Proposta de Open RAN Seguras Através de Distribuição De Chaves Quânticas Criptográficas em Redes QKDs Definidas Por Software

Fernando N. N. Farias[1], Diego Abreu[2], Antônio J. G. Abelém[2]

[1]Redes Nacional de Ensino e Pesquisa – RNP
Rio de Janeiro – RJ – Brazil

[2]Universidade Federal do Pará – UFPA
Belém – PA – Brazil

fernando.farias@rnp.br, diego.abreu@itec.ufpa.br, abelem@ufpa.br

Abstract. *This article proposes the integration of the Open RAN architecture with software-defined Quantum Key Distribution (QKD) networks to enhance the security of cryptographic key exchanges. The initiative introduces a service layer, called O-QKDN, which automates key transfer through quantum channels, mitigating vulnerabilities inherent in conventional methods. The architecture integrates QKD nodes near Open RAN components and employs SDN to orchestrate key distribution in critical channels, such as Fronthaul links and the connection between DU and CU, while remaining compliant with O-RAN Alliance specifications.*

Resumo. *Este artigo propõe a integração entre a arquitetura Open RAN e redes de distribuição de chaves quânticas (QKD) definidas por software, visando aprimorar a segurança na troca de chaves criptográficas. A iniciativa introduz uma camada de serviço, denominada O-QKDN, que automatiza a transferência de chaves por canais quânticos, mitigando vulnerabilidades dos métodos convencionais. A arquitetura integra nós QKD próximos aos componentes Open RAN e emprega SDN para orquestrar a distribuição de chaves em canais críticos, como os links Fronthaul e o enlace entre DU e CU, mantendo conformidade com as especificações da O-RAN Alliance.*

1. Introdução

As redes de acesso via rádio abertas (*Radio Access Network*, RAN), em sua quinta geração (5G), têm ganhado destaque significativo tanto na academia quanto na indústria, devido à sua facilidade de implantação, desenvolvimento e evolução. O 5G está expandindo as possibilidades de uso desse modelo de rede sem fio para além da telefonia, abrangendo aplicações como teleconferências, sensoriamento remoto, aviação e veículos não tripulados e conectividade de alta velocidade e baixa latência [Cordovil et al. 2024]. No entanto, elas começaram a ter maior notoriedade, a partir do movimento de desagregação e abertura de sua arquitetura, também chamada de *Open RAN* (*Open Radio Access Network*)[Kempf and Yegani 2002].

As Open RANs permitiram que as BBUs (*Baseband Units*) centralizadas fossem divididas em duas partes: DU (*Distributed Unit*) e CU (*Centralized Unit*). Essa divisão distribui o processamento de sinais de frequência ao longo da arquitetura Open RAN, utilizando o chamado *split* 7.2x. Além disso, padronizam interfaces abertas, o que possibilita interoperabilidade, flexibilidade e neutralidade entre fabricantes de equipamentos [Wani et al., 2024]. Com o objetivo de padronizar esse movimento, foi

fundada a ORAN Alliance, responsável por definir toda a especificação da arquitetura em diversas áreas, como orquestração, controlador inteligente da RAN (*RAN Intelligent Controller* - RIC), *fronthaul* e segurança.

O Open RAN, como uma tecnologia emergente, ainda apresenta lacunas em sua arquitetura, especialmente no que diz respeito à segurança. Atualmente, o grupo de trabalho da ORAN Alliance estabeleceu que a base criptográfica dessa arquitetura é fundamentada em trocas de chaves entre pares utilizando canais tradicionais, como a internet [O-RAN Alliance 2025]. No entanto, ainda não há uma padronização definida para garantir a comunicação segura dessas chaves criptográficas dentro da arquitetura Open RAN. Essa ausência de padronização gera vulnerabilidades de segurança, particularmente no caso de interceptações de chaves durante a comunicação entre pares, as quais podem ocorrer sem que sejam detectadas.

Nesse contexto, as redes quânticas de distribuição de chaves definidas por software (*Software Defined Quantum Key Distribution* – SD-QKD) oferecem interfaces abertas para solicitação, alocação e transferência de chaves criptográficas. Essa tecnologia utiliza uma rede QKD baseada em protocolos de detecção de intrusos no canal quântico, como BB84, E91, B92, SARG04 e outros [Mehic et al. 2024]. Atualmente, essa arquitetura de distribuição é considerada a mais segura para a troca de chaves criptográficas.

Portanto, este trabalho tem como objetivo apresentar uma proposta de extensão da arquitetura Open RAN para suportar a transferência de chaves criptográficas em canais quânticos, oferecendo também o serviço de requisição e transferência de chaves entre os diversos elementos que compõem o Open RAN. A proposta utiliza a arquitetura baseada na especificação da O-RAN Alliance [ORAN Alliance 2025], que sugere a inclusão de uma interface aberta para consumo dos serviços pelos componentes da arquitetura Open RAN (por exemplo, DU, CU e Core 5G)

Além desta seção introdutória, o artigo está dividido em duas outras partes. A Seção 2 apresenta a definição da proposta, abordando brevemente o estado da arte sobre Open RAN e Redes QKD. Já a Seção 3 traz as conclusões e os trabalhos futuros relacionados à proposta.

2. Habilitando Redes Open RAN Seguras

Nesta seção, aborda-se a proposta de habilitar redes Open RAN seguras baseadas em comunicação quântica. Inicialmente, apresenta-se uma revisão dos conceitos de Open RAN e Redes QKD. Em seguida, detalha-se a proposta de integração desses conceitos para aumentar a segurança na arquitetura Open RAN.

2.1. Open RAN

Open RAN refere-se a um ecossistema de tecnologias e padrões abertos que permitem a separação dos componentes da RAN, como hardware e software. Essa abordagem permite que diferentes fornecedores forneçam componentes interoperáveis, estimulando a concorrência e a escolha de soluções mais eficientes e econômicas.

A desagregação e abertura da RAN têm como objetivo otimizar o desempenho da rede e a utilização de recursos, ao desacoplar suas funções principais em componentes distintos. A desagregação, que foca principalmente na separação das funcionalidades

dentro da RAN, divide o gNB em dois componentes essenciais: a Unidade Centralizada (Central Unit - CU) e a Unidade Distribuída (*Distributed Unit* - DU), configuração conhecida como Split 7.2. O plano de usuário da CU (CU-UP) e o plano de controle da CU (CU-CP). O CU-UP é responsável por gerenciar o tráfego do usuário, como dados e voz, enquanto o CU-CP lida com sinalização de controle e tarefas de gerenciamento de rede. Por outro lado, a DU lida com as funções das camadas inferiores, incluindo o processamento da camada de controle de acesso ao meio (*Medium Access Control* - MAC), da camada física (*Physical Layer* - PHY) e a transmissão dos sinais de radiofrequência (*Radio Frequency* - RF).

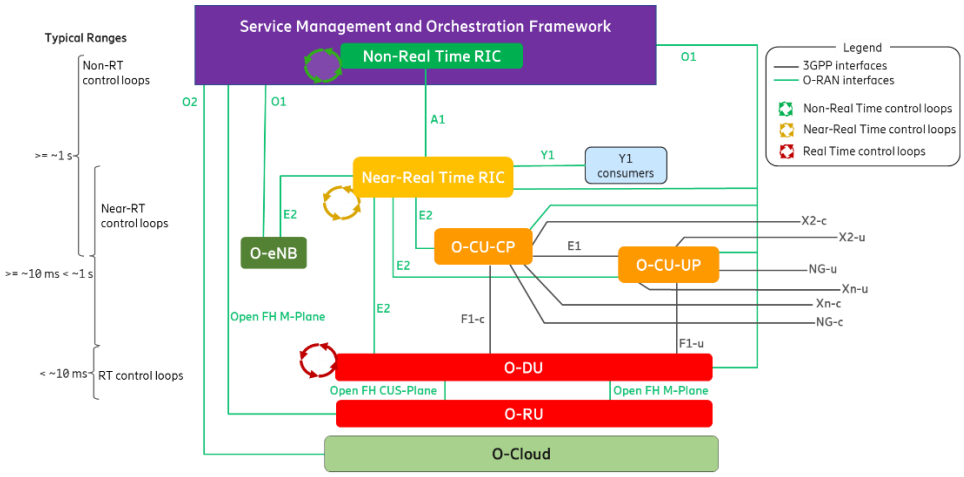

Figura 1. Arquitetura do Modelo Open RAN. Fonte: ORAN Alliance [2025]

Open RAN também apresenta o conceito de RIC, como um componente chave desagregado, projetado para aprimorar a inteligência e a adaptabilidade da RAN. Existem dois tipos de controladores RIC com características e propósitos distintos, onde a principal diferença é o tempo de atuação. Como os próprios nomes sugerem, o *Near-RT* RIC é projetado para executar ações em tempo quase real e o *Non-RT RIC* age mais lentamente, podendo realizar os controles com intervalos de alguns minutos ou horas.

Já a *O-Cloud* é uma plataforma de computação em nuvem que consiste em uma coleção de nós de infraestrutura física que atendem aos requisitos do Open RAN para hospedar as funções de rede relevantes, por exemplo, RIC, CU e DU, os componentes de software de suporte como sistema operacional, máquina virtual, contêiner e outros, e as funções de gerenciamento e orquestração.

Por fim, a abertura promove interfaces de comunicação entre os elementos da arquitetura Open RAN. As interfaces da Open RAN desempenham papéis distintos e complementares: a A1 conecta os RICs para controle e políticas de alto nível, enquanto a O1 oferece serviços de gerenciamento e ciclo de vida dos componentes. A interface E2 conecta o *Near-RT* RIC aos nós E2, possibilitando o controle e coleta de métricas da RAN. A F1, por sua vez, liga os elementos CU e DU, separando os planos de controle e dados, enquanto a E1 gerencia a transmissão de sinais entre a DU e RU, incluindo funções relacionadas à camada física da rede. Cada interface é fundamental para a coordenação e otimização da infraestrutura O-RAN.

2.2. Redes QKD

As redes QKD (*Quantum Key Distribution*) têm como principal objetivo a distribuição

segura de chaves criptográficas entre partes distantes, aproveitando os princípios da mecânica quântica para garantir a confidencialidade contra qualquer tipo de interceptação, apresentado na Figura 2 - A.

Para que essas redes sejam aplicáveis em ambientes reais, é fundamental que elas se integrem eficientemente às redes clássicas de comunicação. Essa integração ocorre através de arquiteturas híbridas, onde a camada de distribuição de chaves quânticas é conectada a uma infraestrutura de rede clássica, composta por elementos como switches, roteadores e controladores definidos por software (SDN), conforme ilustrado na Figura 2-A. A adoção de SDN facilita o gerenciamento dinâmico dos canais de comunicação e a orquestração do fluxo de chaves, maximizando tanto o desempenho quanto a segurança da rede, conforme representado na Figura 2-B e C.

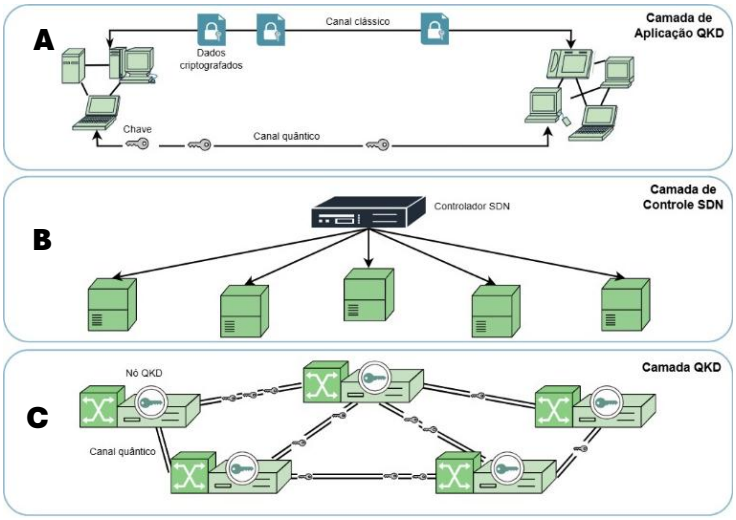

Figura 2. Arquitetura das Redes QKD definidas por softwares.

Um componente central dessa arquitetura é o KMS (Key Management System), que atua como um intermediário entre a rede QKD e os aplicativos finais. O KMS é responsável por armazenar, gerenciar e distribuir as chaves geradas pelos links QKD, garantindo que apenas entidades autorizadas possam utilizá-las. Dessa forma, as redes QKD, integradas a redes clássicas, oferecem um modelo prático e escalável de segurança da informação, no qual a distribuição de chaves ocorre de forma autêntica, confidencial e resistente a ataques, mesmo de adversários com acesso a computadores quânticos.

2.3. Redes Open RAN Seguras com Redes QKD

Atualmente, não há uma padronização para a comunicação segura de chaves criptográficas na arquitetura Open RAN, apenas padrões de criptografia e especificações de protocolos seguros baseados em definições da 3GPP, IETF ou O-RAN Alliance. No entanto, as chaves ainda são compartilhadas por meio de canais tradicionais/clássicos, como a internet.

O uso de Redes de Distribuição de Chaves Quânticas (QKD) pode auxiliar na troca de chaves seguras entre as interfaces das redes Open RAN, oferecendo um nível de segurança baseado em princípios físicos que são, atualmente, a forma mais segura para distribuição de chaves criptográficas baseados em algoritmos de detecção de intrusos no canal quântico. A tecnologia QKD já é uma realidade e está sendo desenvolvida para aplicações práticas, como a futura internet quântica.

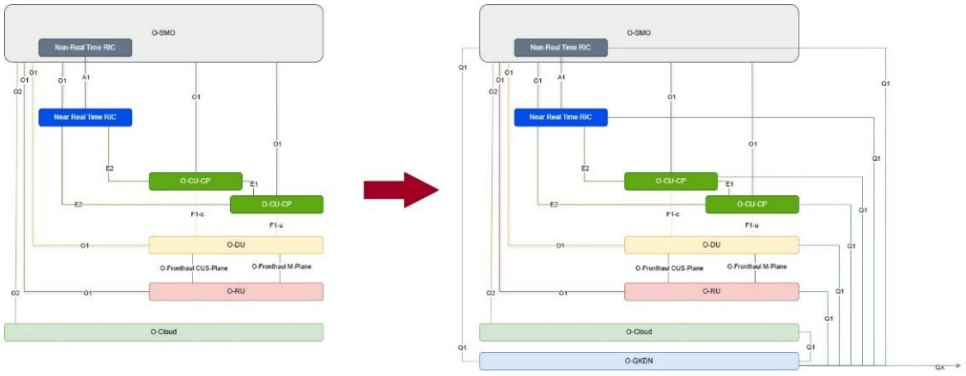

Figura 3. Proposta de adoção das QKDs em Open RANs.

A Figura 3 apresenta a proposta de integração das redes QKD à arquitetura Open RAN, utilizando uma camada de serviço chamada *Open Quantum Key Distributed Network* (O-QKDN). Essa camada opera por meio da interface Q1, que permite a aquisição e transferência de chaves entre pares de componentes. Por exemplo, para o canal de *Fronthaul* (F1 ou FAPI) entre RU ↔ DU (eCPRI) e DU ↔ CU (F1), utilizando MACsec [IEEE 802.1AE 2018], cuja implementação tradicionalmente requer trocas de chaves de forma manual. Nesse contexto, o O-QKDN é empregado para automatizar a troca de chaves em canais quânticos entre os componentes O-DU e O-RU, por meio dos KMSs do O-QKDN, gerenciados pelo controlador SDN dá O-QKDN.

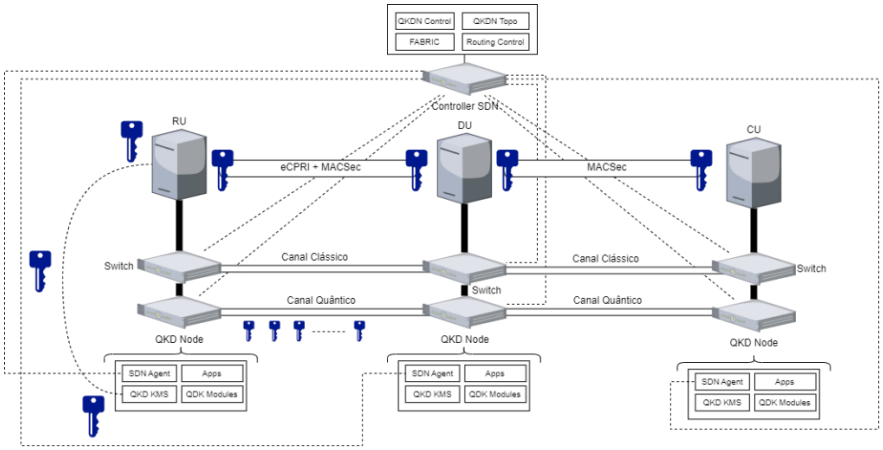

Figura 4. Proposta de arquitetura de integração O-RAN e SD-QKD (O-QKDN).

A Figura 4 apresenta a arquitetura proposta de integração, que inclui a inserção de nós QKD próximos aos componentes das redes Open RAN. Esses nós oferecem suporte ao uso do canal quântico para o consumo de chaves criptográficas quânticas, eliminando a necessidade de compreender os detalhes do processo de geração. De forma automatizada, essa abordagem reduz significativamente a participação de terceiros no processo de transferência dessas chaves. Além disso, haveria pouca ou nenhuma necessidade de modificar os protocolos existentes para a utilização mesmo no modelo atual.

Atualmente, a proposta de desenvolvimento está focada na emulação de elementos por meio de conteinerização, utilizando soluções como Mininet e vSDNEmul como base [Farias et al. 2019]. Para a Open RAN, o objetivo é empregar o software SRS-RAN[1] com

[1]Projeto srsRAN: https://www.srsran.com/

seus próprios emuladores de UEs e RUs. Por outro lado, a parte dedicada aos nós quânticos está sendo desenvolvida com base no plano de controle proposto pela ITU-T Y3805 [2021], juntamente com a simulação do comportamento de canais quânticos. Neste momento, o objetivo não é criar um emulador de nó QKD, mas sim analisar o comportamento do plano de controle em operação e sua integração com controlador SDN.

3. Conclusão e Trabalhos Futuros

Este artigo apresentou uma proposta de integração entre redes QKDs definidas por software e a arquitetura Open RAN. O principal objetivo é desenvolver uma rede que combine a segurança robusta da criptografia quântica com a flexibilidade e eficiência das redes Open RAN. Além disso, busca-se oferecer à arquitetura O-RAN um serviço dedicado ao consumo e publicação de chaves criptográficas quânticas, atendendo às demandas de serviços que requerem criptografia.

Os trabalhos futuros devem se concentrar em aprimorar a integração das redes QKDs à arquitetura Open RAN, explorando métodos para automatizar a troca de chaves criptográficas quânticas em múltiplos cenários. Será essencial validar o desempenho do plano de controle proposto, otimizando sua operação em cenários híbridos que combinem elementos clássicos e quânticos. Simulações e experimentos adicionais serão fundamentais para avaliar a viabilidade de diferentes abordagens e identificar possíveis desafios operacionais na interação entre as camadas quânticas e os componentes O-RAN

Agradecimentos

Este projeto conta com o apoio do Ministério da Ciência, Tecnologia e Inovação por meio dos recursos da Lei nº 8.248, de 23 de outubro de 1991, conforme orientação da Secretaria de Empreendedorismo e Inovação do MCTI, consolidado no projeto Programa OpenRAN@Brasil, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) projeto 2023/00811-0, projeto 2023/00673-7, projeto 2021/00199-8 (CPE SMARTNESS), projeto 2020/04031-1, e projeto 2018/23097-3

Referências

Cordovil, M. G. da C., Silva, M., Leite, V. D., et al. (oct 2024). Um Framework de Coleta de Indicadores-Chave de Desempenho para Redes 5G O-RAN. In *Anais do XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*. . Sociedade Brasileira de Telecomunicações.

Farias, F. N. N., Junior, A. O., Da Costa, L., Pinheiro, B. A. and Abelem, A. J. G. (28 aug 2019). vSDNEmul: A Software-Defined Network Emulator Based on Container Virtualization. *International journal of simulation: systems, science & technology*,

IEEE 802.1AE (jan 2018). Local and metropolitan area networks Media Access Control (MAC) Security.

ITU-T (2021). ITU-T Quantum key distribution networks – Software-defined networking control. http://handle.itu.int/11.1002/1000/.

Kempf, J. and Yegani, P. (may 2002). OpenRAN: a new architecture for mobile wireless internet radio access networks. *IEEE Communications Magazine*, v. 40, n. 5, p. 118–123.

Mehic, M., Michalek, L., Dervisevic, E., et al. (2024). Quantum Cryptography in 5G Networks: A Comprehensive Overview. *IEEE Communications Surveys and Tutorials*, v. 26, n. 1, p. 302–346.

ORAN Alliance (feb 2025). O-RAN Architecture Description. https://specifications.o-ran.org/download?id=789, Acessado em: 28/03/2025.

O-RAN Alliance (mar 2025). O-RAN Security Requirements and Controls Specifications. https://specifications.o-ran.org/download?id=843, Acessado em: 26/03/2025.