Mitigação Inteligente de Ataques DDoS em Redes O-RAN Utilizando Aprendizado de Máquina

Victor Dias[1], Murilo Silva[1], Matheus Gomes[1], Lucas B. Oliveira[1,2], André Riker[1], Antônio Abelém[1]

[1] Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Universidade Federal do Pará (UFPA) – Belém – PA – Brasil

[2]Rede Nacional de Ensino e Pesquisa (RNP) – Rio de Janeiro – RJ – Brasil

{murilosilva,matheus.cordovil,lucas.borges}@itec.ufpa.br

victor.leite@ig.ufpa.br,abelem@ufpa.br,ariker@ufpa.br

Abstract. *The transition of mobile networks to 5G has stimulated the adoption of technologies such as NFVs, SDN, slices, and open and interoperable standards like Open RAN (O-RAN). Regarding security, O-RAN networks are in the early stages of ensuring integrity and reliability. In this context, this work proposes the SID-xApp (Slice Intelligent Defender xApp), an application integrated with the near real-time network controller (Near-RT RIC), aiming to identify and mitigate DDoS attacks that may compromise the slices present in the O-RAN. The proposed solution is designed to enalbe modular development and to support metrics from devices connected to the network, identify patterns through machine learning models (ML), and dissociate malicious users, providing a layer of security to the O-RAN's open fronthaul.*

Resumo. *A transição das redes móveis para o 5G estimulou a adoção de tecnologias como NFVs, SDN, slices e de padrões abertos e interoperáveis como o Open RAN (O-RAN). Em relação à segurança, as redes O-RAN se encontram nos estágios iniciais para garantir a integridade e confiabilidade. Diante deste cenário, este trabalho propõe o SID-xApp (Slice Intelligent Defender xApp), uma aplicação integrada ao controlador de quase tempo real da rede (Near-RT RIC), com o objetivo de identificar e mitigar ataques DDoS que possam comprometer os slices presentes na O-RAN. A solução proposta é projetada para permitir o desenvolvimento de forma modular e suportar o recebimento de métricas dos dispositivos conectados à rede, identificar padrões por meio de modelos de aprendizado de máquina (AM) e desassociar usuários mal-intencionados, proporcionando uma camada de segurança ao open fronthaul da O-RAN.*

1. Introdução

A evolução das redes móveis tem sido marcada por avanços significativos, culminando na quinta geração de redes móveis (5G), que por sua vez adotou tecnologias existentes, como Virtualização das Funções de Rede (NFV) e Redes Definidas por Software (SDN). Com o aumento do poder de programabilidade na rede, um novo paradigma surgiu, conhecido como Open RAN [Marinova and Leon-Garcia 2024]. Esta abordagem inovadora permite a interoperabilidade de hardware e software de diferentes fornecedores, isto reduz a dependência de fornecedores, como também, proporciona maior espaço para inovação. No

entanto, apesar das vantagens em redução de custos e melhoria na experiência do usuário, questões de segurança permanecem uma preocupação crítica nesse cenário em constante evolução [Polese et al. 2023].

A O-RAN traz o *open fronthaul* como um dos pontos de diferenciação em relação à RAN tradicional. Ele apresenta novos componentes e interfaces padronizadas pela O-RAN Alliance, como as Unidades Distribuídas Abertas (O-DUs), as Unidades Centralizadas Abertas (O-CUs) e os Controladores Inteligentes da RAN (RIC), que são divididos em Non-RT RIC (não opera em tempo real) e Near-RT RIC (opera próximo do tempo real), responsáveis por desempenhar um papel crucial na gestão e otimização da rede por meio de aplicações.

A presença desses componentes e interfaces abertos ainda carece de uma padronização com base nas melhores práticas da indústria, como processos de autenticação e autorização, proteção contra ataques, entre outros. Entre diversos ataques, o de negação de serviço (DoS) ou negação de serviço distribuídas (DDoS) em O-RAN [Liyanage et al. 2022], é particularmente crítico, pois além do impacto nos componentes do *open fronthaul*, esses ataques são danosos também para infraestruturas sensíveis que são gerenciadas por eles como é o caso dos *slices*, que necessitam de uma qualidade de serviço (QoS) específica para cada tipo de aplicação aos quais estejam atribuídos.

Com isso, pesquisa e desenvolvimento de soluções são essenciais para identificar e mitigar de forma rápida e eficiente essas vulnerabilidades na arquitetura O-RAN. Esta arquitetura oferece diversas possibilidades e recursos que podem ser aproveitados para lidar com essas ameaças, como as xApps (*eXtended Applications*) são aplicações acopladas ao controlador Near-RT RIC que surgem como uma solução promissora para fortalecer a segurança em ambientes Open RAN [Hoffmann et al. 2024] e podem se beneficiar do uso de modelos de Aprendizado de Máquina (AM) ou Inteligência Artificial (IA) robustos para detectar padrões maliciosos, possibilitando assim uma melhor resposta.

Desse modo, o objetivo desse trabalho é desenvolver uma solução para detectar e mitigar ataques DDoS em redes O-RAN, com foco na QoS dos *slices* por meio de uma xApp. Será desenvolvida uma aplicação que utilize inteligência computacional acoplada ao Near-RT RIC, a qual contará com 3 módulos responsáveis por receber métricas dos equipamentos dos usuários (UEs), para determinar seu comportamento e com base nessa classificação desassociar usuários maliciosos. Para validar a proposta, serão utilizados ambientes de testes que estejam de acordo com a arquitetura O-RAN. O trabalho está organizado da seguinte forma: primeiro serão apresentados os conceitos teóricos principais na Seção 2, na Seção 3 serão discutidos os trabalhos que estão sendo utilizados como comparativo que contribuíram para o desenvolvimento da proposta. Por fim, a Seção 4 irá descrever a metologia de implementação do projeto e os resultados esperados serão debatidos na Seção 5.

2. Referencial Teórico

No que se diz respeito à segurança em O-RAN, muitos conceitos são necessários para seu pleno entendimento. Desse modo, nessa seção serão abordados os temas mais relevantes para compreensão da solução proposta.

2.1. Redes O-RAN

O Conceito de O-RAN traz consigo a desagregação de hardware e software, possibilitando a incorporação de múltiplos fornecedores e a transição para tecnologias baseadas em nuvem. Essa abordagem amplia a flexibilidade, interoperabilidade e fomenta a inovação nas redes de nova geração. Nesse contexto, esse paradigma só é possível com uma arquitetura que possibilite tais inovações. Desse modo, organizações como a O-RAN Alliance e 3GPP (3rd Generation Partnership Project) trabalham em sua padronização.

A arquitetura O-RAN conta com os principais componentes e interfaces ilustrados na Figura 1. Primeiramente, tem-se o SMO (Gerenciamento e Orquestração de Serviços), o qual é um *framework* utilizado para o gerenciamento do domínio da RAN. Dentro do SMO está contido o Non-RT RIC, responsável por otimizar a RAN através da interface A1, utilizando modelos de ML e IA para treinamento e atualizações, além de orientações baseadas em políticas de aplicativos e recursos no Near-RT RIC, em um *loop* com intervalos maiores que 1 segundo.

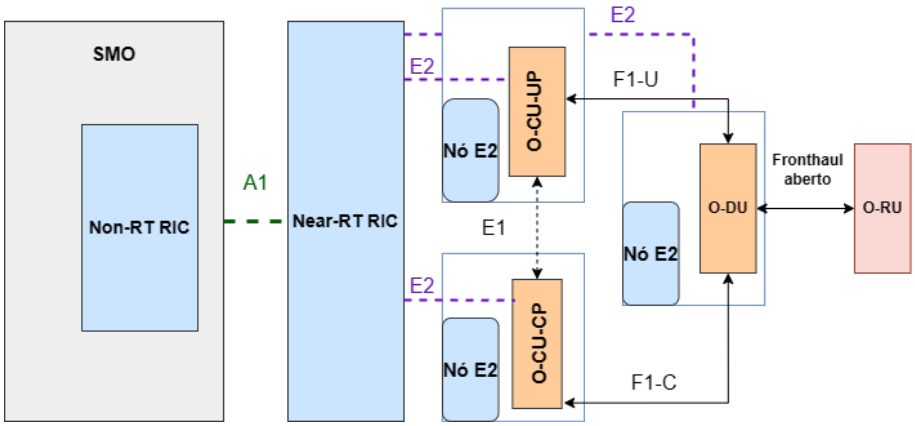

Figura 1. Arquitetura O-RAN (Adaptada [Marinova and Leon-Garcia 2024]).

Por sua vez, o Near-RT RIC é uma função de rede O-RAN que gerencia os recursos da RAN via interface E2, com um tempo de resposta entre 10 ms e 1 segundo, permitindo o uso de xApps para diversas funções. Também, há na arquitetura O-RAN uma série de nós lógicos, sendo eles: O-DU, abriga as camadas RLC/MAC/High-PHY; O-RU, hospeda a camada Low-PHY e o processamento de RF. Por fim, o nó E2 que se comunica com a interface E2, podendo ser utilizado pelos nós lógicos previamente citados.

Outros componentes fundamentais na arquitetura que permitem a comunicação e gerenciamento de seus componentes são as interfaces. A interface A1 tem a função de intermediar a comunicação entre Non e Near-RT RIC para a implantação de configurações e políticas de otimização. Já a interface O1 trabalha junto ao SMO para gerenciar as funções de rede O-RAN. A interface E2 conecta os diferentes elementos da RAN, como O-CU-CPs/UPs, O-DUs e com o Near-RT RIC, permitindo o controle dos procedimentos e funcionalidades desses nós.

Por fim, outra ferramenta importante presente nessa arquitetura são as aplicações nativas do Near-RT RIC, conhecidas como xApps. Elas são microsserviços que definem

os recursos a serem consumidos e providos no momento de sua integração. São aplicações independentes no sentido de que podem ser provisionadas por diferentes indivíduos para diferentes funções. A E2 permite a associação direta entre a aplicação e as funcionalidades da RAN. Em síntese, as xApps trazem espaço para a inovação dentro do ambiente.

2.2. Fatiamento de rede

Uma das tecnologias centrais da O-RAN é a adaptação do conceito de *network slicing*, ou fatiamento de rede, presente no 5G, no qual a infraestrutura de rede é dividida em várias fatias lógicas, cada uma dedicada a fornecer serviços específicos, compartilhando uma estrutura física comum. Ou seja, tem-se a divisão da rede física em múltiplas redes virtuais com suporte aos diferentes tipos de serviço da RAN [O-RAN Alliance 2024].

Essa abordagem desempenha um papel fundamental, pois cada serviço possui requisitos específicos de desempenho e funcionalidade, sendo assim necessária a disponibilidade de fatias especializadas para atender para diferentes casos. A exemplo, as aplicações de URLLC priorizam a mínima latência para operações críticas em tempo real como exemplo carros autônomos. As fatias eMBB são vitais para oferecer experiências de alta velocidade e qualidade em *streaming* de mídia e jogos online. Por fim, a mMTC é essencial para suportar o grande número de dispositivos conectados na Internet das Coisas (IoT), presentes em cenários como cidades inteligentes. Desse modo, é correto afirmar que os *slices* têm papel crucial em um ambiente O-RAN [Donatti et al. 2024], e ataques podem influenciar e degradar seu funcionamento, como será discutido na Seção 3.

2.3. Segurança

Como mencionado anteriormente, a rede O-RAN é a união de diversas tecnologias para permitir um padrão aberto e desagregado. Com isso, muitas tecnologias, RAN, 5G, *cloud*, entre outras, estão presentes na sua concepção, essa características por si só, além dos benefícios, traz seus desafios, e em um ambiente cada vez mais complexo, a segurança está entre as principais preocupações da comunidade, pois isso cria uma superfície de ataque extensa [Polese et al. 2023].

Desse modo, é possível dividir em 3 áreas (Processo, Tecnologia e Global) de pesquisa os problemas de segurança encontrados, possibilitando assim um melhor entendimento de qual área o trabalho se encaixa [Liyanage et al. 2022]. As duas que não estão no escopo do projeto são relativas às ameaças relacionadas à supervisão, padronização, regras, boas práticas e a ataques envolvendo riscos globais como espionagem.

Esta proposta utiliza como base os ataques presentes na área de tecnologia da arquitetura O-RAN, sendo a maior entre as 3, por considerar as diferentes tecnologias que compõem a O-RAN (software aberto, interface aberta, inteligência, virtualização). Entre os ataques presentes, ganham destaque os ataques de DoS/DDoS, pois podem comprometer diretamente componentes vitais da rede, com os do *open fronthaul* e consequentemente influenciar na degradação da QoS para serviços críticos, como procedimentos de operações remotas e direção de carros autônomos, que por utilizarem os *slices* do tipo URLLC, demandam alta confiabilidade e tempo de resposta reduzido.

3. Trabalhos relacionados

O cenário de segurança em O-RAN ainda é recente, portanto, trabalhos como [Polese et al. 2023] e [Liyanage et al. 2022] são fundamentais, possibilitando um ponto

de partida dos principais desafios já encontrados. Em [Polese et al. 2023] é realizado um apanhado geral sobre o O-RAN, sua arquitetura, desafios e possibilidades de pesquisa. Já [Liyanage et al. 2022] aprofunda mais a discussão, dividindo em diversas áreas técnicas e possíveis soluções. Ambos os trabalhos servem como motivação de pesquisa, trazendo para discussão ataques DDoS envolvendo as interfaces do *open fronthaul* O-DU/CU e RIC.

O trabalho de [Samarakoon et al. 2022] usa uma rede 5G para criação de um banco de dados que contenha ataques como *scan* de portas e DoS. Após a criação do banco de dados, ele foi submetido a diferentes modelos de AM dos quais o que obteve a maior acurácia foi uma rede neural MLP (*Multi Layer Perceptron*). O trabalho [Khan et al. 2022] utiliza AM, em uma rede 5g para detectar ataques DoS e DDoS e o seu impacto nos *slices*, partindo dos UEs, o qual utilizou uma RNN (Rede Neural Recorrente) do tipo bidirecional LSTM (Memória de Longo e Curto Prazo). Ambos os trabalhos exploram a segurança em uma rede 5G, mas não da arquitetura Open RAN.

Já há registros da utilização de xApp em segurança na O-RAN, conforme é visto no trabalho [Xavier et al. 2023], que utiliza uma versão própria do Near-RT RIC e um *framework* de classificação adaptado para um xApp que utiliza aprendizado de máquina para detecção de ataques DoS. Além disso, traz uma discussão interessante sobre o tempo de resposta de diferentes modelos de ML, esse é um ponto fundamental, devido o Near-RT RIC exigir operações sensíveis ao tempo. Por fim, o trabalho de [Moore et al. 2023], onde uma xApp é utilizada para monitorar e desassociar os UEs com comportamento malicioso, porém não é realizado um detalhamento sobre a utilização de IA/ML, bem como quais os tipos de *slices* utilizados para teste.

Em suma, os trabalhos apresentados expõem resultados relevantes abordando o impacto de ataques DDoS tem em estruturas sensíveis como os *slices* de redes 5G e consequentemente herdados em O-RAN. Além disso, destacam a importância de soluções que usem ferramentas nativas dessa arquitetura, como as xApps. Este projeto propõe a utilização de uma xApp para detectar e mitigar ataques DDoS que possam degradar a QoS dos *slices*, trazendo como diferencial a adição da utilização de inteligência computacional para gestão e desassociação de usuários maliciosos nos *slices*.

4. *Slice Intelligent Defender xApp*

Nesta seção, primeiro será abordada a arquitetura da proposta e o seu funcionamento, além dos requisitos definidos para seu funcionamento. Em seguida, serão discutidas as ferramentas para implementação e teste da solução.

4.1. Arquitetura Proposta

Como mencionado previamente, a segurança de uma função tão importante quanto os *slices* em O-RAN é fundamental, pois caso algo ocorra com essa estrutura, fatores como a qualidade de serviços críticos e a experiência dos usuários seriam gravemente afetados. Sendo assim, além de ser necessária uma detecção eficaz, a qual é possibilitada pela utilização de IA/AM, também é necessário um tempo de resposta mínimo para mitigar os danos causados caso ocorra tal ataque. Nesse sentido, a utilização de uma xApp contempla as questões abordadas.

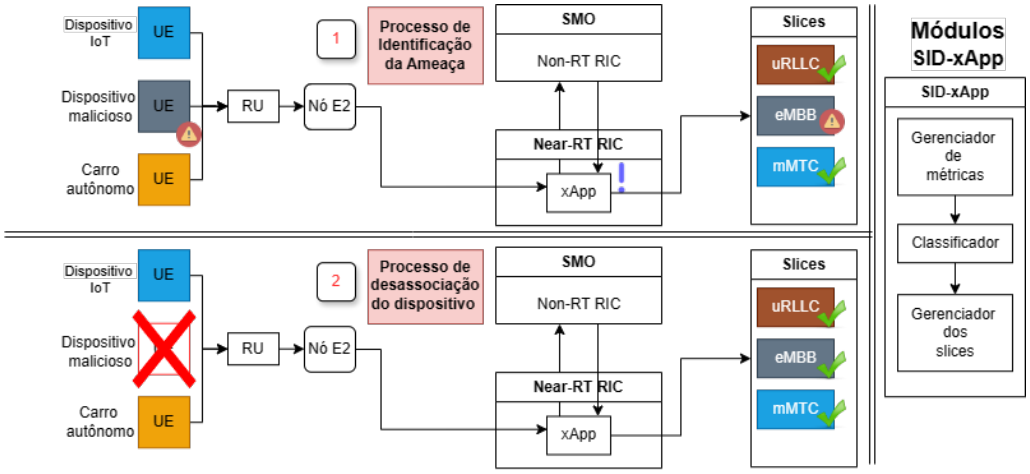

Figura 2. Arquitetura SID-xApp.

A Figura 2 apresenta o esquemático do funcionamento do SID-xApp (*Slice Intelligent Defender xApp*), a qual está organizada a fim de ilustrar o processo de identificação da ameaça e mitigação, bem como os módulos presentes na aplicação. Ela atua acoplada no Near-RT RIC, possibilitando que receba as métricas de fluxo de cada UE que esteja alocado em seu respectivo *slice*, o qual está conectado ao SMO/Non-RT RIC, via interface A1, para definições de políticas e funcionamento da xApp, ilustrado na parte 1 da Figura 2. Com isso, o modelo de IA/AM presente na xApp analisa as características mais relevantes para caracterizar um comportamento malicioso. Caso o comportamento seja confirmado como um ataque, o xApp inicia o processo de desassociação do usuário via interface E2, representado na parte 2 da Figura 2.

Para alcançar esse objetivo, a xApp irá contar primeiro com um sistema modular. Inicialmente, o módulo dedicado a receber métricas dos UEs, que podem ser dispositivos IoT, *smarthphones*, carros autônomos, etc. Este módulo é responsável pela coleta das métricas mais representativas e, posteriormente, o tratamento dos dados e envio para o segundo módulo denominado de classificador.

Em O-RAN, diversos trabalhos vem apresentando bons resultados utilizando modelos de Redes Neurais, Aprendizado por Reforço, Aprendizado Profundo e Aprendizado Federado [Nagib et al. 2024] [Amiri et al. 2024]. Sendo assim, o segundo módulo da xApp, denominado como classificador, desempenha um papel fundamental na detecção de padrões maliciosos na rede. O reconhecimento de comportamentos fora do padrão se dá por meio da utilização de modelos de AM ou IA para análise dos UEs que estão associados aos *slices*, caso o resultado identifique um padrão fora do normal, é realizado o repasse para o terceiro e último módulo.

O terceiro módulo é responsável por desassociar o equipamento comprometido de seu *slice*. A alocação dos dispositivos maliciosos para um *slice* com recursos mínimos, abordagem utilizada em trabalhos citados anteriormente, traz como desvantagem a permanência dos atacantes na rede, e para ataques de larga escala (DDoS) o número de dispositivos pode exceder a capacidade dos slices. Desse modo, o processo de desassociação é realizado retirando os usuários da rede, assim, interrompendo por completo sua utilização.

4.2. Estado Atual de Implementação e Resultados Esperados

O desenvolvimento da xApp está concentrado na implementação do primeiro módulo, gerenciador de métricas, utilizando a linguagem de programação GO para escrita de seu código, a xApp ONOS-RSM [ONOS Project 2022] está sendo usada como base para o processo de coleta das métricas dos *slices* e dos UEs bem como o controle da criação e associação dos *slices* necessários para testes futuros.

A plataforma definida para teste segue o padrão da O-RAN Alliance e 3GPP, é o projeto da ONF chamado de SD-RAN [ONF 2023], que utiliza o Near-RT RIC conhecido como µONOS e componentes de código aberto para integração entre plano de controle e usuário da RAN. Entre as interfaces que ele oferece suporte estão E2, A1 e O1 e, como destaque, o serviço UE-NIB, que extrai informações sobre os UEs. O SD-RAN permite a integração de xApps via APIS gRPC disponibilizada pelo µONOS.

Após o processo de implementação e refinamento da aplicação utilizando o ambiente simulado, espera-se validar a solução no *testbed* do projeto OpenRAN Brasil [RNP 2023], a fim de realizar ajustes de estabilidade da aplicação e avaliar seu desempenho e tempo de resposta com dados reais dos equipamentos reais presentes no *testbed*, resultando em uma validação sólida em um ambiente próximo ao de produção.

5. Considerações Finais

O tema de segurança é fundamental para qualquer área de redes, principalmente para a evolução e consolidação das redes O-RAN. Como foi abordado, ainda é um tema pouco explorado e com poucas soluções práticas, porém, com temas de pesquisas promissores. Com essa mentalidade, foi definida essa proposta, a fim de fomentar o desenvolvimento e segurança na área, a disponibilidade e a qualidade serviço são fundamentais para os usuários, sendo assim, estruturas vitais como os *slices* que permitem serviços críticos devem ser asseguradas.

Fatores importantes serão considerados como requisitos de avaliação para o funcionamento adequado da xApp, como as métricas de acurácia, precisão, *recall* e *f1-score* dos modelos de AM/IA. Outro fator são as métricas coletadas, que caso sejam sensíveis, resultará na priorização de métodos de Aprendizado Federado para garantir a segurança dos dados dos usuários. Além disso, dada a integração da xApp com o Near-RT RIC, cujo *loop* de controle opera entre 10 ms e 1 segundo, é crucial que a xApp tenha um tempo de resposta máximo de 1 segundo. Para isso, diferentes modelos serão testados para determinar o melhor equilíbrio entre desempenho e tempo de resposta.

Desse modo, espera-se que o desenvolvimento do SID-xApp proporcione uma camada adicional de segurança em um ponto crucial das redes O-RAN. A utilização de modelos de AM/IA por parte da aplicação permite uma adaptação dinâmica do ambiente, ao serem considerados requisitos como tempo de resposta, sensibilidade dos dados analisados e desempenho dos modelos, espera-se contribuir com o cenário de pesquisa nesta área. Por fim, resultados e testes realizados durante este trabalho contribuirão para formação de uma base de dados que ficará disponível para estudos futuros.

Agradecimentos

Este trabalho foi realizado com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), da Rede Nacional de Ensino e Pesquisa (RNP) e da Funda-

ção de Amparo à Pesquisa do Estado de São Paulo (FAPESP), por intermédio do projetos No. 2023/00811-0, No. 2020/04031-1, No. 2021/00199-8, e projeto No. 2018/23097-3.

Referências

Amiri, E., Wang, N., Shojafar, M., and Tafazolli, R. (2024). Edge-ai empowered dynamic vnf splitting in o-ran slicing: A federated drl approach. *IEEE Communications Letters*, 28(2):318–322.

Donatti, A., Corrêa, S. L., Martins, J. S. B., Abelem, A. J. G., Both, C. B., de Oliveira Silva, F., Suruagy, J. A., Pasquini, R., Moreira, R., Cardoso, K. V., and Carvalho, T. C. (2024). Survey on machine learning-enabled network slicing: Covering the entire life cycle. *IEEE Transactions on Network and Service Management*, 21(1):994–1011.

Hoffmann, M., Janji, S., Samorzewski, A., Kułacz, , Adamczyk, C., Dryjański, M., Kryszkiewicz, P., Kliks, A., and Bogucka, H. (2024). Open ran xapps design and evaluation: Lessons learnt and identified challenges. *IEEE Journal on Selected Areas in Communications*, 42(2):473–486.

Khan, S., Farzaneh, B., Shahriar, N., Saha, N., and Boutaba, R. (2022). Slicesecure: Impact and detection of dos/ddos attacks on 5g network slices. pages 639–642.

Liyanage, M., Braeken, A., Shahabuddin, S., and Ranaweera, P. (2022). Open ran security: Challenges and opportunities.

Marinova, S. and Leon-Garcia, A. (2024). Intelligent o-ran beyond 5g: Architecture, use cases, challenges, and opportunities. *IEEE Access*, 12:27088–27114.

Moore, J., Abdalla, A. S., Zhang, M., and Marojevic, V. (2023). Demo: Ssxapp: Secure slicing for o-ran deployments. In *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, pages 251–252.

Nagib, A. M., Abou-Zeid, H., and Hassanein, H. S. (2024). Safe and accelerated deep reinforcement learning-based o-ran slicing: A hybrid transfer learning approach. *IEEE Journal on Selected Areas in Communications*, 42(2):310–325.

O-RAN Alliance (2024). Openran specifications. `https://orandownloadsweb.azurewebsites.net/specifications`.

ONF (2023). Sd-ran documentation. `https://docs.sd-ran.org/master/`.

ONOS Project (2022). ONOS-RSM. `https://github.com/onosproject/onos-rsm`.

Polese, M., Bonati, L., D'Oro, S., Basagni, S., and Melodia, T. (2023). Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges. *IEEE Communications Surveys Tutorials*, 25(2):1376–1411.

RNP (2023). Projeto OpenRAN Brasil. `https://www.rnp.br/projetos/openranbrasil`.

Samarakoon, S., Siriwardhana, Y., Porambage, P., Liyanage, M., Chang, S.-Y., Kim, J., Kim, J., and Ylianttila, M. (2022). 5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network.

Xavier, B. M., Dzaferagic, M., Collins, D., Comarela, G., Martinello, M., and Ruffini, M. (2023). Machine learning-based early attack detection using open ran intelligent controller. In *ICC 2023 - IEEE International Conference on Communications*, pages 1856–1861.