS, SSH	TLS, SSH, mTLS, X.509v3	802.1X	
Confidencialidade	TLS	TLS	TLS	IPsec		PDCP	TLS, SSH		
Integridade	TLS	TLS	TLS	IPsec		PDCP	TLS, SSH		
Autorização	OAuth 2.0	NACM	OAuth 2.0		OAuth 2.0	802.1X		802.1X	802.1X
Proteção contra reprodução	TLS	TLS	TLS	IPsec		PDCP	TLS, SSH		

A interface A1 deve suportar autenticação mútua, autorização, confidencialidade, integridade e proteção contra reprodução. A autenticação é feita por mTLS e autorização por OAuth2.0. Os outros requisitos são suportados pelo protocolo TLS. A interface O1

pode revelar informações sensíveis a usuários não autorizados caso seja implementada inadequadamente. A interface deve prover confidencialidade, integridade e autenticidade por meio de TLS e autorização usando NACM [O-RAN Working Group 11, 2023c]. As interfaces O2 e E2 devem suportar confidencialidade, integridade, proteção contra reprodução e autenticação da origem dos dados. A interface O2 suporta TLS, enquanto a E2 suporta IPsec. A autenticação mútua na interface O2 ocorre por meio de mTLS com certificados X.509v3. A interface Open FH é dividida em planos. O plano de controle deve suportar autenticação e autorização das O-DUs, usando o protocolo IEEE 802.1X. O plano de usuário deve suportar confidencialidade e integridade, o que é feito por meio do protocolo PDCP (*Packet Data Convergence Protocol*). O plano de sincronização deve suportar autenticação e autorização, proteção contra ataques de *spoofing* de relógio mestre e homem no meio. A arquitetura de sincronização deve prover redundância, suportando múltiplos relógios mestres. A autenticação e autorização ocorrem por meio do protocolo IEEE 802.1X. O plano de gerenciamento deve prover integridade, confidencialidade e autenticação por meio de SSH e TLS. As sessões NETCONF devem ser protegidas por conexões TLS ou túneis SSH. Podem ser utilizadas senhas e certificados X.509 para autenticação. A interface R1 deve suportar autorização via OAuth2.0, autenticação mútua via mTLS, e confidencialidade, integridade e proteção contra reprodução via TLS. A interface ONI deve suportar autenticação mútua por meio de mTLS com certificados X.509v3 e autorização por meio de OAuth2.0 [O-RAN Working Group 11, 2023c].

4.2.3. Requisitos Transversais

Na última categoria estão os requisitos transversais, formulados de forma mais genérica e que se aplicam a todo o sistema O-RAN. Existem grupos de requisitos transversais, que incluem, por exemplo, protocolos e serviços de rede e gerenciamento do ciclo de vida das aplicações. Os protocolos e serviços devem ser robustos o suficiente para lidar com entradas não esperadas, ataques DDoS massivos e ataques contra autenticação baseada em senha, caso esse tipo de autenticação seja usado. Também deve haver robustez do sistema operacional e das aplicações instaladas, com identificação e documentação clara das vulnerabilidades conhecidas. O gerenciamento de ciclo de vida das aplicações requer a garantia de autenticidade e integridade de xApps, rApps, O-CU, O-DU, O-RU e Near-RT RIC; proteção da integridade das aplicações e funções virtualizadas; capacidade de atualização segura dessas aplicações e funções; monitoramento do consumo e disponibilidade de recursos dessas aplicações e funções; controle de acesso e a divulgação imediata de vulnerabilidades descobertas com atualizações rápidas com intuito de mitigá-las. No entanto, a especificação não detalha concretamente como prover a segurança nessa categoria [O-RAN Working Group 11, 2023c].

4.3. Vulnerabilidades e Ameaças de Segurança

Esta seção discute ameaças e vulnerabilidades de segurança dos componentes e interfaces da RAN aberta e das tecnologias relacionadas. Destacam-se riscos tecnológicos referentes à adição de novos componentes à RAN e ao uso de interfaces abertas, de *software* de código-fonte aberto, de técnicas de virtualização e de inteligência artificial.

4.3.1. Vulnerabilidades

Existem potenciais vulnerabilidades na RAN aberta que podem ser exploradas por ataques contra a confidencialidade, integridade e disponibilidade. Essas vulnerabilidades podem ser específicas da arquitetura O-RAN ou gerais [O-RAN Working Group 11, 2023a].

Entre as vulnerabilidades específicas da arquitetura O-RAN estão (i) o acesso não-autorizado aos componentes O-DU, O-CU-CP, O-CU-UP e O-RU para degradar o desempenho da RAN ou executar um ataque mais abrangente à rede, comprometendo a disponibilidade da RAN; (ii) a falta de proteção à sincronização e ao tráfego de controle na interface Open FH, que pode afetar a integridade e disponibilidade; (iii) a desabilitação da cifragem na transmissão aérea (*over-the-air*) para bisbilhotagem e, assim, comprometer a confidencialidade dos dados transmitidos; (iv) os conflitos entre o Near-RT RIC e a O-eNB e entre as xApps e rApps, que podem comprometer a disponibilidade dos serviços da RAN; (v) o acesso das xApps e rApps a dados da rede e de seus usuários, o que caracteriza quebra da confidencialidade; (vi) a interface de gerenciamento não protegida que implica problemas de confidencialidade, integridade e disponibilidade e, por fim, (vii) o ataque por injeção de mensagens do O-CU-CP ao O-CU-UP, comprometendo sua disponibilidade.

Entre as vulnerabilidades gerais estão (i) o desacoplamento de funções sem uma Raiz de Confiança protegida por *hardware* ou uma Cadeia de Confiança em *software*, o que pode levar a problemas de integridade; (ii) a exposição a explorações públicas e conhecidas em função do uso de *software* com código-fonte aberto e, por fim, (iii) a configuração incorreta, o isolamento fraco ou o gerenciamento de acesso insuficiente na plataforma O-Cloud. Tanto (ii) quanto (iii) podem trazer problemas de confidencialidade, integridade e disponibilidade.

4.3.2. Ameaças

O modelo de ameaças, adotado neste capítulo, determina a superfície de ataque e identifica os pontos de entrada e os agentes de ameaças à RAN aberta. Sabe-se que a RAN aberta introduz novos componentes e adota interfaces padronizadas e abertas entre eles. Tal característica, aliada à desagregação de *hardware* e *software*, à virtualização, ao uso de componentes de *software* de código e aberto e ao uso de inteligência artificial, expande a superfície de ataque da rede, como mostra a Figura 4.2. No caso da arquitetura O-RAN, a superfície de ataque é definida pelos (i) novos componentes, SMO, Non-RT RIC e Near-RT RIC; (ii) as novas interfaces, A1, E2, O1, O2 e Open FH; (iii) o uso de virtualização para desagregação do *software* e *hardware*; (iv) o uso de *software* de código-fonte aberto e (v) o uso de técnicas de inteligência artificial. Ameaças para cada um dos pontos da superfície de ataque da O-RAN são apresentadas nas próximas seções. São considerados, ainda, pontos de entrada: as APIs entre os planos que facilitam a propagação de ameaças, as ameaças vindas de dentro da RAN aberta e as ameaças vindas de fora da RAN aberta. São considerados agentes de ameaças cibercriminosos, atacantes internos, ativistas, ciberterroristas, *script kiddies* e nações-estado [O-RAN Working Group 11, 2023a].

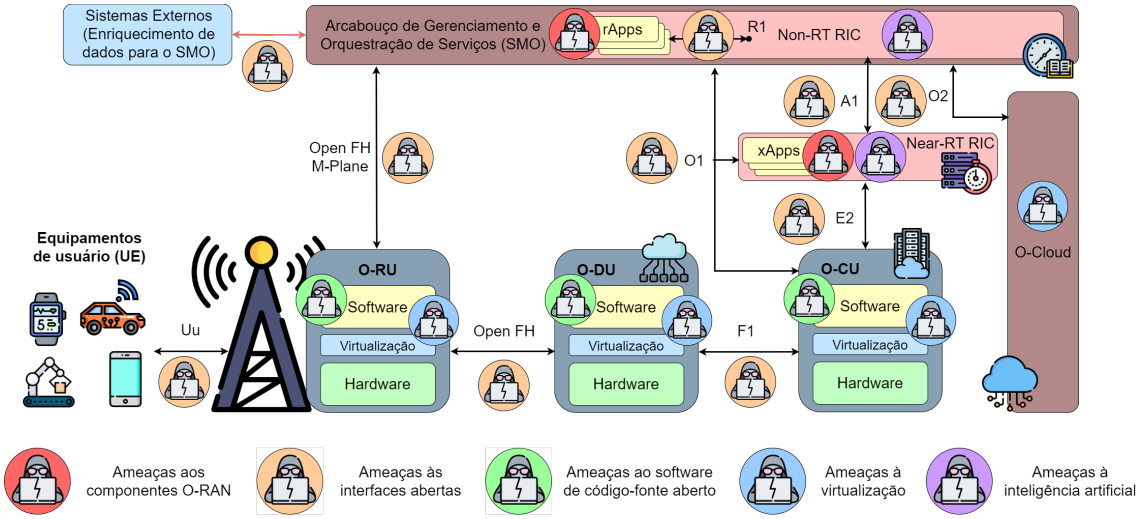

Figura 4.2. A superfície aumentada de ataque da RAN aberta com base na arquitetura O-RAN.

4.3.2.1. Novos Componentes: Controladores Inteligentes e Arcabouço de Orquestração e Gerenciamento de Serviços

Qualquer xApp pode possuir vulnerabilidades. Porém, se a xApp for desenvolvida por uma fonte não confiável ou por uma fonte que não a mantenha de forma adequada, as chances de vulnerabilidades aumentam [Open RAN Policy Coalition, 2021]. Se atacantes identificam uma xApp que pode ser explorada, eles podem interromper o serviço oferecido pela rede e potencialmente assumir o controle de outra xApp ou de todo Near-RT RIC. Nesse cenário, um atacante pode ganhar a habilidade de alterar dados transmitidos através das interfaces A1 e E2, extrair informação sensível e impactar as funções do Near-RT RIC para degradar o seu desempenho [Abdalla et al., 2022].

Uma xApp maliciosa em execução no Near-RT RIC pode explorar a identificação de um equipamento de usuário, rastrear a localização de um UE e alterar a prioridade do UE [O-RAN Working Group 11, 2023a]. As xApps no Near-RT RIC podem manipular o comportamento de uma célula, de um grupo de UEs e até mesmo de um UE específico. A ausência de uma raiz de confiança ou uma raiz de confiança com mau funcionamento pode causar problemas na rede e comprometer o desempenho da RAN e a privacidade dos usuários. Uma xApp pode, por exemplo, rastrear um dado usuário ou impactar o serviço para um assinante ou o serviço para uma determinada área coberta pela RAN. As xApps podem receber uma ordem através da Interface A1 para priorizar um determinado UE. Se uma xApp for maliciosa e receber tal ordem, então o proprietário da xApp maliciosa saberá que há um usuário privilegiado em uma determinada área. Assim, a partir dessa exposição de comandos, a xApp maliciosa poderá rastrear o usuário privilegiado ou até mesmo alterar seu nível de privilégio.

A Interface E2, que faz a comunicação do Near-RT RIC e os nós E2, também expõe a identificação de um UE que pode ser explorada por uma xApp maliciosa. Assim como a A1, a Interface E2 pode apontar para um UE específico na rede, criando uma correlação entre as identidades aleatórias (anonimizadas) dos UEs entre os nós da RAN.

Por exemplo, uma xApp pode ser usada como um farejador de rede para identificar um UE, como mostra a Figura 4.3. Essa vulnerabilidade também está presente na comunicação Non-RT RIC-A1. Entretanto, o desafio para a comunicação Near-RT RIC-E2 é maior do que para a comunicação Non-RT RIC-A1, porque espera-se que a frequência de sinalização na E2 será maior para possibilitar a operação em quase tempo real. Assim, o identificador do UE será mais frequentemente enviado pela Interface E2 do que pela A1.

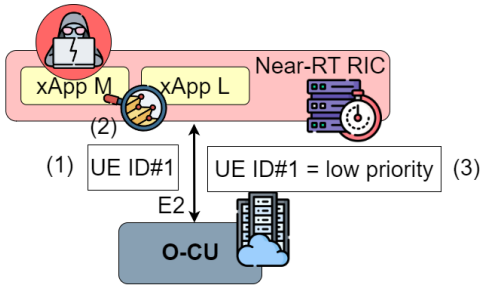

Figura 4.3. Uma xApp maliciosa atua como farejador de rede. A xApp legítima L recebe a identificação de um UE via interface E2 (Passo 1). A xApp maliciosa M tem a capacidade de escutar todas as mensagens que são enviadas pela interface E2. Por isso, também recebe o identificador do UE (Passo 2). Em seguida, a xApp M pode enviar uma mensagem à O-CU para reduzir a prioridade do UE #1 (Passo 3).

Outra ameaça às xApps é a criação de políticas A1 falsas que podem impactar o desempenho da RAN. Isso é possível no cenário em que há acesso não autorizado ao Non-RT RIC. É esse controlador que cria as políticas A1 e as envia ao Near-RT RIC para sua aplicação. Além disso, políticas enviadas ao Near-RT RIC, falsas ou legítimas, são persistentes até que sejam modificadas ou excluídas pelo Non-RT RIC ou até que o Near-RT RIC seja desligado. Políticas A1 falsas podem ser criadas do zero ou a partir da modificação de uma política A1 legítima existente para se chegar a uma política A1 falsa. Uma política A1 falsa pode, por exemplo, ter como alvo um UE específico, grupos de UEs ou uma célula inteira. Em outro exemplo, uma política falsa A1 pode fazer com que o Near-RT RIC configure funções da O-DU e da O-RU para iniciar um ataque de negação de serviço usando dados de realimentação para degradar o desempenho da RAN. As políticas A1 falsas também podem ser usadas para localizar um UE ou um grupo de UEs. Nesse caso, a política A1 falsa faz com que o Near-RT RIC isole um UE na O-CU. O Near-RT RIC também pode usar a conformação de feixe do MIMO (*Multiple Input Multiple Output)* na O-DU e na O-RU para isolar o UE em um único feixe. Os dados de realimentação da RAN podem incluir a localização do UE ou a informação de trajetória obtidas com os dados de GPS. A localização do usuário seria obtida a partir do acesso ao Non-RT RIC.

Outras ameaças ao Near-RT RIC são xApps maliciosas que obtenham acesso não-autorizado ao próprio Near-RT RIC e aos nós E2, que abusem de informações de rádio e recursos de controle sobre funções da RAN, que impactem o serviço de um usuário ou de uma dada área, que explorem a identificação de um UE, rastreiem a localização do UE e mudem a prioridade da fatia de rede do UE.

Assim como podem existir vulnerabilidades nas xApps, também podem existir vulnerabilidades nas rApps. Caso consiga explorar uma rApp, um atacante pode alterar

dados transmitidos pela Interface A1, extrair informações sensíveis, interromper o serviço oferecido pela rede e assumir o controle de outra rApp ou até mesmo do Non-RT RIC. Um atacante pode penetrar o Non-RT RIC através do SMO para disparar um ataque de negação de serviço e, assim, degradar o desempenho desse controlador. Nesse caso, o Non-RT RIC não seria confiável para garantir (i) o monitoramento da rede para entender o efeito de uma política A1 no desempenho do Near-RT RIC; (ii) a atualização de uma política A1; (iii) a exposição e a entrega segura da informação enriquecida A1 para o Near-RT RIC e, por fim, (iv) a implantação de regras de controle de acesso. Além disso, um atacante que consiga penetrar o Non-RT RIC através do SMO pode rastrear um UE e modificar e corromper dados.

Podem existir também conflitos entre rApps, causados de forma não intencional ou de forma maliciosa, que impactem o desempenho da RAN. Esses conflitos são possíveis porque as rApps são fornecidas por diferentes vendedores. Por exemplo, um vendedor fornece a rApp para escalonamento de licença de operadora, outro vendedor fornece a rApp para gerenciamento do consumo de energia etc. Com isso, há o risco de diferentes rApps tomarem decisões conflitantes ao mesmo tempo para um dado usuário. Os conflitos podem ser (i) diretos, nos quais diferentes rApps solicitam alteração de um mesmo parâmetro, (ii) indiretos, quando diferentes rApps solicitam alteração de diferentes parâmetros que criam efeitos opostos, e (iii) implícitos, quando diferentes rApps solicitam alteração de diferentes parâmetros que não criam efeitos opostos óbvios, mas que resultam em degradação do desempenho de toda a rede, instabilidades etc.. Os conflitos implícitos são difíceis de serem resolvidos por conta da dificuldade de se observar e identificar as dependências entre os parâmetros modificados pelas rApps.

Atacantes externos e internos podem explorar mecanismos fracos de autenticação e autorização no SMO. Se mecanismos de autenticação não são implementados corretamente ou não são suportados pelas Interfaces A1, O1, O2 e interfaces externas no SMO, um atacante externo pode explorar tais interfaces sem credenciais apropriadas para ganhar acesso ao SMO. Um atacante externo também pode explorar a ausência ou deficiência dos mecanismos de autorização do SMO. Nesse caso, um atacante externo que acesse as Interfaces A1, O1, O2 e as interfaces externas do SMO, mesmo sem autorização ou com um *token* de acesso incorreto, pode invocar uma função do SMO. Dados relacionados a tal função serão, então, vazados para o atacante. Além disso, o atacante pode executar determinadas ações como divulgar informações sensíveis da O-RAN ou alterar os componentes da O-RAN. Da mesma forma, atacantes internos que acessem a Interface R1 e o barramento interno de mensagens podem invocar funções e executar ações. Por fim, uma vez que tenha acesso ao SMO, um atacante pode ver, modificar ou apagar arquivos de registros (*log*) armazenados no arcabouço, bem como envenenar dados de treinamento ou os modelos de inteligência artificial armazenados no SMO para influenciá-los.

4.3.2.2. Interfaces Abertas

Existem ameaças às diferentes interfaces que interconectam os componentes da arquitetura O-RAN, como a O-CU, O-DU e O-RU, e também à interface de rádio que dá acesso aos usuários da RAN.

Um atacante pode penetrar e comprometer a RAN aberta através das Interfaces Open FH, O1, O2, A1 e E2 da RAN. Tais interfaces permitem a programabilidade da rede e podem não estar protegidas de acordo com as melhores práticas de segurança da indústria, por exemplo, não implementando mecanismos de autenticação e processos de autorização adequados, cifragem e verificações de integridade, proteção contra ataques de repetição, prevenção de reutilização de chaves, validação de entradas, resposta a condições de erro, entre outros [Open RAN Policy Coalition, 2021]. As interfaces O-RAN permitem o uso do TLS ou SSH. As atuais melhores práticas da indústria obrigam o uso de TLS versão 1.2 ou superior ou SSH com autenticação baseada em cerificados [O-RAN Working Group 11, 2023a]. Uma interface que em sua implementação use uma versão do TLS inferior a 1.2 ou SSH com autenticação baseada em senha pode ser o ponto-chave a ser explorado por um atacante que deseja comprometer a RAN aberta.

Se forem usados mecanismos de autenticação e controle de acesso fracos, é possível para um atacante criar uma estação-base falsa para enganar a O-DU e as UEs para se associarem a ela e não a uma estação-base legítima. Para tanto, um atacante se passa por uma rede móvel legítima e emprega um ataque de homem-no-meio entre o UE e a rede móvel, como mostra a Figura 4.4. Um atacante sequestra a rede *fronthaul*, isto é, o atacante (i) desabilita o acesso da O-RU legítima e operacional à Interface Open FH, (ii) conecta a estação-base falsa na Interface Open FH da O-RU legítima e, em seguida, (iii) inicia o ataque da estação-base falsa com a O-RU fornecendo a interface aérea para os UE. Para um UE, a estação-base falsa é legítima e ele se conectará a ela. Assim, a estação-base falsa é capaz de interceptar e divulgar a identidade de um usuário e registrar de forma não autorizada sua localização e movimentação. Para o operador da rede móvel legítima, a O-RU legítima simplesmente deixou de servir os UEs em sua área de cobertura, desde que o atacante desabilitou a Interface Open FH. Ataques que implementam estações-base falsas são conhecidos desde as primeira gerações de redes móveis e, apesar dos incrementos de segurança, ainda estão presentes nas redes 5G [O-RAN Working Group 11, 2023a].

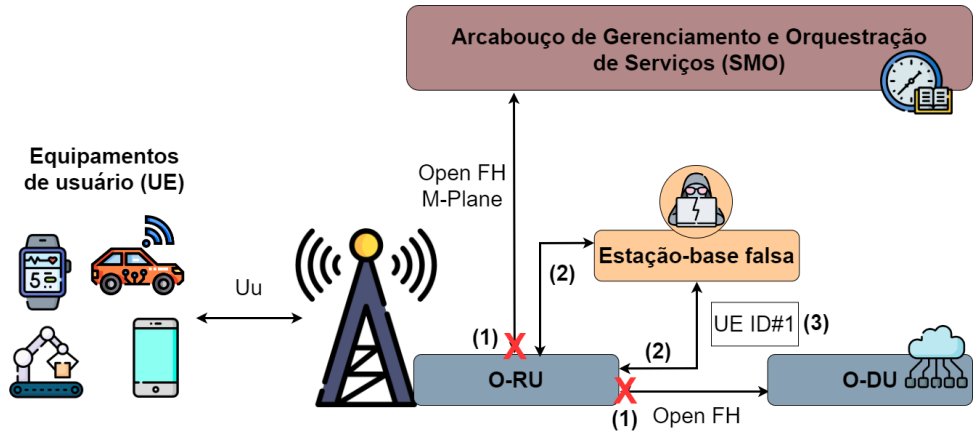

Figura 4.4. O ataque da estação-base falsa. Um atacante desabilita o acesso da O-RU legítima à Interface Open FH (Passo 1). Em seguida, o atacante conecta a estação-base falsa na Interface Open FH da O-RU legítima (Passo 2) e inicia o ataque com a O-RU ainda fornecendo a interface aérea para os UEs. O atacante pode, por exemplo, obter um identificador de um UE, conectado à O-RU legítima (Passo 3).

A Interface A1 é usada para comunicação entre o Non-RT RIC e o Near-RT RIC. Se um mecanismo fraco de autenticação mútua é usado entre esses controladores, um Non-RT RIC malicioso pode se tornar par de um Near-RT RIC legítimo através da Interface A1 ou um Near-RT malicioso pode se tornar par de um Non-RT RIC legítimo, também através dessa interface. Além disso, se um ataque de homem-no-meio é implementado entre os controladores, as políticas enviadas pela Interface A1 podem ser lidas e modificadas e falsas políticas podem ser injetadas. Com isso, o Near-RT RIC pode receber políticas maliciosas.

Ataques à interface de rádio que dá acesso aos usuários da RAN são ataques clássicos a sistemas de comunicação sem fio, como o *jamming*, farejamento e falsificação (RAN *sniffing and spoofing*). Esses ataques estão fora do escopo deste capítulo.

4.3.2.3. Virtualização

A virtualização envolve funções físicas de rede (*Physical Network Function* – PNF), funções virtuais de rede (*Virtual Network Function* – VNF), funções em nuvem de rede (*Cloud Network Function* – CNF), o SMO, o hipervisor, as máquinas virtuais e os contêineres. Todos esses elementos podem sofrer com ameaças e vulnerabilidades. São considerados cinco tipos de ameaças à virtualização: (i) comprometimento de imagens VNF/CNF, (ii) configurações fracas do orquestrador, controles de acesso e isolamento fracos, (iii) uso indevido de uma máquina virtual ou contêiner para atacar outra máquina virtual ou contêiner, hipervisor ou motor de contêiner, e outros sistemas finais, (iv) bisbilhotagem do tráfego de rede para acessar todos os dados da RAN aberta processados na carga de trabalho e (v) comprometimento dos serviços de rede auxiliares e de suporte. Um atacante pode, por exemplo, explorar uma falha de configuração ou uso de mecanismos fracos de controle de acesso e isolamento para ganhar acesso não-autorizado ao SMO. Tal orquestrador pode executar diferentes máquinas virtuais/contêineres, cada uma gerenciada por diferentes usuários e com diferentes níveis de sensibilidade. Se o acesso fornecido aos usuários não estiver em conformidade com seus requisitos específicos, um atacante ou usuário descuidado pode afetar a operação de outra máquina virtual/contêiner gerenciada pelo SMO. Dados sensíveis de usuários também podem ser acessados e vazados caso implementações da RAN aberta nativas em nuvem sofram com mecanismos de isolamento insuficientes. Ao se implementar uma O-CU em nuvem, é possível comprometê-la por meio de vetores de ameaças, como a migração de serviço, descarregamento de tráfego ou mecanismos de *handover* [Ranaweera et al., 2021]. Uma O-CU comprometida é capaz de prejudicar as direções *fronthaul* e *backhaul* se aproveitando das interfaces abertas da Open RAN.

Um exemplo de ameaça pela falta de isolamento forte é o ataque de fuga de máquina virtual ou contêiner (*VM/Container escape attack*) [O-RAN Working Group 11, 2023a], ilustrado na Figura 4.5. VNFes/CNFes em execução na mesma máquina física como inquilinos compartilham o mesmo núcleo e os recursos do sistema operacional do hospedeiro. A falta de isolamento forte entre as máquinas virtuais ou contêineres e o hospedeiro traz o risco de uma máquina virtual ou contêiner não-autorizado escapar do confinamento e impactar outras máquinas virtuais

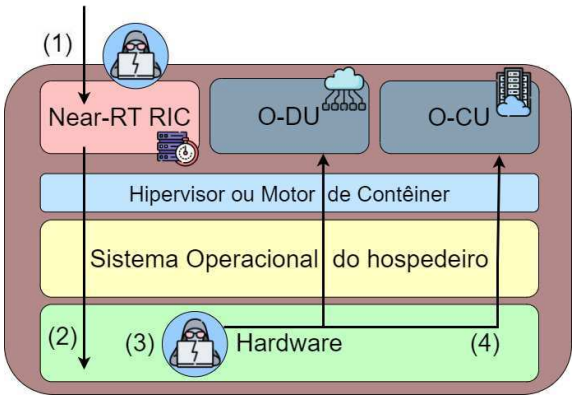

Figura 4.5. O ataque de fuga de uma máquina virtual ou contêiner. Nesse exemplo, o Near-RT RIC, a O-DU e a O-CU são inquilinos de um mesmo hospedeiro. Um atacante consegue acesso não-autorizado ao Near-RT RIC (Passo 1). Em seguida, por falta de isolamento forte, o Near-RT RIC malicioso escapa do isolamento (Passo 2) e ganha controle do hospedeiro (Passo 3). O atacante incia um ataque de negação de serviço contra a O-DU e a O-CU (Passo 4).

ou contêineres co-hospedados. Se uma máquina virtual ou contêiner malicioso escapa do isolamento, ela pode ganhar controle total do seu hospedeiro e o atacante pode: (i) se tornar capaz de iniciar ataques do hospedeiro ou comprometer o hospedeiro, (ii) comprometer a confidencialidade e a integridade das máquinas virtuais co-hospedadas e dos inquilinos, (iii) iniciar um ataque de negação de serviço às máquinas virtuais ou aos contêineres co-hospedados e aos serviços do hospedeiro para degradar seu desempenho e, por fim, (iv) introduzir novas vulnerabilidades no hospedeiro para serem exploradas em ataques futuros.

Um atacante também pode criar uma nova máquina virtual ou contêiner malicioso configurado sem regras de rede, limitações de usuários etc. para contornar as defesas existente na infraestrutura da O-Cloud. Se essa máquina virtual ou contêiner malicioso escapa do hospedeiro e alcança o *hardware* do hospedeiro, ela pode ganhar acesso de super-usuário de todo o hospedeiro no qual reside. Isso dá à máquina virtual ou ao contêiner malicioso total controle sobre as máquinas virtuais ou contêineres hospedados no mesmo hospedeiro comprometido. Com isso, o atacante pode impactar a confidencialidade, a integridade e a disponibilidade dos recursos das VNFes/CNFes.

4.3.2.4. Software de Código-Fonte Aberto

Espera-se que os componentes da RAN aberta sejam implementados baseados em *software* de código-fonte aberto e, por isso, herdem as vulnerabilidades conhecidas pela comunidade pelo uso desse tipo de *software* [Liyanage et al., 2023]. A O-RAN Software Community[2] (OSC) é responsável pela implementação das especificações O-RAN em código aberto. É um projeto da Linux Foundation, apoiado pela O-RAN Alliance.

Tanto a academia quanto a indústria reconhecem que o uso de *software* de código-fonte aberto apresenta riscos de segurança. Por falta de conhecimento, desenvolvedores podem usar componentes de *software* com vulnerabilidades conhecidas em listas públi-

[2]Disponível em: `https://www.o-ran.org/software`

cas, por exemplo, a *National Vulnerability Database* (NVD) [3], mantida pela agência NIST do governo norte-americano. Embora tais listas se destinem a desenvolvedores para divulgar vulnerabilidades, elas também podem ser usadas por atacantes para explorar as vulnerabilidades divulgadas. Sabe-se ainda que as vulnerabilidades se propagam mais rapidamente à medida que há reuso de *software* de código-fonte aberto mais frequentemente. Desenvolvedores podem também usar bibliotecas não confiáveis, sem o devido cuidado com o gerenciamento de dependências e correções. Da mesma forma, desenvolvedores podem obter componentes de *software* de código-fonte aberto em repositórios não confiáveis. Tais problemas se agravam porque fornecedores e operadores da RAN aberta podem não ter inventários precisos de dependências de *software* de código-fonte aberto usadas por suas diferentes aplicações ou um processo para receber e gerenciar notificações sobre vulnerabilidades descobertas ou remendos disponíveis da comunidade que oferece suporte ao código-fonte aberto.

Outra vulnerabilidade é a introdução de *backdoors* por desenvolvedores confiáveis, que inserem intencionalmente linhas de código malicioso em um componente de código-fonte aberto a ser usado na RAN aberta. Enquanto esse componente é usado e a vulnerabilidade não é detectada, o desenvolvedor confiável, mas, na verdade, malicioso, pode acessar o componente, comprometer dados sensíveis e iniciar ataques de negação de serviço para reduzir o desempenho da RAN.

4.3.2.5. Inteligência Artificial

Há ameaças específicas aos algoritmos e modelos de aprendizado de máquina usados pelos controladores RIC e pelo arcabouço SMO. Uma das ameaças são os ataques de envenenamento de dados, nos quais o atacante altera os conjuntos de dados destinados a treinamento, teste ou validação [Sun et al., 2022]. No caso da alteração dos dados de treinamento, serão usados dados incorretos na modelagem, resultando em um modelo não-confiável. Assim, decisões, previsões, classificações e detecções com base nesse modelo não serão apropriadas. Outro cenário pode ser uma situação em que um modelo está *online* e continua aprendendo durante o uso operacional, modificando seu comportamento ao longo do tempo. Nesse caso, um invasor pode alimentar o modelo com dados incorretos e o modelo pode aprender com esses dados incorretos e, como resultado, afetar negativamente seu desempenho e treinar novamente o modelo para tomar decisões erradas.O acesso para realizar alterações nos dados pode ser obtido via penetração através das redes *fronthaul* ou *mid-haul*, xApps ou rApps.

Outra possível ameaça é o ataque de alteração de modelo, relacionado à integridade da predição. O ataque ocorre quando um atacante obtém acesso não-autorizado ao modelo em produção e altera os parâmetros do modelo, influenciando os resultados produzidos pelo modelo. Consequentemente, isso pode levar a predições erradas e a tomadas de decisão erradas pelo operador da rede. Por fim, ataques de transferência de aprendizado podem ocorrer quando um atacante ajusta de forma maliciosa um modelo pré-treinado já disponível, mascarando seu comportamento malicioso. Mais detalhes sobre ataques aos sistemas de aprendizado de máquina são discutidos na Seção 4.4.

[3]Disponível em `https://nvd.nist.gov/`

4.4. Ataques baseados em Aprendizado de Máquina para RAN

Um modelo de aprendizado de máquina / inteligência artificial desenvolvido de maneira legítima pode ser comprometido posteriormente [Habler et al., 2022]. O comprometimento pode ocorrer por diversos motivos, incluindo um desenvolvedor de aplicações inteligentes malicioso, *hardware* ou *software* da infraestrutura que sofreu um ataque ou um usuário malicioso que fabrica dados para alterar o modelo ou forçar determinadas respostas na sua inferência.

Os ataques aos sistema de aprendizado de máquina são classificados de acordo com três características principais: (i) capacidade do atacante acessar os parâmetros do modelo; (ii) momento no qual o atacante possui acesso ao modelo; e (iii) acesso ao conjunto de dados utilizado pelo modelo.

A característica (i) é subdividida em três: caixa-branca, caixa-preta e caixa-preta interativa. Em ataques do tipo caixa-branca, o agente malicioso possui acesso ao modelo e seus parâmetros de forma direta. Por outro lado, um ataque caixa-preta identifica que o atacante não possui nenhuma informação sobre o modelo e seus parâmetros. O modelo de atacante caixa-preta interativa assume que o atacante desconhece os parâmetros do modelo, porém é possível interagir com o modelo, recebendo resultados de classificação após o envio de uma amostra. Além disso, quando se considera que o atacante tem acesso ao modelo, o acesso pode ocorrer durante o treinamento ou no momento de inferência, conforme a característica (ii). Por fim, a característica (iii) identifica se o atacante tem acesso ao conjunto de dados de treinamento, podendo ajustar indiretamente os parâmetros do modelo, ou de teste, alterando a entrada sem modificar seus parâmetros internos.

McGraw et al. identificam, a partir da Análise de Risco Arquitetural (*Architectural Risk Analysis* – ARA), dez principais riscos de segurança na implementação de qualquer sistema que possui modelos de aprendizado de máquina em sua linha de execução [McGraw et al., 2020]. Esses riscos podem ser explorados por atacantes para afetar os modelos de aprendizado de máquina incluídos na arquitetura O-RAN:

- **Exemplos adversariais**, em que a entrada do modelo de aprendizado de máquina é alterada intencionalmente por atacantes. O objetivo é produzir entradas parecidas, porém que gerem erros de classificação. Dessa forma, o atacante interfere nos resultados de predição sem modificar os parâmetros do modelo;
- **Envenenamento de dados**, em que um atacante que possua acesso ao conjunto de dados de treinamento introduz pertubações controladas em amostras. O padrão adicionado às amostras faz com que o processo de classificação de amostras futuras seja controlado. Assim, o atacante modifica a predição do modelo de aprendizado de máquina por meio do ajuste de seus parâmetros diretamente;
- **Manipulação de sistemas *online***, em que sistemas que possuem aprendizado contínuo são ajustados ao longo de sua execução. Esse ajuste pode ocorrer de forma controlada por um atacante, com a intenção de prejudicar o sistema de classificação;
- **Ataque à transferência de aprendizado**, em que o atacante pode atacar um modelo base pré-treinado e ajustado, causando vulnerabilidades no modelo final após o reajuste de pesos;

- **Confidencialidade dos dados**, em que é possível inferir informações sobre a entrada de dados a partir de resultados parciais do modelo, gerando risco à privacidade. Dessa forma, é essencial proteger a confidencialidade dos dados e do modelo utilizado, impedindo que o atacante possa executar ataques do tipo caixa-branca. Porém, a interação com o modelo e a observação de sua classificação permite a execução de ataques de extração de modelo;
- **Confiabilidade dos dados**, em que é necessário assegurar que o conjunto de dados é coletado de forma bem definida e com baixo erro de medida. A falta de garantia de integridade pode resultar em ataques de envenenamento de dados. Além disso, erros de captura geram modelos com alta interferência de ruídos, dificultando a predição de comportamentos em novos dados analisados;
- **Reprodutibilidade**, em que é necessário assegurar que os resultados obtidos por modelos de aprendizado de máquina implantados em sistemas reais sejam reprodutíveis em condições semelhantes. Dessa forma, a documentação dos processos desenvolvidos, como a coleta do conjunto de dados, etapas de pré-processamento, hiperparâmetros utilizados, têm que ser apresentados de forma clara e objetiva;
- **Sobreajuste**, em que um atacante com acesso aos hiperparâmetros do modelo ou a grande parte do conjunto de dados de treinamento é capaz de enviesar resultados com a intenção de criar um modelo sobreajustado;
- **Integridade de codificação**, já que a codificação dos dados de entrada é uma parte essencial do problema de otimização de modelos de aprendizado de máquina. A representação utilizada para as amostras é capaz de aumentar a acurácia do modelo final se utilizada da melhor forma. Porém, representações incorretas podem enviesar os resultados de classificação. É necessário garantir que as características de entrada do modelo sejam íntegras, para evitar queda de desempenho em ambiente de produção e o lançamento de ataques através da inserção de valores controlados;
- **Integridade de predição**, o resultado de predição de amostras por um modelo de aprendizado de máquina pode ser alterado tanto a partir da produção de dados falsificados de entrada ou dados falsificados na saída, quanto na alteração direta de parâmetros do modelo ou sua completa substituição. Assim, é necessário garantir a integridade do modelo e de sua predição.

A privacidade do modelo de aprendizado de máquina também é um fator crucial no sistema. Ataques do tipo caixa-branca costumam ser mais efetivos do que ataques nos quais o atacante desconhece os parâmetros do modelo. Contudo, uma forma de obter conhecimento sobre um modelo S sem acesso direto a ele é criar um novo modelo S', com hiperparâmetros similares ao modelo original. Isso é feito através do ataque de extração de modelo, no qual o atacante realiza requisições ao modelo S e o agente malicioso, então, gera um conjunto de dados estimado, $\hat{X}$ e com amostras $\hat{x}_i$ não rotuladas. Os rótulos são obtidos a partir do modelo S, que recebe $\hat{x}_i$ e retorna a sua classe $\hat{y}_i$. Após iterar sobre todas as amostras do conjunto de dados $\hat{X}$, o atacante obtém um conjunto de dados rotulado $(\hat{X}, \hat{Y})$. Então, o atacante treina um modelo S' a partir do conjunto de dados rotulado gerado. O ataque de extração de modelo está relacionado com a confidencialidade dos

dados. Espera-se que a fronteira de decisão do modelo S' seja a mesma ou a mais próxima possível do modelo S. Uma vez que o modelo S' é conhecido pelo atacante, é possível utilizá-lo para estimar os atributos mais discriminantes de S.

Diversas funcionalidades da RAN aberta dependem do funcionamento adequado de modelos de aprendizado de máquina, como direcionamento de tráfego e otimização de recursos. Entretanto, a RAN aberta permite que desenvolvedores, potencialmente maliciosos, implementem as aplicações inteligentes [Groen et al., 2023]. Adicionalmente, equipamentos podem gerar tráfego malicioso. Por exemplo, ataques com exemplos adversariais em caixa preta [Ilyas et al., 2018] podem ser preocupantes. Nesses ataques, assume-se que o atacante pode realizar consultas ao modelo de classificação. No entanto, nos ataques em caixa preta, o atacante não é capaz de conhecer o modelo por completo e nem de derivar outras informações a partir do ataque. Ainda assim, o atacante é capaz de propositalmente gerar amostras que serão classificadas de maneira errônea pelo modelo. Esses erros de classificação podem então ser explorados pelo atacante para causar perturbações a todo o sistema. Dessa forma, um usuário de um sistema de RAN aberta é capaz de enganar o modelo de aprendizado de máquina para obter recursos de rede indevidos a partir da geração de indicadores de desempenho falsificados. Esse problema é uma preocupação comum em infraestruturas gerenciadas por aprendizado de máquina. Por exemplo, Usama *et al.* propõem a combinação do ataque de extração de modelo com exemplos adversariais para enganar classificadores de tráfego [Usama et al., 2019]. Um classificador baseado em redes neurais profundas (*Deep Neural Networks* – DNNs) classifica o tráfego Tor nas classes "*browsing*", "*chat*", "*streaming* de áudio", "*streaming* de vídeo", "email", "transferência de arquivos", "voz sobre IP" e "*peer-to-peer*". Com as entradas maliciosas, a acurácia da classificação decai de 96,3% para 2%. Uma vez que a tarefa de classificação de tráfego orienta diversos mecanismos da RAN aberta, uma classificação com baixa acurácia pode causar sérios prejuízos à rede. Assim, é necessário conhecer os ataques ao aprendizado de máquina que realiza as tarefas, a fim de mitigar seus impactos.

Os ataques mencionados anteriormente fazem parte do grupo geral de ataques a sistemas de aprendizado de máquina. A O-RAN Alliance identifica como ameaças relacionadas aos modelos de aprendizado de máquina o envenenamento de dados do modelo de aprendizado de máquina, a alteração de modelo e o ataque de transferência de aprendizado [O-RAN Working Group 11, 2023a], discutidos na Seção 4.3.2.5. As ameaças da especificação são divididas de uma maneira mais genérica [O-RAN Working Group 11, 2023a], pois visam abranger diversos cenários de implementação. Um dos cenários considerados é aquele no qual ambos o Non-RT RIC e o SMO atuam no treinamento e inferência dos modelos. Em outro cenário, considera-se que o Non-RT RIC atua no treinamento e o Near-RT RIC atua na inferência do modelo. Por fim, considera-se o cenário no qual o Non-RT RIC atua no treinamento e o O-DU e o O-CU atuam na inferência do modelo.

Inicialmente, esta seção apresenta os trabalhos que mencionam componentes O-RAN. Em seguida, apresentam-se trabalhos mais gerais que abordam os ataques baseados em aprendizado de máquina em RAN. Apesar de gerais, esses ataques podem ocorrer na arquitetura O-RAN e em outras arquiteturas de RAN aberta, por serem inerentes ao uso de aprendizado de máquina na interface sem fio.

4.4.1. Ataques na Arquitetura O-RAN

Habler *et al.* fornecem uma análise sistemática de aprendizado de máquina adversarial na arquitetura O-RAN [Habler et al., 2022]. Assim, os autores avaliam as ameaças na arquitetura utilizando uma ontologia de avaliação de riscos e propondo uma taxonomia para tal. O modelo de ameaças proposto define o modelo do atacante, os agentes de ameaça e seus objetivos. O modelo do atacante de Habler *et al.* lista diferentes capacidades que o atacante precisa conhecer ou acessar para realizar um ataque bem-sucedido. O trabalho propõe uma nomenclatura para classificar as diferentes capacidades, que podem ser de acesso ou de conhecimento. Na capacidade de acesso, o atacante possui acesso não-autorizado a componentes, como RICs, O-CUs e O-DUs, e consegue acessar componentes utilizados no fluxo de trabalho de aprendizado de máquina. Na capacidade de conhecimento, o atacante não possui acesso ao sistema, mas possui algum tipo de informação sobre os alvos. A Figura 4.6 mostra a nomenclatura proposta por Habler *et al.* [Habler et al., 2022].

As capacidades de acesso podem ser subdivididas em acesso ao modelo e acesso aos dados, como mostra a Figura 4.6. Na primeira categoria, o atacante tem o conhecimento da saída do modelo. Assim, é possível realizar uma requisição ao modelo e obter uma resposta. A saída pode ser o vetor de probabilidades da inferência, como a saída da

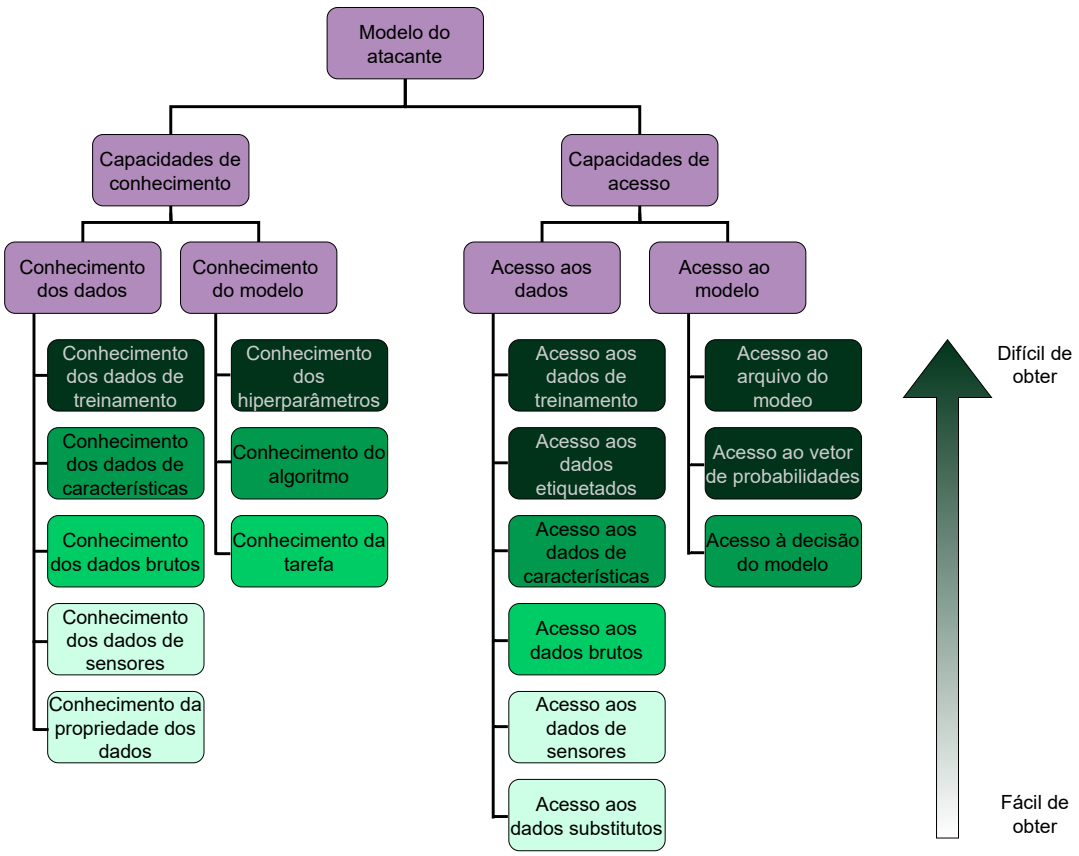

Figura 4.6. Modelo de atacante de Habler *et al.*, com as diferentes capacidades que o atacante pode ter. Os blocos referentes a cada capacidade estão marcados em verde. A cor mais escura representa as capacidades mais difíceis de o atacante obter. Adaptado de [Habler et al., 2022].

função *softmax* em uma DNN, ou apenas sua decisão, isto é, a classe inferida pelo modelo. No acesso aos dados, o atacante obtém os dados usados em alguma fase do fluxo de trabalho de aprendizado de máquina. Como exemplo, é possível citar dados brutos ou pré-processados usados no treinamento, vetores de características retirados do modelo, dados obtidos dos sensores, como UEs conectados à rede, e acesso a um conjunto de dados substituto, com as mesmas características e distribuição do utilizado no modelo.

As capacidades de conhecimento, por sua vez, consistem em conhecer informações da arquitetura e da implantação da infraestrutura O-RAN. Essas capacidades podem ser de conhecimento do modelo e conhecimento dos dados. No conhecimento do modelo, é possível conhecer seus hiperparâmetros, tais como a arquitetura da rede neural e a taxa de aprendizado, o algoritmo usado para o treinamento ou a tarefa realizada na inferência, por exemplo, classificação de tráfego. No conhecimento dos dados, o atacante pode conhecer informações sobre os dados de treinamento, os vetores de características, os dados brutos ou propriedades dos dados, como sua distribuição.

Os agentes de ameaça do modelo, que podem ter as capacidades mencionadas anteriormente, são [Habler et al., 2022]:

- **Desenvolvedor de aplicações de *software* O-RAN.** Responsável por desenvolver o software implantado nos componentes O-RAN, como rApps, xApps e mecanismos da O-DU e O-CU. O modelo assume que esse agente possui controle total do contêiner que executa o componente atacado. Entretanto, por atuar a nível de aplicação, suas ações e capacidades estão limitadas à aplicação específica desenvolvida pelo agente;
- **Desenvolvedor de infraestrutura de *software* O-RAN.** Responsável por desenvolver a infraestrutura O-RAN, por exemplo, seus mecanismos de escalonamento, de troca de mensagens, de banco de dados, e arcabouços de desenvolvimento de xApps e rApps. As ações e capacidades desse tipo de agente podem comprometer qualquer aplicação executada na infraestrutura;
- **Provedor da infraestrutura de *software* de conteinerização.** A infraestrutura de *software* consiste em implantações de contêineres, como as fornecidas pelo Kubernetes. Esse agente pode comprometer qualquer um dos contêineres que controla e, consequentemente, suas aplicações;
- **Provedor da infraestrutura de *hardware*.** Esse agente pode comprometer todo o *software* que executa na infraestrutura, visto que controla o seu *hardware*, como os servidores que hospedam os contêineres;
- **Equipamento de Usuário (UE).** Esse agente pode manipular seu próprio comportamento para atacar os modelos de aprendizado de máquina, por exemplo, manipulando dados de seus sensores para enganar sistemas de aprendizado contínuo;
- **Dados de terceiros e/ou provedores de modelo.** Modelos de O-RAN podem ser baseados em dados de terceiros [Couto et al., 2023a]. Esses dados podem ser maliciosos, comprometendo os modelos usados na infraestrutura. Além disso, modelos obtidos via provedores podem ser comprometidos.

Dentre os objetivos do atacante definidos por Habler *et al.*, é possível citar a manipulação, que compromete a integridade da rede. Como exemplo, é possível citar a geração de amostras adversariais para enganar os modelos. Outro objetivo é a negação de serviço, comprometendo a disponibilidade da rede. Nesse caso, o exemplo pode ser comprometer um modelo que classifica uma O-RU como a melhor a ser escolhida por todos os UEs. Dessa forma, o enlace de rádio será sobrecarregado, comprometendo todos os UEs que acessam essa O-RU. O terceiro objetivo definido é a divulgação de informações, comprometendo a privacidade na rede. Um exemplo é a exposição dos padrões de *handover* de um usuário a partir de análise das saídas ou vetores de características dos modelos.

O modelo de ameaças é proposto para mapear quais tipos de ataques, também chamados de famílias de ataques, são possíveis para cada modelo do atacante e agente de ameaça. Esses tipos são listados a seguir:

- **Evasão.** Consiste em induzir o modelo a fornecer saídas incorretas para uma entrada específica, comprometendo a integridade da RAN aberta. Como exemplo, um modelo de QoE (*Quality of Experience*) pode classificar um sinal de uma O-RU como excelente que, na verdade, seria classificado como ruim;
- **Envenenamento.** Similar à evasão, mas que gera uma saída errada para um conjunto de amostras, comprometendo a integridade e disponibilidade da RAN aberta. Por exemplo, um modelo de QoE pode alocar todos os UEs para um determinado O-RU, tornando-a indisponível;
- **Inferência de associação.** O atacante pode verificar se uma determinada amostra está no conjunto de treinamento, comprometendo a privacidade na RAN aberta. Ou seja, é possível saber, por exemplo, a localização de um UE por meio da identificação de padrões específicos do conjunto de treinamento;
- **Reconstrução dos dados.** O vazamento de informações do modelo, como vetores de características, pode permitir a reconstrução dos dados usados no seu treinamento, comprometendo a privacidade. Por exemplo, pode ser possível inferir um padrão de mobilidade entre os usuários de uma localidade da rede;
- **Extração de modelo.** Esse tipo de ataque compromete a privacidade por meio de extração de informações sobre o modelo. Essas informações são usadas para construir uma réplica do modelo e, assim, obter informações do ambiente. Por exemplo, é possível replicar um modelo de QoE e conseguir classificar o tráfego de uma determinada O-RU;
- **Exaustão de recursos.** Nesse tipo de ataque, que compromete a disponibilidade, o atacante torna a inferência do modelo mais lenta para um conjunto de amostras. Por exemplo, um modelo de QoE pode demorar um tempo proibitivo para classificar o tráfego e tomar decisões.

Shi e Sagduyu propõem um ataque a tarefas de fatiamento de rede executadas por uma xApp que utilize aprendizado por reforço [Shi e Sagduyu, 2021]. Os autores utilizam aprendizado por reforço em um UE malicioso para realizar pedidos por recursos de uma

RBS até que seus recursos sejam exauridos. Os autores assumem que o atacante conhece a recompensa do modelo utilizado pela RBS para oferecer recursos aos UEs. Assim, o trabalho aplica aprendizado por reforço para construir pedidos falsos que maximizem a recompensa do algoritmo de gerenciamento ao mesmo tempo, de forma a ocupar o máximo de recursos da RBS. Os autores demonstram uma queda significativa na recompensa obtida pelos algoritmos de gerenciamento sob ataque. Em outro trabalho, Shi e Sagduyu descrevem um ataque de inferência de associação em um modelo de classificação de sinais da rede sem fio [Shi e Sagduyu, 2023]. Nesse trabalho, a classificação é utilizada para autorizar o acesso de dispositivos em uma rede sem fio por meio de sinais da camada física. De acordo com os autores, esse tipo de classificação pode executar como uma xApp no Near-RT RIC. Assim, a xApp legítima pode utilizar um modelo treinado para classificar UEs como autorizados ou não. A autenticação pela camada física é uma estratégia que pode ser utilizada com dispositivos computacionalmente limitados, como os dispositivos da Internet das Coisas (*Internet of Things* – IoT), que não suportam mecanismos sofisticados de segurança. Para treinar o modelo, os UEs autorizados enviam previamente sinais para o provedor de serviços, por exemplo, uma O-RU. Devido às características do *hardware* de rádio, o sinal é enviado com um deslocamento de fase específico de cada equipamento [Shi e Sagduyu, 2023]. Além disso, o canal utilizado entre o usuário e a O-RU possui características únicas de ganho e deslocamento de fase, o que também diferencia os UEs. Dessa forma, um processo de autenticação pelos sinais da camada física consiste em um modelo receber o deslocamento de fase e potência do sinal de um UE e classificá-lo como "autorizado" e "não-autorizado".

O ataque descrito no trabalho de Shi e Sagduyu é do tipo caixa preta, uma vez que consiste em o atacante observar diferentes resultados de classificação para diversos sinais do meio sem fio [Shi e Sagduyu, 2023]. A partir dessa observação, treina-se um modelo substituto, que pode ser utilizado para o atacante produzir sinais que possam burlar o mecanismo de autenticação. Para construir o modelo, o atacante se beneficia do sobreajuste do modelo original. Como o modelo original não é perfeitamente generalista, é possível diferenciar se uma determinada amostra está presente no conjunto de treinamento, isto é, se é oriunda de um usuário legítimo, e então construir o substituto. Para evitar o ataque, Shi e Sagduyu propõem um esquema de defesa que tenta construir um modelo próximo ao do atacante, um modelo sombra. A ideia é adicionar ruído ao sinal para diminuir a acurácia do modelo sombra e, consequentemente, do modelo do atacante.

O Envenenamento de Migração de Portadores (*Bearer Migration Poisoning* – BMP) [Soltani et al., 2023] é um ataque ao RIC quase tempo-real que dispara um processo de migração de portadora de forma maliciosa. O contexto de portadoras se refere a um processo de sinalização transmitido por meio da interface E1. Essa informação é necessária para estabelecer requisitos de recursos e encaminhamento de mensagens dos serviços de plano de usuário. O RIC quase tempo-real é o elemento da arquitetura O-RAN responsável por estabelecer as informações e alterar o contexto de portadoras. O objetivo do atacante é modificar o caminho do plano de tráfego e causar anomalias na rede, atacando o modelo de aprendizado de máquina do RIC, que toma decisões automáticas sobre o plano de tráfego da rede. Os autores que propõem o ataque assumem que um modelo no qual o atacante é capaz de comprometer dispositivos com vírus, cavalos de troia e *malwares* ou ser um usuário interno ao sistema. Assim, controlando dispositi-

vos internos, o adversário falsifica mensagens do protocolo de descoberta da camada de enlace (*Link Layer Discovery Protocol* – LLDP), que são propagadas para o RIC, que é forçado a tomar decisões incorretas. Esse ataque utiliza o princípio de exemplos adversariais para gerar mensagens incorretas, utilizadas como entrada do modelo de aprendizado de máquina, para prevenir decisões corretas do controlador de rádio inteligente.

4.4.2. Outros Ataques à Interface Sem Fio

Ataques à interface sem fio podem ocorrer em diversas arquiteturas RAN. Assim, há na literatura trabalhos que, independentemente da existência de uma RAN aberta ou não, abordam ataques baseados em aprendizado de máquina na interface sem fio. A camada física da RAN aberta pode utilizar inteligência artificial para sensoriamento de espectro, classificação automática de sinais e alocação ótima de blocos de recurso. Entretanto, um atacante que observa o meio e envia um sinal malicioso gera perturbações na entrada de modelos em treinamento ou em produção para efetuar ataques. Os ataques e defesas utilizados em outros problemas de aprendizado de máquina não são necessariamente aplicáveis em comunicações sem fio, devido à natureza dinâmica do canal de comunicação [Adesina et al., 2023]. Os trabalhos relacionados a esse tópico são muito heterogêneos quanto ao tipo de tarefa de aprendizado, aos tipos de ataque, aos mecanismos de defesa e às tecnologias de radiofrequência (RF) utilizadas. A discussão a seguir oferece um panorama dos tipos mais comuns de ataques e defesas em diversas aplicações de aprendizado de máquina na interface sem fio.

Restuccia *et al.* formulam um problema de otimização para calcular um sinal modulado em fase e quadratura (I/Q) malicioso [Restuccia et al., 2020]. O atacante envia sinais que interferem com os sinais dos usuários legítimos para trocar o resultado de um modelo para classificação de espectro no receptor. Os autores realizam experimentos com conjuntos de dados reais e demonstram a eficácia do treinamento adversarial, um mecanismo de defesa baseado em treinar o modelo já usando amostras maliciosas. Karunaratne *et al.* considera um receptor que utiliza um modelo de aprendizado profundo, denominado autenticador, para decidir se as amostras I/Q vêm de um transmissor autorizado a transmitir [Karunaratne et al., 2021]. O atacante utiliza uma Rede Generativa Adversarial (*Generative Adversarial Network* – GAN), na qual o discriminador é o autenticador e o gerador é uma rede que deve aprender a gerar amostras que imitem as de um usuário autêntico. O trabalho realiza experimentos com um Rádio Definido por *Software* comercial (*Software Defined Radio* – SDR), mas não apresenta nenhum mecanismo de defesa.

Os ataques de cavalo de troia à interface sem fio consistem em realizar um envenenamento de dados ao longo do treinamento do modelo de aprendizado de máquina associado ao gerenciamento da interface sem fio [Davaslioglu e Sagduyu, 2019]. O objetivo do ataque é ativar um comportamento desejado pelo atacante durante a execução do modelo. Para isso, o atacante necessita ter acesso ao modelo de treinamento e ao conjunto de dados utilizado para alterar rótulos das amostras de treinamento e criar os padrões que mudam o comportamento do modelo. Davaslioglu *et al.* apresentam um ataque de cavalo de troia a uma rede neural que classifica a técnica de modulação a partir do sinal I/Q recebido [Davaslioglu e Sagduyu, 2019]. O atacante adiciona amostras envenenadas ao conjunto de treinamento e, posteriormente, transmite sinais com a mesma fase para provocar erros. O aumento da base de dados e o uso de testes estatísticos na inferên-

cia reduzem a eficácia do ataque. No trabalho de Wang *et al.*, os transmissores utilizam um modelo de aprendizado por reforço profundo para escolher a frequência do melhor canal na hora de acessar o meio [Wang et al., 2020b]. O atacante também utiliza um mecanismo adaptativo para ocupar o canal selecionado pelo modelo da vítima e bloquear sua transmissão, reduzindo a acurácia do aprendizado por reforço. Uma das contribuições do trabalho é propor mecanismos de defesa que forçam a escolha de um canal pior, dificultando o atacante em encontrar padrões de ataque.

A Tabela 4.7 compara os trabalhos discutidos nessa seção, classificando-os entre os tipos definidos por Habler *et al.* e descritos na Seção 4.4.1.

Tabela 4.7. Trabalhos sobres ataques à RAN baseados em aprendizado de máquina.

Trabalho	Fase do ataque	Acesso ao modelo	Tarefa de aprendizado	Tipo de ataque	Defesa
[Shi e Sagduyu, 2021]	Treinamento Inferência	Caixa branca	Alocação de recursos	Exemplos Adversariais	-
[Shi e Sagduyu, 2023]	Inferência	Caixa preta	Autenticação de sinal	Inferência da associação	Aprendizado adversarial
[Soltani et al., 2023]	Inferência	Caixa preta	Disparo de migração de portadores	Exemplos adversariais	Aprendizado adversarial
[Restuccia et al., 2020]	Inferência	Caixa branca	Classificação de espectro	Evasão	Aprendizado adversarial
[Karunaratne et al., 2021]	Inferência	Caixa preta	Autenticação de sinal	Extração de modelo Evasão	-
[Davaslioglu e Sagduyu, 2019]	Treinamento	Caixa preta	Classificação de modulação	Envenenamento	Testes estatísticos
[Wang et al., 2020b]	Treinamento Inferência	Caixa preta	Seleção de canal para MAC	Evasão	Teoria de controle, políticas ortogonais

4.5. Desafios e Tendências de Pesquisa

Esta seção foca desafios de segurança em aberto[4] e tendências de pesquisa. O primeiro desafio está relacionado à falta de um arcabouço de segurança abrangente e universal para RAN aberta que atenda a todos os requisitos de segurança e permita o controle da segurança durante o ciclo de vida da RAN aberta[5]. As soluções existentes concentram-se em questões específicas de segurança em diferentes planos da arquitetura lógica, mas nenhuma é capaz de defender contra todas as ameaças ou satisfazer todos os requisitos. Outro desafio está relacionado à necessidade de aprimorar as soluções de alocação e gerenciamento de recursos de rádio para assegurar a disponibilidade do sistema da RAN aberta [Wang et al., 2021]. O gerenciamento seguro de recursos de espectro, incluindo detecção, compartilhamento e alocação de espectro, representa um desafio significativo. As técnicas atuais de detecção de espectro, como métodos de detecção de energia, são insuficientes para lidar com todas as ameaças de espectro no complexo ambiente de comunicação da RAN aberta. O terceiro desafio é a preservação da privacidade na RAN aberta [Singh e Khoa Nguyen, 2022]. A preservação da privacidade é essencial para garantir a conformidade com as leis de proteção de dados pessoais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) na União Europeia. A RAN aberta emprega

[4]Disponível em `https://ntia.gov/sites/default/files/publications/open_ran_security_report_full_report_0.pdf`.

[5]Disponível em `https://www.vodafone.com/sites/default/files/2023-02/joint-mou-white-paper-mwc-2023.pdf`.

dados pessoais dos usuários para a prestação de serviços personalizados e otimizados, como localização e identidades dos usuários. O gerenciamento da confiança na RAN aberta [Ramezanpour e Jagannath, 2022] é um desafio importante, uma vez que a rede aberta estabelece a interoperação entre *hardware* e *software* de diferentes fornecedores. Estabelecer um ambiente confiável é crucial para a segurança da cooperação entre diferentes operadoras e fornecedores. O quinto desafio de segurança que se destaca na RAN aberta é a segurança da camada física devido à natureza aberta e desacoplada dessa camada [Polese et al., 2023]. Por fim, ainda existem desafios de segurança para a camada de virtualização e contêineres, como garantir o isolamento entre ambientes e assegurar o desempenho adequado, além de desafios relacionados às interfaces abertas. As interfaces abertas implementam serviços de mensageria que requerem atenção para evitar a injeção de mensagens e para garantir a integridade e confidencialidade das mensagens trocadas. Para abordar essas lacunas de pesquisa, tendências promissoras incluem: (i) desenvolver um arcabouço de segurança abrangente e universal para a RAN aberta; (ii) desenvolver um mecanismo de autenticação contínua, eficiente e seguro, baseado no conceito de "confiança-zero" (zero-trust)[Ramezanpour e Jagannath, 2022], para acesso e comutação de usuários na RAN aberta, considerando cenários de migração de usuários entre operadoras; (iii) desenvolver mecanismos de reputação que permitam o compartilhamento seguro de recursos entre diferentes operadoras; (iv) projetar um mecanismo de preservação de privacidade para RAN aberta, com o objetivo de evitar vazamento de dados e garantir a conformidade com as leis de proteção de dados pessoais; e (v) propor mecanismos de isolamento seguros para ambientes de virtualização e contêineres, visando garantir a segurança geral da infraestrutura virtualizada. As tendências de pesquisa têm como objetivo o desenvolvimento de uma RAN aberta abrangente e segura, melhorando sua resiliência contra ameaças de segurança e atendendo aos requisitos das arquiteturas de referência para os casos de uso previstos. A seguir, os desafios, tendências e oportunidades de pesquisa são detalhados.

4.5.1. Desafios de Pesquisa

Embora existam iniciativas com o intuito de gerar especificações e viabilizar a criação de RANs abertas, interoperáveis, virtualizadas e inteligentes, existem desafios a serem superados, conforme ilustrados na Figura 4.7. Esta seção discute os desafios de pesquisa no gerenciamento e orquestração de serviços em RAN aberta.

Virtualização da Infraestrutura

A arquitetura de referência O-RAN para as RANs abertas enfrenta o desafio de virtualizar a infraestrutura para fornecer serviços mais avançados e ágeis aos usuários finais [Niknam et al., 2022]. A virtualização é uma técnica que permite criar ambientes com interfaces semelhantes às reais, isolados, sobre uma infraestrutura física compartilhada, permitindo que diferentes serviços e aplicativos sejam executados. A virtualização permite que diferentes serviços e aplicativos sejam executados em um ambiente isolado dos demais, melhorando a eficiência de alocação de recursos e a escalabilidade da rede, possibilitando à rede oferecer os serviços avançados e ágeis. No entanto, a virtualização da infraestrutura pode ser um desafio significativo na arquitetura O-RAN. Isso ocorre porque a virtualização requer uma infraestrutura de *hardware* e *software* que possa suportar a execução de diferentes serviços nos ambientes virtuais. Além disso, a virtualização pode

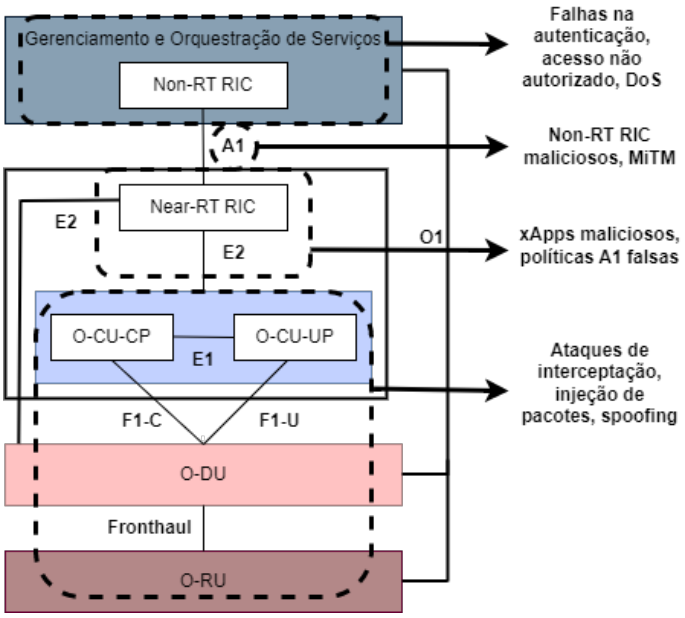

Figura 4.7. Desafios de segurança na arquitetura O-RAN. As aplicações e interfaces em uma rede O-RAN estão sujeitas a sofrerem certos tipos de ataque como de injeção de pacotes ou *spoofing*, mas também podem sofrer com vulnerabilidades na má autenticação, que podem levar usuários maliciosos a comprometerem a rede.

aumentar a complexidade da rede, o que pode tornar a implantação e a manutenção mais difíceis. Para superar esse desafio, é importante desenvolver novas técnicas e tecnologias para virtualizar a infraestrutura de forma eficiente e eficaz. Isso inclui o uso de tecnologias de virtualização de rede, como NFV. Além disso, é importante desenvolver novas técnicas de gerenciamento e orquestração para garantir que diferentes serviços e aplicativos possam ser executados de forma eficiente e segura em um ambiente virtualizado. Contudo, ressalta-se que a virtualização amplia a superfície de ataque da RAN, já que introduz novos componentes de *software* e realiza o compartilhamento de *hardware*. Assim, é também essencial o desenvolvimento de ferramentas de acompanhamento do ciclo de vida de funções virtuais de rede para mitigar possíveis riscos de segurança durante a execução da função.

Suporte a Diferentes Requisitos de Qualidade de Serviço (QoS)

Um dos desafios associados à implementação da O-RAN é projetar uma arquitetura autônoma orientada a serviços que possa suportar diferentes requisitos de Qualidade de Serviço (QoS). Isso é importante porque diferentes aplicativos têm requisitos de QoS diferentes e a rede deve ser capaz de atender a esses requisitos de forma eficiente [Xu et al., 2021b].

Para enfrentar esse desafio, a arquitetura O-RAN deve ser projetada para ser flexível e adaptável. Isso pode ser alcançado por meio da virtualização da rede, através da execução de diferentes funções da rede em ambientes virtuais, em vez de *hardware* dedicado e de propósito específico. Nesse sentido, adicionar novas funções à rede e atualizá-las conforme necessário são tarefas facilitadas pela virtualização. A arquitetura O-RAN deve ser orientada a serviços, o que significa que a rede deve ser projetada para fornecer

serviços específicos para diferentes aplicativos [Xu et al., 2021b]. Isso pode ser alcançado por meio da segmentação da rede em diferentes fatias de rede (*slices*), cada uma projetada para atender a requisitos específicos de QoS de diferentes serviços, conforme apresentado na Figura 4.8, que mostra um exemplo de rede separada em fatias que receberão recursos de acordo com o perfil de usuários, otimizando a utilização da rede. Outro desafio é garantir que a rede possa gerenciar e controlar o tráfego de forma eficiente, para garantir que os requisitos de QoS sejam atendidos. Isso pode ser alcançado por meio de algoritmos de gerenciamento de tráfego inteligentes, que priorizam o tráfego de serviços críticos e garantem que a largura de banda seja alocada de forma eficiente [Xu et al., 2021b, Das et al., 2017]. Assim, projetar uma arquitetura autônoma orientada a serviços, que possa suportar diferentes requisitos de Qualidade de Serviço (QoS), é um desafio importante na implementação O-RAN que impacta diretamente a segurança da RAN. Isso pode ser alcançado por meio da virtualização da rede, segmentação da rede em diferentes fatias e algoritmos de gerenciamento de tráfego inteligentes.

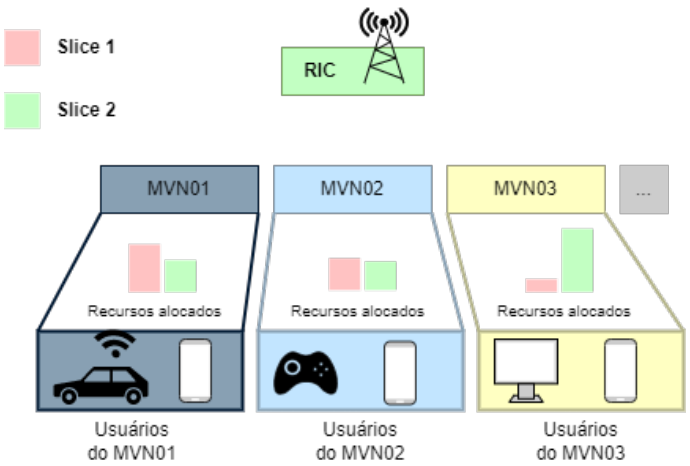

Figura 4.8. Representação de uma forma de segmentação da rede em diferentes fatias, cada uma projetada para atender a um propósito específico. Adaptado de [Xu et al., 2021b].

Controle Inteligente em Tempo Real

O desafio do controle em tempo real na arquitetura O-RAN refere-se à necessidade de garantir que as decisões de controle sejam tomadas em tempo hábil para atender aos requisitos de desempenho das aplicações em tempo real. Isso é particularmente importante para aplicações que exigem uma resposta rápida e confiável da rede, como a automação industrial, a realidade virtual, holografia e a telemedicina. Para atender a esses requisitos, propõe-se a implementação de um terceiro laço de controle em tempo real (RT RIC) a ser situado no O-CU, O-DU ou O-RU. Esse laço de controle em tempo real pode hospedar qualquer tipo de funcionalidade de controle da RAN de camada inferior, que são chamadas de zApps, aplicações de controle de terceiros hospedadas no RT RIC. A introdução de inteligência artificial (IA) permitirá lidar com a complexidade da camada física, dos recursos heterogêneos e dos ambientes operacionais para construir RANs altamente configuráveis e gerenciáveis [Azariah et al., 2022]. No entanto, a implementação de um laço de controle em tempo real apresenta vários desafios de segurança. Um dos principais desafios à disponibilidade é a capacidade de processamento dos nós (O-CU/O-DU) que

precisam ser capazes de lidar com grandes quantidades de dados em tempo real. Além disso, a eficiência energética é uma preocupação importante, pois a implementação de um laço de controle em tempo real pode aumentar o consumo de energia. Outro desafio é a capacidade dos modelos de IA de fornecer decisões em uma escala de tempo de submilissegundos, devido a restrições de tempo de resposta, o que pode ser difícil de alcançar em ambientes de rede em tempo real. Finalmente, a quantidade de sobrecarga de sinalização para o controle de camada física de baixo nível também é um fator crítico que pode ter um impacto adverso no cumprimento dos requisitos de redes celulares de próxima geração com baixa latência [Azariah et al., 2022]. Dessa forma, o desafio do controle em tempo real na arquitetura O-RAN refere-se à necessidade de garantir que as decisões de controle sejam tomadas em tempo hábil para atender aos requisitos de disponibilidade e desempenho das aplicações em tempo real, enquanto se lida com a complexidade da camada física, dos recursos heterogêneos e dos ambientes operacionais. A implementação de um laço de controle em tempo real apresenta vários desafios. Superar esses desafios é fundamental para garantir que a arquitetura O-RAN possa fornecer redes celulares de próxima geração com baixa latência e alto desempenho para aplicações em tempo real. Assim, o controle em tempo real impacta a segurança da rede em duas vertentes principais: a disponibilidade e a confiabilidade. A disponibilidade é afetada pelos desafios referentes ao atendimento dos requisitos de tempo de resposta em escala de submilissegundos. A confiabilidade é afetada pelas necessidade de validação dos modelos de IA para que as ações tomadas em tempo real estejam de acordo com o comportamento esperado da rede. Por fim, ao se considerar o controle em tempo real, a confiabilidade também é diretamente impactada pela explicabilidade dos modelos de IA, já que muitos modelos não são possíveis de serem compreendidos devido à sua complexidade e ao grande número de parâmetros.

Interoperabilidade

O desafio de garantir a interoperabilidade entre diferentes fornecedores e a integração de diferentes tecnologias na arquitetura O-RAN é um dos principais enfrentados na implementação da arquitetura. A interoperabilidade é a capacidade de diferentes sistemas e tecnologias trabalharem juntos de forma eficiente e eficaz, enquanto a integração é a capacidade de diferentes sistemas e tecnologias trabalharem juntos de forma harmoniosa e sem problemas [Wang et al., 2020a, Thiruvasagam et al., 2023]. A interoperabilidade é essencial para permitir que diferentes componentes da arquitetura O-RAN, como as O-RUs, O-DUs e O-CU possam se comunicar e trabalhar juntas de forma eficiente e confiável [Thiruvasagam et al., 2023]. Sem padrões claros e precisos para as interfaces entre esses componentes, pode haver problemas de compatibilidade, interoperabilidade e vulnerabilidades, o que pode levar a atrasos na implantação da arquitetura O-RAN, a custos mais elevados e riscos de segurança. No entanto, garantir a interoperabilidade e a integração segura entre diferentes fornecedores e tecnologias pode ser um desafio significativo. Isso, porque diferentes fornecedores podem ter diferentes abordagens e tecnologias para implementar os componentes da rede. Além disso, as tecnologias podem ter diferentes requisitos de desempenho e segurança, o que pode tornar a integração mais difícil. A falta de padronização de interfaces abertas pode levar ao problema de fornecedor único, em que os fornecedores de equipamentos de rede têm um controle excessivo sobre a arquitetura O-RAN e, então, cobram preços mais elevados por seus produtos e serviços

[Thiruvasagam et al., 2023], além de gerar o aprisionamento (*lock in*) a seus produtos. Isso pode levar a um mercado menos competitivo e menos inovador, o que prejudica a adoção da arquitetura O-RAN e a evolução da segurança da arquitetura. Para superar esse desafio, é importante estabelecer padrões e protocolos comuns para garantir a interoperabilidade e a integração bem sucedidas entre diferentes fornecedores e tecnologias. Além disso, é importante promover a colaboração e a padronização entre diferentes fornecedores para garantir que componentes da rede possam trabalhar juntos de forma harmoniosa. É importante que as organizações de padronização trabalhem em conjunto com outras organizações, como a 3GPP, para garantir a harmonização dos padrões e a interoperabilidade entre as diferentes arquiteturas [O-RAN Alliance, 2021]. Isso é essencial para garantir que a arquitetura O-RAN possa ser integrada com outras arquiteturas de rede existentes e futuras, permitindo que as operadoras de rede possam escolher a melhor solução para suas necessidades específicas [O-RAN Alliance, 2021]. A padronização de interfaces abertas é um desafio importante para a arquitetura O-RAN, mas pode ser abordada por meio do estabelecimento de padrões abertos e acessíveis a todos os fornecedores e desenvolvedores de *software* [Thiruvasagam et al., 2023]. As organizações de padronização devem trabalhar em conjunto para garantir a harmonização dos padrões e a interoperabilidade entre as diferentes arquiteturas [Thiruvasagam et al., 2023, O-RAN Alliance, 2021]. O uso de tecnologias de código aberto também pode ser uma solução para esse desafio [O-RAN Alliance, 2021]. O uso de padrões abertos permitem a escrutinação do código e validação por uma comunidade de desenvolvedores das arquiteturas e tecnologias adotadas. Com isso, há uma mitigação de riscos à segurança e de interoperabilidade.

Privacidade e Proteção dos Dados

A arquitetura O-RAN enfrenta o desafio de garantir a privacidade do usuário e a proteção de dados sensíveis. Isso ocorre porque a arquitetura O-RAN é baseada em uma abordagem aberta e virtualizada, o que significa que diferentes componentes da rede podem ser fornecidos por diferentes fornecedores e podem ser executados em um ambiente virtualizado sobre *hardware* de propósito geral [Firoozjaei et al., 2017]. O Grupo de Trabalho 11 da O-RAN Alliance tem estudado os aspectos de segurança da arquitetura O-RAN, incluindo modelagem de ameaças, avaliação de riscos, requisitos de segurança, mecanismos e protocolos de segurança para atender aos requisitos, e testes de segurança para validação e avaliação [O-RAN Alliance, 2020]. No entanto, apenas algumas interfaces e funções de rede relacionadas à segurança foram estudadas, e há muito espaço para explorar e analisar os aspectos de segurança para várias entidades e interfaces [O-RAN Alliance, 2020]. Por exemplo, as funções de rede, como O-CU-CP, O-CU-UP, O-DU, O-RU, e as interfaces, como E2, R1, Y1, O-Cloud Notification e Cooperative Transport Interface, precisam ser estudadas em relação à segurança [Thiruvasagam et al., 2023]. Como mostrado na Figura 4.7, diferentes serviços e interfaces de rede estão sujeitos a ataques e outros tipos de vulnerabilidades. Os aspectos de segurança da infraestrutura de nuvem compartilhada, integração de nós e funções de rede, *software* de código aberto e gerenciamento seguro do ciclo de vida das funções de rede também precisam ser estudados [O-RAN Alliance, 2020]. Com isso, a virtualização e a abertura da arquitetura O-RAN podem aumentar o risco de violações de privacidade e segurança, especialmente quando se trata de dados sensíveis do usuário. Por exemplo, a implantação de uma rede O-RAN pode envolver o compartilhamento de recursos de

processamento e armazenamento entre diferentes usuários, o que pode aumentar o risco de acesso não autorizado a dados sensíveis. Para superar esse desafio, é importante implementar medidas de segurança e privacidade robustas na arquitetura O-RAN. Isso pode incluir o uso de técnicas de criptografia para proteger dados sensíveis em trânsito e em repouso, bem como o uso de técnicas de autenticação e autorização para garantir que apenas usuários autorizados possam acessar dados sensíveis. É importante implementar medidas de segurança e privacidade em todos os componentes da rede, incluindo rádios, controladores e elementos de orquestração. Isso pode incluir o uso de técnicas de *software* de segurança, como *firewalls* e detecção de intrusão, bem como o uso de técnicas de *hardware* de segurança, como módulos de segurança de *hardware*. Por fim, é importante estabelecer padrões e protocolos comuns para garantir a segurança e a privacidade em toda a arquitetura O-RAN. Isso pode incluir o desenvolvimento de padrões de segurança e privacidade para diferentes componentes da rede, bem como o desenvolvimento de protocolos de segurança e privacidade para garantir a interoperabilidade entre diferentes componentes da rede. A segurança e privacidade são desafios importantes para a arquitetura O-RAN, e é necessário continuar a estudar e desenvolver mecanismos de segurança para a arquitetura. É essencial que as organizações que implementam a arquitetura adotem melhores práticas de segurança e privacidade adequadas e implementem políticas de segurança e privacidade para garantir a proteção das informações confidenciais e o controle dos usuários sobre suas informações pessoais.

Gerenciamento de recursos e otimização de desempenho

O gerenciamento de recursos e a otimização de desempenho são desafios importantes em muitos sistemas computacionais, incluindo sistemas de rede e telecomunicações. Em sistemas de rede, como a arquitetura O-RAN, o gerenciamento de recursos refere-se à alocação e utilização eficiente de recursos de rede, como largura de banda, capacidade de processamento e armazenamento. A otimização de desempenho refere-se à melhoria do desempenho do sistema, como a redução do tempo de latência e a melhoria da qualidade de serviço [Niknam et al., 2022, Kavehmadavani et al., 2023]. Nas redes de acesso via rádio, o gerenciamento de recursos e a otimização de desempenho são desafios complexos devido à natureza distribuída e heterogênea dos sistemas. A arquitetura O-RAN, por exemplo, é composta por vários componentes que têm requisitos de recursos, segurança e desempenho diferentes, e a alocação e utilização eficiente desses recursos é essencial para garantir o desempenho adequado do sistema. Para garantir a qualidade de serviço, o desempenho e a disponibilidade, é necessário garantir que as aplicações críticas tenham latência baixa e previsível [Abdalla et al., 2022]. Isso é particularmente importante para aplicações em tempo real que exigem uma resposta rápida e confiável da rede. A latência determinística é a capacidade de garantir que um pacote de dados chegue ao seu destino dentro de um tempo previsível e consistente. Na RAN aberta, isso requer a implementação de mecanismos de controle de latência em toda a rede, incluindo a RAN, a rede de transporte e a rede de núcleo [Abdalla et al., 2022, O-RAN Alliance, 2021]. Para garantir a latência determinística, é necessário minimizar a variação da latência em toda a rede. Isso pode ser alcançado por meio de técnicas como a alocação de recursos de rede dedicados para aplicações críticas, a priorização de tráfego em tempo real e a implementação de mecanismos de controle de congestionamento [Abdalla et al., 2022]. Contudo, ataques de injeção de tráfego podem interferir na previsibilidade do sistema e,

portanto, são uma ameaça ao gerenciamento otimizado de recursos, pois desviam do modelo de funcionamento do sistema. Por fim, o gerenciamento de recursos e a otimização de desempenho são desafios para a segurança da RAN, pois introduzem meios de controle automatizados que podem ser subvertidos por injeção de tráfego e comportamentos anômalos da rede. Para enfrentar esses desafios, é necessário desenvolver soluções adaptáveis, escaláveis e eficientes que possam lidar com a natureza distribuída e heterogênea dos sistemas e com as mudanças dinâmicas nas demandas de recursos e desempenho.

4.5.2. Tendências de Pesquisa

Tendências atuais de pesquisa focada em segurança das arquiteturas de RAN aberta incluem o desenvolvimento de novas técnicas de transporte (*fronthaul*) para atender aos requisitos de ultra-redução de latência e comunicação confiável (uRLLC)e aprimorar a virtualização da infraestrutura para fornecer serviços mais avançados e ágeis aos usuários finais. Continuar a explorar soluções de segurança para garantir a privacidade do usuário e a proteção de dados sensíveis na arquitetura O-RAN também despontam como tendências de pesquisa [Niknam et al., 2022, Wang et al., 2020a].

Novas Técnicas para a Rede de Transporte (*Fronthaul*)

Fronthaul é a conexão entre a estação base e o processador de sinalização, que é responsável por processar os sinais de rádio, sendo crítica para a qualidade de serviço, pois o transporte do sinal deve ser feito com baixa latência e alta confiabilidade.No entanto, a *fronthaul* baseada em *Common Public Radio Interface* (CPRI) tem limitações em termos de largura de banda e latência, o que pode dificultar a implantação de aplicativos uRLLC. Para superar esse desafio, é necessário desenvolver novas técnicas de transporte que possam atender aos requisitos de largura de banda e latência para aplicações uRLLC. Uma das soluções propostas é o uso de Ethernet como uma alternativa ao CPRI para a rede de transporte, por ter a capacidade de atender aos requisitos de largura de banda e latência para aplicações uRLLC. No entanto, a rede de transporte baseada em Ethernet também apresenta desafios, como a necessidade de garantir a qualidade do serviço e a segurança dos dados. Portanto, é necessário desenvolver novas técnicas de gerenciamento e orquestração para garantir que o transporte baseado em Ethernet possa atender aos requisitos de largura de banda e latência para aplicativos uRLLC, mas também solucionar desafios clássicos do Ethernet em prover qualidade de serviço e segurança aos dados.

Aprimoramento da Virtualização

Aprimorar a virtualização da infraestrutura contribui para fornecer serviços mais avançados e ágeis aos usuários finais na arquitetura O-RAN [Niknam et al., 2022, Singh e Khoa Nguyen, 2022]. Para aprimorar a virtualização da infraestrutura na arquitetura O-RAN, é necessário desenvolver novas técnicas e tecnologias para virtualizar a infraestrutura de forma eficiente e eficaz, capazes de abarcar o uso de tecnologias de NFV. O desenvolvimento de mecanismos para aprimorar o desempenho e a segurança da virtualização de redes é uma tendência de pesquisa atual. Kawahara *et al.* propõem um método para melhorar a taxa de transferência e minimizar a sobrecarga do plano de controle em plataformas de nuvem virtualizadas. Ao enfrentar os desafios relacionados ao encapsulamento e ao roteamento de comunicação, a proposta oferece instâncias de rede virtual eficientes em centros de dados, garantindo desempenho ideal em dispositivos

padrão e em interfaces de redes virtuais [Kawahara et al., 2019]. Sadok *et al.* propõem Ensō, uma nova interface por fluxo para a ligação da interface de rede à aplicação. Ensō evita *buffers* de tamanho fixo e estrutura a comunicação como um fluxo que pode ser usado para enviar tamanhos de dados arbitrários.

Análises da Arquitetura de RAN Aberta

A possibilidade de pesquisa sobre análise da arquitetura de RAN aberta e suas principais características envolve a investigação detalhada da arquitetura O-RAN e inclui a evolução da RAN, que é a base para a arquitetura O-RAN, bem como as funções da RAN desagregadas e as interfaces entre elas. A análise da evolução da arquitetura da RAN inclui a revisão de padrões anteriores, como 3GPP, e a comparação com a arquitetura O-RAN. A revisão da arquitetura visa entender as principais diferenças entre as arquiteturas e as vantagens e desvantagens de cada uma. A análise das funções RAN desagregadas consiste na revisão das principais funções RAN, como processamento de sinalização, processamento de dados, gerenciamento de recursos de rádio e gerenciamento de mobilidade, e como essas funções podem ser desagregadas em componentes menores e independentes. Isso pode ajudar a entender como a arquitetura O-RAN pode ser mais flexível e escalável do que as arquiteturas RAN tradicionais. A análise das interfaces entre as funções da RAN desagregadas revisa as interfaces definidas pela O-RAN Alliance. O objetivo dessa área de pesquisa é entender como as funções da RAN desagregadas podem ser interconectadas de forma eficiente e eficaz.

Atividades de Padronização da O-RAN Alliance

A possibilidade de pesquisa sobre o estudo das atividades de padronização da O-RAN Alliance envolve uma análise detalhada das atividades de padronização em andamento na organização, bem como suas implicações para a indústria de telecomunicações. Essa pesquisa pode ser realizada por meio da revisão de documentos e especificações técnicas publicados pela O-RAN Alliance, que descrevem as atividades de padronização em andamento e as especificações técnicas que estão sendo desenvolvidas para promover a interoperabilidade e a implementação de RANs abertas. A pesquisa envolve a análise das atividades de padronização em andamento, como a definição de interfaces abertas e a especificação de requisitos de implementação. Paralelamente, a pesquisa sobre a revisão das iniciativas de implementação em andamento visa identificar as implicações regulatórias e de mercado da adoção dessas tecnologias e identificar as melhores práticas e lições aprendidas na implementação de tecnologias de RAN aberta.

Utilização de Aprendizado Federado

O aprendizado federado é uma técnica de aprendizado de máquina distribuída que permite que várias instância de computação de borda cooperem para treinar um modelo de aprendizado de máquina sem transferir seus dados de treinamento [Konečnỳ et al., 2016]. Essa técnica é particularmente útil em sistemas de RAN aberta, nos quais a computação de borda é distribuída em várias instâncias e a transferência de dados é limitada devido a restrições de comunicação. No contexto do problema de alocação ótima de recursos, o aprendizado federado pode ser utilizado para permitir que várias instâncias de computação de borda cooperem para treinar um modelo sem transferir dados privados de treinamento [Chen e et al., 2021, Abouaomar et al., 2022]. Isso permite que o modelo seja

treinado de forma mais eficiente e privada, pois os dados de treinamento permanecem na borda e não são transferidos para um servidor centralizado. Para implementar o aprendizado federado no contexto do problema de alocação ótima de recursos, é necessário selecionar um conjunto de nós de treinamento locais em cada iteração global de aprendizado federado. Esses nós de treinamento locais são responsáveis por treinar o modelo em seus próprios dados de treinamento e enviar as atualizações do modelo para um servidor centralizado para agregação. A seleção dos nós de treinamento locais deve ser feita de forma a maximizar a eficiência do processo de treinamento e minimizar o custo de recursos. É necessário alocar recursos de forma ótima para os nós de treinamento locais selecionados. Isso inclui a alocação de recursos de computação, armazenamento e comunicação. A alocação ótima de recursos deve levar em consideração as restrições de comunicação e as limitações de recursos de cada nuvem de borda. Dessa forma, o aprendizado federado é uma tendência de pesquisa para solucionar o problema de alocação ótima de recursos em sistemas de RAN aberta, permitindo que várias instâncias de computação de borda cooperem para treinar um modelo de aprendizado de máquina de forma eficiente e privada. A seleção ótima de nós de treinamento locais e a alocação ótima de recursos são fundamentais para o sucesso do processo de treinamento.

Estudo de Casos de Uso

Uma tendência de pesquisa em segurança em RAN aberta é o estudo de casos de uso específicos de RAN aberta em diferentes cenários, explicitando a análise de como as tecnologias de RAN aberta estão sendo implementadas em diferentes contextos. Essa tendência consiste na revisão de estudos de caso e relatórios que descrevem a implementação de tecnologias de RAN aberta em cenários como redes móveis 5G, redes de acesso fixo sem fio (*Fixed Wireless Access* – FWA), redes privadas e redes de IoT. A implementação de RAN aberta nesses cenários envolve a utilização de tecnologias de virtualização e desagregação para permitir a implementação de funções de rede em *hardware* genérico. Isso permite que as operadoras de rede móvel reduzam os custos de *hardware* e aumentem a flexibilidade e escalabilidade da rede.

4.5.3. Oportunidades de Segurança

É importante continuar a explorar soluções de segurança para garantir a privacidade do usuário e a proteção de dados sensíveis na arquitetura O-RAN porque a arquitetura O-RAN é baseada em uma abordagem aberta e virtualizada, o que pode aumentar o risco de ataques cibernéticos e violações de segurança. Para garantir a privacidade do usuário e a proteção de dados sensíveis na arquitetura O-RAN, é necessário explorar soluções de segurança que possam mitigar esses riscos. Isso pode incluir o uso de técnicas de criptografia para proteger os dados em trânsito e armazenados, bem como o uso de técnicas de autenticação e autorização para garantir que apenas usuários autorizados possam acessar os dados [Wang et al., 2020a, Wang et al., 2021]. Logo, é importante desenvolver soluções de segurança que possam detectar e responder a ameaças de segurança em tempo real. Isso inclui o uso de técnicas de detecção de intrusão e análise de comportamento para identificar atividades suspeitas na rede e o uso de técnicas de resposta a incidentes para mitigar os efeitos de um ataque cibernético ou violação de segurança [Singh e Khoa Nguyen, 2022, Kavehmadavani et al., 2023]. Ao explorar soluções de segurança para garantir a privacidade do usuário e a proteção de dados sensíveis na

arquitetura O-RAN, é possível mitigar os riscos de ataques cibernéticos e violações de segurança, o que pode melhorar a confiança dos usuários finais na rede e promover a adoção da arquitetura O-RAN. A segurança é um requisito fundamental para a implantação de serviços críticos, como serviços de saúde e serviços financeiros, que exigem um alto nível de proteção de dados sensíveis.

Como a RAN aberta é derivada de princípios de virtualização, herda alguns desafios relacionados à segurança. Esses desafios incluem autenticação e autorização de migrações de máquinas virtuais, instanciações de ambientes virtuais, segurança dos hipervisores e orquestração [Firoozjaei et al., 2017]. Embora a RAN aberta possibilite a criação de serviços flexíveis sob medida para cada usuário, é importante considerar os benefícios sob a ótica dos desafios relacionados à segurança trazidos por redes abertas virtualizadas [Niknam et al., 2022]. As principais oportunidades para aprimorar a segurança da RAN aberta são listadas a seguir [NIS Cooperation Group, 2022]:

- **Diversidade de Fornecedores na RAN**. A Open RAN possibilita o surgimento e uso de mais fornecedores na RAN juntamente com uma RAN desagregada, interfaces interoperáveis e o aumento do uso de *hardware* de código aberto e comercial (COTS). Assim, é possível reduzir os riscos relacionados à dependência de um único fornecedor. Contudo, ainda há o risco de centralização do mercado em torno de um número reduzido de fornecedores, integradores de sistemas e provedores nuvem, indo contra a diversificação;

- **Visibilidade e Auditoria**. O uso de padrões abertos para as interfaces entre componentes da RAN implica que componentes diferentes fornecedores se conectam de maneira semelhante, melhorando a visibilidade e a transparência. Quanto à auditoria, o uso de interfaces de padrão aberto torna mais fácil para auditores de segurança entenderem como uma determinada implementação de RAN está funcionando e se está funcionando corretamente. O aumento do uso de código aberto na RAN aberta tende a permitir uma maior visibilidade e transparência sobre como os componentes funcionam internamente. Contudo, o código aberto não é uma garantia de melhor segurança, pois também pode conter vulnerabilidades;

- **Interoperabilidade**. Para manter a estabilidade e confiabilidade em uma RAN aberta, produtos de diferentes operadoras devem interoperar. Para isso, estratégias de mitigação de risco devem ser aplicadas em caso de conflitos [Niknam et al., 2022]. É crucial identificar os riscos das incompatibilidades entre produtos de rádio e controle de diferentes provedores de serviço;

- **Desempenho**. Um desafio relacionado ao desempenho decorre da virtualização das RANs abertas. Diferentes funções de rede e módulos podem ser migrados dinamicamente de uma infraestrutura para outra. Porém, prever congestionamentos ou falhas iminentes se torna uma tarefa complexa, especialmente em sistemas RAN dinâmicos e escaláveis [Thiruvasagam et al., 2023];

- **Inteligência Artificial**. A iniciativa do O-RAN Alliance prioriza o uso de RICs para operar e manter o desenvolvimento de redes escaláveis e altamente dependentes de modelos de inteligência artificial e aprendizado de máquina

[Thiruvasagam et al., 2023]. Esses modelos são usados para realizar análise de dados e entregar resultados em quase-tempo real. O desafio técnico é garantir que a acurácia e outras métricas de desempenho dos modelos estejam em um patamar aceitável do ponto de vista de garantir a qualidade dos serviços. Caso contrário, os modelos de inteligência artificial se tornam altamente danoso para a rede se não forem capazes de desempenhar dentro dos limites aceitáveis. Técnicas de aprendizado profundo (*deep learning*) também são tendências para o treinamento de modelos em não-tempo real para funcionalidades da RAN, mas com o compartilhamento dos modelos em tempo próximo ao tempo real. Porém, certos modelos são considerados modelos de caixa-preta, logo, torna-se difícil entender como as operações ocorrem neles e como as decisões e ações são tomadas [Fiandrino et al., 2022]. A automação consolidada por modelos de inteligência artificial pode trazer riscos adicionais de segurança, responsabilidade e disponibilidade, e as operadoras de rede podem perder o controle sobre processos críticos. A falta de transparência nos modelos pode levar a vulnerabilidade a ataques. Para oferecer maior segurança aos serviços, os modelos de inteligência artificial devem ser explicáveis, robustos a ataques adversariais e verificáveis.

- **Confiança Distribuída e *Blockchain***: A segurança atual da RAN aberta depende de soluções de criptografia e autenticação baseadas em Infraestrutura de Chave Pública (*Public Key Infraestructure* – PKI) de adesão voluntária, transferindo a confiança para uma Autoridade de Certificação (AC) centralizada como parte confiável. Isso faz com que a rede falhe catastroficamente caso ocorra uma falha de comunicação com a AC ou ocorra um ataque que comprometa o seu funcionamento. Para superar essa vulnerabilidade, segurança e autenticação garantidos por cadeia de blocos (*blockchain*) se tornam atrativos para o desenvolvimento da rede [Giupponi e Wilhelmi, 2022]. Novas arquiteturas estão sendo desenvolvidas nesse sentido, como a BE-RAN, da O-RAN Alliance [Xu et al., 2021a]. Estudos futuros são necessários para compreender o impacto dessa abordagem nas interfaces de controle, usuário e no plano de sincronização.

4.6. Considerações Finais

As redes de acesso via rádio abertas (*Open RAN*) introduzem interfaces abertas e viabilizam a desagregação de componentes, o que suscita considerações de segurança, abrangendo tanto as interfaces abertas quanto a adoção de modelos de inteligência artificial para a automação do gerenciamento e orquestração da rede. A implementação das interfaces abertas promove maior transparência e facilita a adoção de padrões de segurança. Paralelamente, a desagregação dos componentes permite que atualizações de segurança e novas funções possam ser implementadas de forma eficiente em componentes de *software* individuais. Modelos de inteligência artificial asseguram o gerenciamento e a orquestração da rede autônomos através de laços fechados de controle e gerenciamento. Entretanto, implantações da *Open RAN* implicam novos desafios de segurança para operadoras de redes móveis (*Mobile Network Operators* – MNOs). Um ecossistema aberto e multi-fornecedor demanda um foco específico no aumento da superfície de ataque nas interfaces entre tecnologias integradas. Além das considerações de segurança relacionadas

à integração de componentes provenientes de diversos fornecedores, as operadoras de serviços também enfrentarão desafios referentes ao uso de *software* de código-fonte aberto e à implementação de novas funções da rede 5G, bem como interfaces cujos padrões ainda estão em desenvolvimento. As MNOs devem, então, lidar com questões de segurança que abarcam, mas não se restringem, à *Open RAN*, tais como infraestrutura de nuvem, ataques à virtualização/conteinerização e ataques de negação de serviço distribuídos.

Para enfrentar esses desafios, a arquitetura de referência O-RAN enfatiza a adoção de melhores práticas de segurança. A proteção das interfaces de gerenciamento engloba a utilização de protocolos criptográficos, cifras robustas, autenticação mútua, rigorosos controles de acesso e registros detalhados. A separação entre O-DU e O-RU exige uma compreensão ampla das possíveis ameaças para desenvolver controles de segurança eficazes. A integração de microsserviços em controladores inteligentes da RAN requer uma arquitetura de segurança sólida, que garanta análises em tempo real e potencialize as capacidades de segurança e gerenciamento. A adoção da arquitetura de confiança zero (*Zero-Trust Architecture* – ZTA) enfatiza a proteção de recursos e a avaliação contínua de dispositivos e usuários, aumentando a segurança ao eliminar a confiança implícita. A adoção da ZTA na O-RAN visa reduzir os riscos associados à ampliada superfície de ataque, mantendo a arquitetura da RAN segura e aberta.

É importante ressaltar que a arquitetura O-RAN negligencia o conceito de "segurança/privacidade por *design*/padrão" [Köpsell et al., 2022], o que resulta em um sistema que apresenta vários riscos de segurança. Soluções de segurança tradicionais conseguem mitigar os riscos das redes de acesso via rádio abertas e podem ser implementadas sem grande esforço, e com baixo investimento de capital, combatendo de forma eficaz as ameaças individuais. No entanto, para reduzir riscos de segurança específicos, como os relacionados às soluções de inteligência artificial, são necessários esforços para adaptar as especificações e implementar as salvaguardas de segurança correspondentes.

As RANs abertas e, particularmente, a arquitetura de referência O-RAN, combinam a abertura e a desagregação com sólidas práticas de segurança. Esse capítulo abordou os desafios de segurança intrínsecos às RANs e discutiu as considerações decorrentes da natureza aberta e desagregada da rede. Mediante a aderência aos padrões da indústria, à arquitetura *Zero-Trust* e outros requisitos de segurança, o capítulo demonstrou que a RAN aberta busca proporcionar um ambiente seguro, aproveitando os benefícios das interfaces abertas e da maior flexibilidade. Por fim, o capítulo elencou desafios em aberto e oportunidades de pesquisa para o desenvolvimento de soluções de segurança adaptadas à nova geração de redes de acesso via rádio com interfaces abertas e componentes desagregados, executando código aberto em *hardware* de propósito geral.

Agradecimentos

Este capítulo foi realizado com recursos do CNPq, FAPERJ e RNP. Além disso, o presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Referências

[Abdalla e Marojevic, 2023] Abdalla, A. S. e Marojevic, V. (2023). End-to-end O-RAN security architecture, threat surface, coverage, and the case of the open fronthaul. *arXiv preprint arXiv:2304.05513*.

[Abdalla et al., 2022] Abdalla, A. S., Upadhyaya, P. S., Shah, V. K. e Marojevic, V. (2022). Toward next generation open radio access networks: What O-RAN can and cannot do! *IEEE Network*, 36(6):206–213.

[Abouaomar et al., 2022] Abouaomar, A., Taik, A., Filali, A. e Cherkaoui, S. (2022). Federated learning for RAN slicing in beyond 5G networks. *arXiv preprint arXiv:2206.11328*.

[Adesina et al., 2023] Adesina, D., Hsieh, C.-C., Sagduyu, Y. E. e Qian, L. (2023). Adversarial machine learning in wireless communications using RF data: A review. *IEEE Communications Surveys & Tutorials*, 25(1):77–100.

[Arnaz et al., 2022] Arnaz, A., Lipman, J., Abolhasan, M. e Hiltunen, M. (2022). Toward Integrating Intelligence and Programmability in Open Radio Access Networks: A Comprehensive Survey. *IEEE Access*, 10:67747–67770.

[Azariah et al., 2022] Azariah, W., Bimo, F. A., Lin, C.-W., Cheng, R.-G., Jana, R. e Nikaein, N. (2022). A survey on open radio access networks: Challenges, research directions, and open source approaches. *arXiv preprint arXiv:2208.09125*.

[Brik et al., 2022] Brik, B., Boutiba, K. e Ksentini, A. (2022). Deep Learning for B5G Open Radio Access Network: Evolution, Survey, Case Studies, and Challenges. *IEEE Open Journal of the Communications Society*, 3:228–250.

[Chen e et al., 2021] Chen, M. e et al. (2021). A joint learning and communications framework for federated learning over wireless networks. *IEEE Transactions on Wireless Communications*, 20(1):269–283.

[Couto et al., 2023a] Couto, R. S., Cruz, P., Campista, M. E. M. e Costa, L. H. M. K. (2023a). Using public datasets to train O-RAN deep learning models. Em *2st International Conference on 6G Networking (6GNet)*, p. 1–8. Artigo aceito para publicação (convidado).

[Couto et al., 2023b] Couto, R. S., Mattos, D. M. F., Moraes, I. M., Cruz, P., Medeiros, D. S. V., Souza, L. A. C., Táparo, F. G., Campista, M. E. M. e Costa, L. H. M. K. (2023b). Gerenciamento e orquestração de serviços em O-RAN: Inteligência, tendências e desafios. Em *Minicursos do XLI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2023)*, p. 1–52.

[Das et al., 2017] Das, S. K., Chowdhury, S. S. e Das, S. K. (2017). A survey on resource allocation in cloud computing: Issues and challenges. *IEEE Transactions on Cloud Computing*, 5(2):358–378.

[Davaslioglu e Sagduyu, 2019] Davaslioglu, K. e Sagduyu, Y. E. (2019). Trojan attacks on wireless signal classification with adversarial machine learning. Em *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, p. 1–6.

[de Oliveira et al., 2023] de Oliveira, N. R., Moraes, I. M., Medeiros, D. S. V., Andreoni, M. e Mattos, D. M. F. (2023). An agile conflict-solving framework for intent-based management of service level agreement. Em *2st International Conference on 6G Networking (6GNet)*, p. 1–8. Artigo aceito para publicação (convidado).

[Dik e Berger, 2023] Dik, D. e Berger, M. S. (2023). Open-RAN fronthaul transport security architecture and implementation. *IEEE Access*, 11:46185–46203.

[Fiandrino et al., 2022] Fiandrino, C., Attanasio, G., Fiore, M. e Widmer, J. (2022). Toward native explainable and robust AI in 6G networks: Current state, challenges and road ahead. *Computer Communications*, 193:47–52.

[Firoozjaei et al., 2017] Firoozjaei, M. D., Jeong, J. P., Ko, H. e Kim, H. (2017). Security challenges with network functions virtualization. *Future Generation Computer Systems*, 67:315–324.

[Giupponi e Wilhelmi, 2022] Giupponi, L. e Wilhelmi, F. (2022). Blockchain-enabled network sharing for O-RAN in 5G and beyond. *Netwrk. Mag. of Global Internetwkg.*, 36(4):218–225.

[Groen et al., 2023] Groen, J., Doro, S., Demir, U., Bonati, L., Polese, M., Melodia, T. e Chowdhury, K. (2023). Implementing and Evaluating Security in O-RAN: Interfaces, Intelligence, and Platforms. *arXiv preprint arXiv:2304.11125*.

[Habler et al., 2022] Habler, E., Bitton, R., Avraham, D., Klevansky, E., Mimran, D., Brodt, O., Lehmann, H., Elovici, Y. e Shabtai, A. (2022). Adversarial machine learning threat analysis in open radio access networks. *arXiv preprint arXiv:2201.06093*.

[Ilyas et al., 2018] Ilyas, A., Engstrom, L., Athalye, A. e Lin, J. (2018). Black-box adversarial attacks with limited queries and information. Em *International conference on machine learning*, p. 2137–2146. PMLR.

[Karunaratne et al., 2021] Karunaratne, S., Krijestorac, E. e Cabric, D. (2021). Penetrating RF fingerprinting-based authentication with a generative adversarial attack. Em *ICC 2021-IEEE International Conference on Communications*, p. 1–6. IEEE.

[Kavehmadavani et al., 2023] Kavehmadavani, F., Nguyen, V.-D., Vu, T. X. e Chatzinotas, S. (2023). Intelligent traffic steering in beyond 5G Open RAN based on LSTM traffic prediction. *IEEE Transactions on Wireless Communications*.

[Kawahara et al., 2019] Kawahara, H., Yamamoto, R., Ohzahata, S. e Kato, T. (2019). Throughput enhancement with overlay network virtualization using commodity devices. Em *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, UCC '19 Companion, p. 147–148, New York, NY, USA. Association for Computing Machinery.

[Konečnỳ et al., 2016] Konečnỳ, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. e Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.

[Köpsell et al., 2022] Köpsell, S., Ruzhanskiy, A., Hecker, A., Stachorra, D. e Franchi, N. (2022). Open RAN risk analysis. Relatório técnico, Federal Office for Information Security (German). Disponível em https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=5, acessado em 20 de agosto de 2023.

[Liyanage et al., 2023] Liyanage, M., Braeken, A., Shahabuddin, S. e Ranaweera, P. (2023). Open RAN Security: Challenges and Opportunities. *Journal of Network and Computer Applications*, 214:103621.

[Lopez et al., 2022] Lopez, M. A., Barbosa, G. N. N. e Mattos, D. M. F. (2022). New Barriers on 6G Networking: An Exploratory Study on the Security, Privacy and Opportunities for Aerial Networks. Em *International Conference on 6G Networking (6GNet)*, p. 1–6.

[McGraw et al., 2020] McGraw, G., Figueroa, H., Shepardson, V. e Bonett, R. (2020). An Architectural Risk Analysis of Machine Learning Systems: Toward More Secure Machine Learning. Relatório técnico, Berryville Institute of Machine Learning.

[Niknam et al., 2022] Niknam, S., Roy, A., Dhillon, H. S., Singh, S., Banerji, R., Reed, J. H., Saxena, N. e Yoon, S. (2022). Intelligent O-RAN for beyond 5G and 6G wireless networks. Em *2022 IEEE Globecom Workshops (GC Wkshps)*, p. 215–220. IEEE.

[NIS Cooperation Group, 2022] NIS Cooperation Group (2022). Report on the cybersecurity of Open RAN. Relatório técnico, European Union. Disponível em https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks, acessado em 20 de agosto de 2023.

[O-RAN Alliance, 2020] O-RAN Alliance (2020). External open source projects. https://www.o-ran.org/resources/external-open-source-projects.

[O-RAN Alliance, 2021] O-RAN Alliance (2021). O-RAN architecture. https://www.o-ran.org/technical-specifications.

[O-RAN Working Group 1, 2023] O-RAN Working Group 1 (2023). O-RAN architecture description 9.0. Especificação Técnica v09.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 10, 2023] O-RAN Working Group 10 (2023). O-RAN operations and maintenance interface specification. Especificação Técnica v10.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 11, 2023a] O-RAN Working Group 11 (2023a). O-ran.wg11.threat-model.o-r003-v06.00. Especificação técnica, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications, Acessado em 15 de agosto de 2023.

[O-RAN Working Group 11, 2023b] O-RAN Working Group 11 (2023b). Security protocols specifications. Relatório Técnico v06.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 11, 2023c] O-RAN Working Group 11 (2023c). Security requirements specifications. Especificação Técnica v06.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 2, 2021] O-RAN Working Group 2 (2021). Non-RT RIC: Functional Architecture. Relatório Técnico v01.01, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 2, 2023] O-RAN Working Group 2 (2023). Non-RT RIC architecture. Especificação Técnica v03.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 3, 2023a] O-RAN Working Group 3 (2023a). Near-rt ric architecture. Especificação Técnica v04.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 3, 2023b] O-RAN Working Group 3 (2023b). O-RAN e2 service model (e2sm). Especificação Técnica v03.01, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[O-RAN Working Group 6, 2023] O-RAN Working Group 6 (2023). O2 Interface General Aspects and Principles. Especificação Técnica v04.00, O-RAN Alliance. Disponível em https://orandownloadsweb.azurewebsites.net/specifications.

[Open RAN Policy Coalition, 2021] Open RAN Policy Coalition (2021). Open RAN security in 5G. Relatório técnico, Open RAN Policy Coalition. Disponível em https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf.

[Polese et al., 2023] Polese, M., Bonati, L., D'Oro, S., Basagni, S. e Melodia, T. (2023). Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges. *IEEE Communications Surveys & Tutorials*, 25(2):1376–1411.

[Ramezanpour e Jagannath, 2022] Ramezanpour, K. e Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, 217:109358.

[Ranaweera et al., 2021] Ranaweera, P., Jurcut, A. D. e Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. *IEEE Communications Surveys & Tutorials*, 23(2):1078–1124.

[Research e Markets, 2022] Research e Markets (2022). 5G Radio Access Network Market Size, Share & Trends Analysis Report By Component (Hardware, Software, Services), By Architecture Type, By Deployment, By End-user, By Region, And Segment Forecasts, 2022 - 2030. Relatório técnico. Disponível em `https://www.researchandmarkets.com/reports/5702152`.

[Restuccia et al., 2020] Restuccia, F., D'Oro, S., Al-Shawabka, A., Rendon, B. C., Chowdhury, K., Ioannidis, S. e Melodia, T. (2020). Generalized wireless adversarial deep learning. Em *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*, p. 49–54.

[Rose et al., 2020] Rose, S., Borchert, O., Mitchell, S. e Connelly, S. (2020). Zero trust architecture. Relatório Técnico NIST Special Publication 800-207, National Institute of Standards and Technology - U.S. Department of Commerce. Disponível em `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf`.

[Shi e Sagduyu, 2021] Shi, Y. e Sagduyu, Y. E. (2021). Adversarial machine learning for flooding attacks on 5G radio access network slicing. Em *IEEE International Conference on Communications Workshops (ICC Workshops)*, p. 1–6.

[Shi e Sagduyu, 2023] Shi, Y. e Sagduyu, Y. E. (2023). Membership inference attack and defense for wireless signal classifiers with deep learning. *IEEE Transactions on Mobile Computing*, 22(7):4032–4043.

[Singh e Khoa Nguyen, 2022] Singh, A. K. e Khoa Nguyen, K. (2022). Joint selection of local trainers and resource allocation for federated learning in Open RAN intelligent controllers. Em *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, p. 1874–1879.

[Soltani et al., 2023] Soltani, S., Shojafar, M., Brighente, A., Conti, M. e Tafazolli, R. (2023). Poisoning Bearer Context Migration in O-RAN 5G Network. *IEEE Wireless Communications Letters*, 12(3):401–405.

[Sun et al., 2022] Sun, G., Cong, Y., Dong, J., Wang, Q., Lyu, L. e Liu, J. (2022). Data poisoning attacks on federated machine learning. *IEEE Internet of Things Journal*, 9(13):11365–11375.

[Thiruvasagam et al., 2023] Thiruvasagam, P. K., Venkataram, V., Ilangovan, V. R., Perapalla, M., Payyanur, R., Kumar, V. et al. (2023). Open RAN: Evolution of architecture, deployment aspects, and future directions. *arXiv preprint arXiv:2301.06713*.

[Usama et al., 2019] Usama, M., Qayyum, A., Qadir, J. e Al-Fuqaha, A. (2019). Black-box adversarial machine learning attack on network traffic classification. Em *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, p. 84–89. IEEE.

[Wang et al., 2020a] Wang, C.-X., Di Renzo, M., Stanczak, S., Wang, S. e Larsson, E. G. (2020a). Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges. *IEEE Wireless Communications*, 27(1):16–23.

[Wang et al., 2020b] Wang, F., Zhong, C., Gursoy, M. C. e Velipasalar, S. (2020b). Defense strategies against adversarial jamming attacks via deep reinforcement learning. Em *2020 54th annual conference on information sciences and systems (CISS)*, p. 1–6. IEEE.

[Wang et al., 2021] Wang, T.-H., Chen, Y.-C., Huang, S.-J., Hsu, K.-S. e Hu, C.-H. (2021). Design of a network management system for 5G Open RAN. Em *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, p. 138–141.

[Xu et al., 2021a] Xu, H., Zhang, L., Sun, Y. e I, C.-L. (2021a). BE-RAN: blockchain-enabled Open RAN with decentralized identity management and privacy-preserving communication. *arXiv preprint arXiv:2101.10856*.

[Xu et al., 2021b] Xu, X., Zhang, Y., Li, X., Zhang, Y. e Zhang, H. (2021b). Open RAN: Challenges and opportunities. *IEEE Communications Magazine*, 59(4):34–39.