Alocação de Recursos em Redes de Distribuição Quântica de Chaves Definidas por Software

Arthur Pimentel [1], **Diego Abreu**[1], **Antônio Abelém**[1]

[1]Universidade Federal do Pará (UFPA)

arthur.pimentel@icen.ufpa.br, diego.abreu@itec.ufpa.br, abelem@ufpa.br

Resumo. *O avanço da criptografia quântica torna premente o uso de recursos em redes de Distribuição Quântica de Chaves (QKD) de forma eficiência. Sob esse contexto, o atual trabalho apresenta uma nova abordagem de arquitetura para redes QKD em conjunto com Redes Definidas por Software (SDN), utilizando estratégias de roteamento e agendamento voltadas para a utilização consciente de recursos. A proposta dessa arquitetura visa otimizar a alocação de recursos, chaves quânticas e rotas, por meio do controle SDN eficiente, à medida que atende às requisições de aplicações da rede. A eficácia da solução foi avaliada em cenários de aplicação utilizando topologias reais de redes QKD, considerando diferentes padrões de requisições para aplicações de autenticação e criptografia, demonstrando ganhos significativos em eficiência e desempenho. Os resultados demonstram a viabilidade dessa arquitetura em diversos ambientes, destacando seu potencial para melhorar a escalabilidade e eficiência das redes quânticas.*

1. Introdução

A segurança na troca de informações é uma premissa fundamental na era digital, onde a vulnerabilidade de dados pode levar a consequências severas. Neste cenário, a Distribuição Quântica de Chaves (QKD, do inglês *Quantum Key Distribution*) tem emergido como uma solução promissora, capaz de utilizar os princípios da mecânica quântica para garantir segurança inquebrável na distribuição de chaves criptográficas [Cao et al. 2022a].

Com a adoção crescente da QKD, redes específicas para sua implementação têm sido estabelecidas globalmente, destacando-se as iniciativas na Europa e na China [Xu et al. 2020, Ribezzo et al. 2023]. Estas redes buscam facilitar uma comunicação segura em massa, mas enfrentam desafios significativos relacionados à gestão da qualidade e segurança dos serviços ofertados [Mehic et al. 2020].

Neste contexto, a integração das Redes Definidas por Software (SDN, do inglês *Software Defined Networks*) se mostram como uma solução viável para o gerenciamento das infraestruturas de QKD. As SDNs proporcionam uma maior flexibilidade e controle sobre as redes, facilitando a implementação de políticas de segurança adaptativas e a gestão eficiente do tráfego de dados.

Este trabalho propõe uma arquitetura para redes de QKD que utiliza a tecnologia SDN visando uma gerência eficiente. O estudo detalha o desenvolvimento de uma plataforma de rede QKD multiprotocolos, explorando a eficácia da arquitetura através de simulações que demonstram a alocação dinâmica de recursos e a resposta às mudanças nas demandas de tráfego.

2. Distribuição Quântica de Chaves

As comunicações quânticas têm evoluído notavelmente, impulsionadas por avanços em campos como redes de emaranhamento quântico, computação quântica distribuída e redes de sensores quânticos [Abreu et al. 2024, Abelém et al. 2020]. No entanto, dentre essas inovações, as redes de Distribuição Quântica de Chaves (QKD) destacam-se por já estarem operacionais em ambientes de produção real, conforme implementações bem-sucedidas reportadas em diversas regiões [Xu et al. 2020, Ribezzo et al. 2023]. A QKD visa o compartilhamento seguro de chaves criptográficas, cruciais para aplicações como criptografia e autenticação, explorando fenômenos quânticos como superposição e entrelaçamento para garantir comunicações à prova de interceptações.

A nossa abordagem de rede QKD trata três protocolos principais: BB84, B92 e E91, cada um contribuindo com estratégias distintas para a segurança quântica. O protocolo BB84, pioneiro na área, fundamenta-se no uso de duas bases de medição e dois estados quânticos. Nele, Alice prepara e envia qubits para Bob, que os mede usando bases aleatórias. A correspondência entre as bases de Alice e Bob determina quais bits serão adicionados à chave compartilhada. Nesse sentido, tentativas de espionagem são reveladas por discrepâncias nos resultados das medições, graças ao princípio da não-clonagem quântica.

O protocolo B92 simplifica o BB84 ao usar apenas um estado quântico por base para representar os bits 0 e 1. Alice envia qubits codificados em uma base ou outra, enquanto Bob, ao medir os qubits, consegue determinar a base usada e adiciona o bit correspondente à chave apenas quando suas bases não coincidem.

Por fim, o protocolo E91, baseado na geração de pares de partículas entrelaçadas (pares EPR), eleva a segurança ao utilizar a correlação quântica inerente ao entrelaçamento. Alice e Bob medem suas partículas entrelaçadas em bases aleatórias e, ao compararem as bases utilizadas, podem determinar quais bits são válidos para a chave final. Este protocolo atua bem, mesmo sobre grandes distâncias, e é particularmente robusto contra tentativas de interceptação devido à natureza imediata do colapso do entrelaçamento.

3. Trabalhos Relacionados

A literatura recente sobre comunicações quânticas reflete um interesse crescente nos desafios associados à gestão de recursos em redes de Distribuição Quântica de Chaves (QKD). Os trabalhos de Cao et al. (2018) [Cao et al. 2018] e Fu et al. (2020) [Fu et al. 2020] concentram-se em estratégias de agendamento para otimizar a eficiência na distribuição de chaves em redes QKD modeladas teoricamente como grafos. Cao et al. aplicam algoritmos de caminho mínimo, como o de Dijkstra, e técnicas de alocação como o método *first-fit*, enquanto Fu et al. investigam abordagens de alocação randômica, ambas visando maximizar a taxa de sucesso das chaves. Em contraste, nossa pesquisa avança ao integrar a flexibilidade de uma arquitetura QKD multiprotocolo com o uso de Redes Definidas por Software (SDN), proporcionando um controle mais abrangente e adaptativo.

Adicionalmente, estudos como os de Yu et al. (2023) [Yu et al. 2023] e Zhang et al. (2023) [Zhang et al. 2023] abordam a otimização do roteamento e da alocação de recursos em redes QKD, focando em parâmetros como eficiência energética e taxa de sucesso das chaves. Embora esses estudos forneçam insights valiosos, eles não contemplam a integração de múltiplos protocolos de QKD em suas análises.

Por fim, trabalhos como os de Cao et al.(2022c) [Cao et al. 2022c] e Cao et al. (2022b) [Cao et al. 2022b] exploram a adaptação das redes QKD para suportar uma variedade de protocolos e a aplicação de tecnologias SDN para facilitar essa adaptação. Nossa proposta alinhada-se com essas abordagens, mas se distingue ao combinar efetivamente um sistema multiprotocolo com a infraestrutura de SDN, resultando em uma solução holística que otimiza a gestão de recursos para aplicações críticas como autenticação e criptografia.

4. Redes de Distribuição Quântica de Chaves Definidas por Software

Uma rede QKD tem como principal objetivo prover serviços de criação, distribuição e gerenciamento de chaves seguras [Pimentel et al. 2024]. A rede QKD funciona em conjunto com serviços de segurança como criptografia e autenticação que utilizam essas chaves em suas aplicações. Com a crescente diversificação de possíveis aplicações e as restrições de recursos existentes, as redes QKD multiprotocolo enfrentam desafios significativos em termos de gerenciamento e controle. Nesta seção, é apresentada a proposta de arquitetura para uma rede QKD baseada em SDN.

4.1. Arquitetura da Rede SDN QKD

A Figura 1 ilustra a arquitetura desenvolvida da rede SDN QKD, que se estrutura em quatro camadas distintas: a camada de aplicação QKD, a camada de controle SDN, a camada de QKD e a camada de dados clássicos.

A camada de aplicação QKD serve como interface para os usuários, gerenciando e encaminhando requisições de chaves criptográficas, selecionando o protocolo mais adequado entre os disponíveis. Já a camada de controle SDN é o núcleo da arquitetura, coordenando a alocação de recursos e roteamento, e comunicando-se com as camadas de dados quânticos e clássicos para manter a eficiência da rede. Os dados quânticos estão na camada QKD, que cuida do preparo e envio dos qubits, incluindo o entrelaçamento e medição. Por fim, a camada de dados clássicos suporta a transmissão das informações necessárias para a operação da rede, como sincronização e controle.

Nesse contexto, o controlador SDN desempenha um papel central na operação da rede, sendo responsável por gerenciar o agendamento das transmissões e alocação das rotas e canais, para otimizar a transmissão de qubits e a distribuição de chaves. Encontra-se a rota mais curta por meio do algoritmo de Dijkstra e verifica-se a disponibilidade de recursos. Após o cálculo das rotas, as requisições são enviadas para os nós, que executam as instruções conforme determinado, e se uma rota viável não for encontrada após um número predefinido de tentativas, a requisição é adiada para reavaliação futura, garantindo flexibilidade e adaptabilidade na rede. Dessa forma, o controlador garante que a troca de chaves seja realizada de forma segura e otimizada, respeitando as características dos protocolos QKD utilizados.

Com a adoção de SDN em redes QKD, busca-se uma série de aprimoramentos importantes, incluindo maior flexibilidade, eficiência e segurança na distribuição de chaves quânticas. Além disso, a camada de controle SDN permite a troca dinâmica de diferentes políticas de roteamento, para o uso eficiente dos recursos, adaptando-se às necessidades dinâmicas da rede e aos requisitos particulares dos diferentes protocolos QKD. Essa abordagem não apenas melhora a escalabilidade das redes QKD, mas também estabelece uma

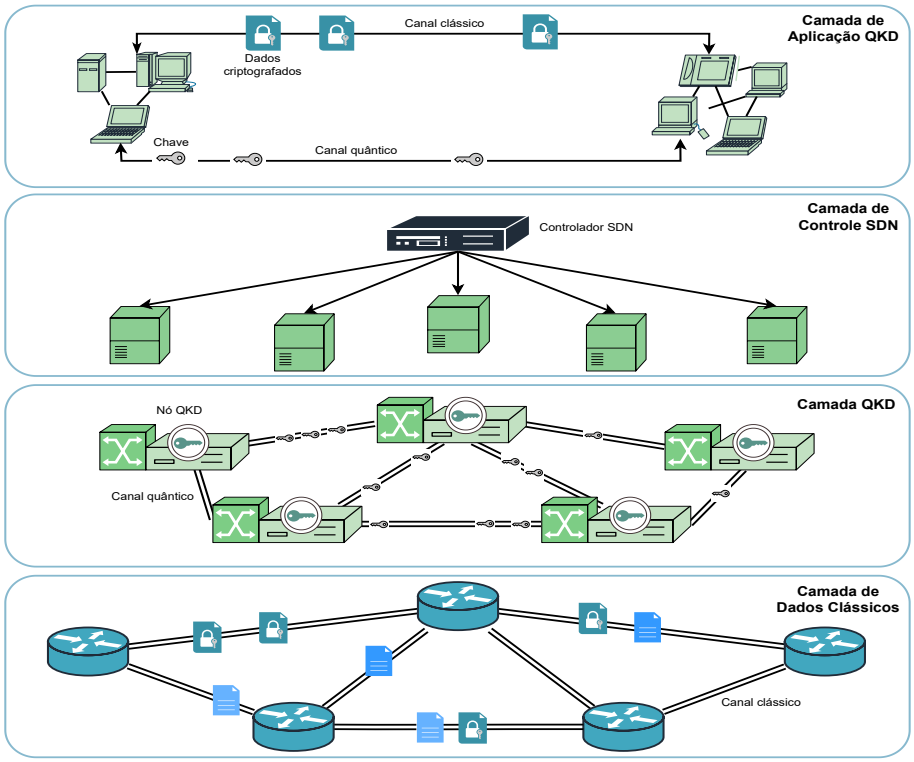


Figura 1. Arquitetura da Rede SDN QKD.

base sólida para inovações futuras, como a integração com outras tecnologias emergentes e o desenvolvimento de redes quânticas mais robustas e seguras.

5. Estudo de Caso

Para avaliar o sistema proposto, foi realizado um estudo de caso com aplicações de segurança. Utilizou-se o OpenQKDSim[1] para simular aplicações de criptografia e autenticação, um simulador que permite a experimentação de aplicações QKD. A modelagem da arquitetura da rede e a alocação de recursos foram implementadas através de simulação discreta, utilizando a linguagem de programação Python. Os códigos desenvolvidos para o sistema, a codificação dos protocolos QKD, assim como os *scripts* específicos para a simulação do estudo de caso, estão disponíveis publicamente no repositório do artigo[2].

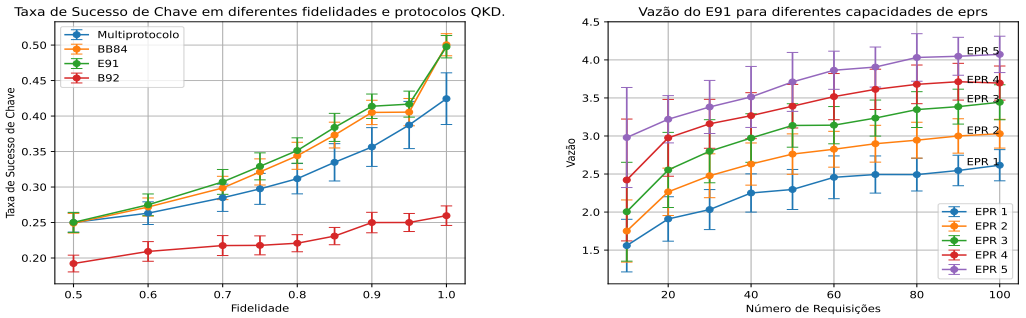
No estudo de caso foram utilizadas duas topologias de rede, as topologias das redes QKD reais da China [Xu et al. 2020] e de Viena [Peev et al. 2009], apresentadas na Figura 5. Essas topologias foram escolhidas por representarem exemplos reais de implementações de redes QKD em ambientes de produção, oferecendo um contexto prático e relevante para a análise. Em nossa abordagem, cada nó na rede é tratado como um potencial ponto de origem ou destino para as requisições de segurança. Isso permite a avaliação do desempenho da rede sob condições variadas de tráfego e padrões de comunicação, refletindo as complexidades e desafios enfrentados em redes QKD reais.

[1]https://www.open-qkd.eu/
[2]https://github.com/artuenric/qkd-net

6. Resultados e Discussões

Na simulação realizada, foram ajustados diversos parâmetros para avaliar o desempenho do sistema, conforme mostrado na Figura 2. Os resultados indicam que o protocolo BB92 teve uma taxa de sucesso inferior na geração de chaves em comparação com os protocolos E91 e BB84, devido ao uso de menos estados quânticos. Quando múltiplos protocolos foram utilizados simultaneamente, a taxa de sucesso global foi ligeiramente inferior, influenciada negativamente pelo desempenho do B92.

A Figura 2.b demonstra o impacto da quantidade de pares EPR disponíveis na vazão da rede e no número de requisições alocadas simultaneamente, no contexto do protocolo E91. Observou-se que a quantidade de pares EPR influencia diretamente a vazão da rede, levando a ajustes na fidelidade e no número de pares EPR por canal para equilibrar a eficácia na geração de chaves e a eficiência no uso dos recursos da rede.



(a) Taxa de Chaves para em diferentes configurações de protocolos QKD.

(b) Vazão em quantidade diferentes de pares EPR no Protocolo E91, em diferentes quantidades requisições.

Figura 2. Experimentos de ajuste dos parâmetros.

7. Conclusão e Trabalhos Futuros

Este estudo comprovou a viabilidade e eficácia de uma arquitetura de rede QKD baseada em SDN para controle da rede destacando a importância da gestão de recursos e distribuição adequada para melhorar a eficiência e vazão das redes QKD. Para trabalhos futuros, recomenda-se a expansão da arquitetura, considerando novos cenários, desafios de segurança e a integração com tecnologias emergentes de computação quântica. Além de investigar sua aplicação em grandes redes e sua interação com redes clássicas, visando uma otimização conjunta dos recursos.

8. Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), projeto 2020/04031-1, projeto 2021/00199-8 (CPE SMARTNESS), projeto 2023/00673-7 e projeto 2023/00811-0.

Referências

Abelém, A., Vardoyan, G., and Towsley, D. (2020). Quantum internet: The future of internetworking. In *Minicursos do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 48–90. SBC.

Abreu, D., Pimentel, A., and Abelém, A. (2024). Reqroute: Protocolo de roteamento por reforço para redes de entrelaçamento quântico. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 630–643. SBC.

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., and Hanzo, L. (2022a). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2):839–894.

Cao, Y., Zhao, Y., Wu, Y., Yu, X., and Zhang, J. (2018). Time-scheduled quantum key distribution (qkd) over wdm networks. *Journal of Lightwave Technology*, 36(16).

Cao, Y., Zhao, Y., Zhang, J., and Wang, Q. (2022b). Software-defined heterogeneous quantum key distribution chaining: An enabler for multi-protocol quantum networks. *IEEE Communications Magazine*, 60(9):38–44.

Cao, Y., Zhao, Y., Zhang, J., Wang, Q., Niyato, D., and Hanzo, L. (2022c). From single-protocol to large-scale multi-protocol quantum networks. *IEEE Network*, 36(5):14–22.

Fu, Y., Hong, Y., Quek, T. Q., Wang, H., and Shi, Z. (2020). Scheduling policies for quantum key distribution enabled communication networks. *IEEE Wireless Communications Letters*, 9(12):2126–2129.

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., et al. (2020). Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41.

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., et al. (2009). The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001.

Pimentel, A., Abreu, D., and Abelém, A. (2024). Alocação de recursos em redes de distribuição quântica de chaves multiprotocolo. In *Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF)*, pages 39–46. SBC.

Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., Oxenløwe, L. K., Lončarić, M., Cvitić, I., Stipčević, M., et al. (2023). Deploying an inter-european quantum network. *Advanced Quantum Technologies*, 6(2):2200061.

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002.

Yu, J., Qiu, S., and Yang, T. (2023). Optimization of hierarchical routing and resource allocation for power communication networks with qkd. *Journal of Lightwave Technology*.

Zhang, Q., Ayoub, O., Gatto, A., Wu, J., Musumeci, F., and Tornatore, M. (2023). Routing, channel, key-rate and time-slot assignment for qkd in optical networks. *IEEE Transactions on Network and Service Management*.