Ataques de Repetidores em Redes de Entrelaçamento Quântico

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

[1]Universidade Federal do Pará (UFPA)

Abstract. *Quantum entanglement networks represent cutting-edge technologies with critical applications in secure communication. However, their reliance on the unconditional trust of quantum repeaters introduces potential vulnerabilities to third-party attacks. Notably, the Quantum Hijacking Attack and the Quantum Black Hole Attack have gained attention for exploiting this trust-based weakness. This study analyzes the mechanisms behind these attacks, with particular emphasis on the Quantum Black Hole Attack, and highlights the limitations of current tomography-based detection methods in effectively identifying such threats.*

1. Introdução

O aumento da complexidade nas redes quânticas — especialmente aquelas fundamentadas no entrelaçamento — tem revelado novas classes de vulnerabilidades [Suzuki and Van Meter 2015]. Procedimentos como a troca de entrelaçamento (*entanglement swapping*) exigem uma coordenação precisa entre os repetidores quânticos para estabelecer pares entrelaçados entre nós geograficamente separados [Zangi et al. 2023]. No entanto, repetidores comprometidos podem interferir nessas operações, manipulando tanto os parâmetros internos dos dispositivos quanto seus canais de controle clássico. Embora alguns estudos anteriores tenham abordado esses cenários de forma introdutória [Satoh et al. 2018, Suzuki and Van Meter 2015], ainda há uma lacuna de investigações aprofundadas que avaliem o impacto dessas ameaças sobre métricas essenciais da rede, considerando o ambiente operacional, as particularidades dos repetidores e os métodos atualmente empregados para o monitoramento de redes quânticas [Guedes de Andrade et al. 2024].

Embora as redes quânticas ofereçam segurança comprovada e contem com uma ampla gama de aplicações, ainda existem fundamentos que podem ser explorados por agentes maliciosos. Apesar de ser impossível violar os dados transmitidos em redes baseadas em entanglement swapping sem detecção — como demonstrado em aplicações de Quantum Key Distribution (QKD) [Yuen 2016] —, é plausível que a rede seja comprometida se o atacante explorar vulnerabilidades nos seus mecanismos operacionais [Satoh et al. 2021]. Nesse contexto, componentes críticos como os repetidores quânticos — dispositivos especializados que viabilizam o tráfego de informação por meio de processos como entanglement swapping e purificação quântica — tornam-se alvos potenciais de ataques. No entanto, os riscos associados a esses elementos ainda não são explorados em toda a sua plenitude na literatura.

A possibilidade de vulnerabilidades em repetidores quânticos põe em xeque a segurança de redes inteiras, e tendo a capacidade de afetar diretamente características essenciais. Ataques com potenciais de raptar pacotes como o *Quantum Black Hole Attack*

(QBHA) ou de sequestro de roteadores como o *Quantum Hijacking Attack* (QHA) afetam diretamente a disponibilidade e confiabilidade da rede, tendo como seus principais alvos *hardwares* de roteamento. Essa frente de ataques é crucial ser estudada e categorizada a fim de minimizar os danos potenciais, por isso, esse artigo irá abordar como os ataques QBHA e QHA podem ser utilizados para ferir a confiabilidade de uma rede e como os mesmo podem vir a ser identificados.

2. Ataque de Repetidores Quânticos

2.1. Hijacking Attack

As redes quânticas, especialmente aquelas que utilizam repetidores para estabelecer conexões entre nós distantes, apresentam vulnerabilidades específicas que podem ser exploradas por agentes maliciosos. Um dos ataques mais críticos nesse contexto é o *Hijacking Attack*, que consiste no sequestro de um repetidor quântico. Ao assumir o controle de um nó intermediário, o invasor adquire a capacidade de manipular operações como o *entanglement swapping*, redirecionar conexões e até entrelaçar estados quânticos com qubits de sua posse.

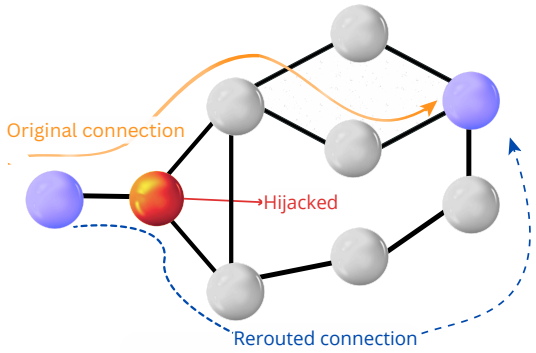


Figure 1. Ataque Hijacking bem sucedido

A *Figura 1* ilustra um cenário em que o ataque é bem-sucedido: o repetidor sequestrado se torna parte essencial do caminho entre os nós, impedindo que os pacotes quânticos sejam transmitidos sem sua mediação. Com isso, o atacante pode interceptar e potencialmente modificar os dados antes de entregá-los ao destino. Além disso, quando não há alternativas de roteamento, o nó malicioso se torna um ponto obrigatório de passagem, o que torna o ataque ainda mais crítico para a continuidade e segurança da rede.

Uma das principais características desse ataque é sua natureza furtiva. O nó comprometido pode operar de forma a simular um comportamento legítimo, dificultando a detecção por meio de verificações locais. Para enfrentar essa limitação, propõe-se o uso de técnicas como a tomografia quântica distribuída, que permite detectar irregularidades estatísticas nos estados quânticos ao comparar o estado ideal com o estado reconstruído, utilizando medições sincronizadas entre os nós da rede. Essa abordagem, embora eficaz, demanda recursos significativos e precisa ser cuidadosamente balanceada com a capacidade da rede.

Além dos danos diretos, o *Hijacking Attack* também permite ao invasor realizar ataques de dissimulação, incriminando repetidores inocentes. Ao alterar seletivamente

estados quânticos que serão analisados, o atacante pode induzir a rede a tomar ações incorretas, como a exclusão de nós legítimos ou a reconfiguração desnecessária da topologia. Esse tipo de manipulação pode reduzir o desempenho da rede e até causar a sua fragmentação. Estudos recentes demonstram que estratégias de seleção aleatória e criptograficamente segura de pares de Bell para verificação podem mitigar esses efeitos e dificultar a ação dos invasores [Satoh et al. 2018].

2.2. Black Hole Attack

O ataque *Black Hole Repeater* constitui uma ameaça crítica em redes quânticas, caracterizado por manipulações maliciosas no processo de *entanglement swapping*. O ataque impede a criação de pares EPR fim-a-fim, necessários para aplicações da Internet Quântica, ao introduzir erros deliberados durante as operações realizadas pelos repetidores. Esse comportamento compromete a integridade da rede, gerando falhas sistemáticas, desperdício de recursos e degradação do desempenho global.

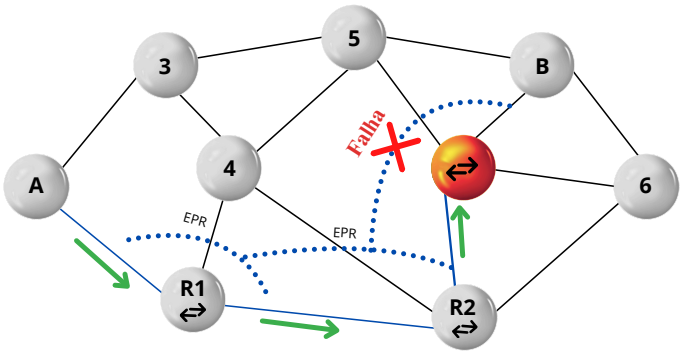


Figure 2. Ataque Black Hole bem sucedido

Em redes clássicas, o ataque *black hole* ocorre quando um nó malicioso intercepta e descarta pacotes de dados, desviando o tráfego para si e interrompendo a transmissão. Em redes quânticas, conforme ilustrado na Figura 2, o ataque *Black Hole Repeater* ocorre durante o processo de *entanglement swapping* realizado pelos repetidores quânticos. No exemplo apresentado, o nó A (Alice) inicia o processo de criação de um par EPR fim-a-fim com o nó B (Bob), utilizando os repetidores R_1 e R_2. Durante as operações de *swapping*, o repetidor R_2 realiza suas funções corretamente, criando EPR intermediários. O ataque acontece quando o repetidor comprometido (destacado em vermelho) introduz erros de operação, reduzindo a probabilidade de sucesso do *entanglement swapping*. Dependendo da intensidade do erro adicionado, ocorre a falha da criação do EPR intermediário. Essa manipulação maliciosa impede a criação do entrelaçamento fim-a-fim, invalidando o processo.

O impacto do ataque é agravado pelo fato de que os pares EPR já alocados nos enlaces da rota, como os gerados entre A e R_1, R_1 e R_2, e R_2 e B, são consumidos durante as etapas intermediárias de *swapping*. Assim, quando o ataque é executado, todos esses recursos são desperdiçados, sobrecarregando a gestão de recursos da rede e aumentando os atrasos para novas requisições. A falha introduzida pelo repetidor malicioso causa não apenas a interrupção do processo, mas também um impacto generalizado na eficiência e na disponibilidade de pares entrelaçados na rede.

3. Monitoramento e Detecção

O monitoramento em redes quânticas é essencial para garantir a confiabilidade, segurança e desempenho das comunicações. Para isso, métricas como fidelidade dos enlaces, capacidade efetiva da rede, quantidade de pares EPR e níveis de ruído são continuamente avaliadas. Essas informações são utilizadas tanto para o controle em tempo real quanto para a escolha de rotas e estratégias de correção de erros, impactando diretamente a qualidade das aplicações, como a distribuição de chaves ou o teleporte quântico. Entre as principais técnicas de monitoramento, destaca-se a Tomografia de Estado Quântico (QST), responsável por reconstruir a matriz densidade de um estado quântico com base em medições realizadas em múltiplas bases [Altepeter et al. 2005]. Essa reconstrução permite avaliar a fidelidade dos estados transmitidos, identificando desvios que possam indicar ruídos, falhas ou ataques. Já a Tomografia de Rede Quântica (QNT) atua em nível mais global, realizando medições nos nós finais da rede. Ao comparar os resultados observados com os dados esperados dos repetidores intermediários, a QNT permite verificar a consistência das métricas reportadas, mesmo sem acesso direto aos nós intermediários [Guedes de Andrade et al. 2024, De Andrade et al. 2022].

Essas técnicas são eficazes para detectar ataques como o *Hijacking Attack*, no qual um repetidor malicioso é sequestrado e manipula o roteamento ou os estados quânticos de forma ativa. Como descrito em [Satoh et al. 2018], o atacante pode alterar destinos de operações, modificar ou atrasar processos de *entanglement swapping*, ou até inserir qubits adicionais aos estados compartilhados. Tais ações impactam diretamente a fidelidade dos estados e podem ser detectadas pela QST ou QNT, desde que os pares de Bell utilizados para as medições sejam escolhidos de forma aleatória e criptograficamente segura, dificultando a camuflagem do atacante.

Entretanto, essas mesmas técnicas mostram-se ineficazes diante de ataques do tipo *Black Hole Repeater*. Neste cenário, o repetidor não interfere diretamente nas métricas observáveis, como fidelidade ou número de qubits transmitidos. Em vez disso, ele altera de forma sutil e precisa apenas o processo de *entanglement swapping*, impedindo que certos pares EPR sejam corretamente estabelecidos entre nós específicos, sem afetar as métricas globais. Como resultado, tanto a QST quanto a QNT continuam reportando valores normais, tornando o ataque praticamente invisível aos métodos tradicionais de detecção.

A diferença central entre os dois tipos de ataque está na natureza do desvio provocado. Enquanto o ataque de *Hijacking* corrompe os estados ou manipula informações de forma ampla e ativa — o que inevitavelmente altera os dados coletados nas tomografias —, o ataque *Black Hole* é projetado para ser passivo e seletivo. Esse comportamento o aproxima de falhas naturais da rede, exigindo técnicas complementares para sua identificação, como auditorias cruzadas entre repetidores, análise de padrões temporais com aprendizado de máquina e verificação independente de rotas e métricas. Assim, o monitoramento torna-se não apenas uma ferramenta de avaliação de desempenho, mas também um componente crítico na defesa contra ataques sofisticados.

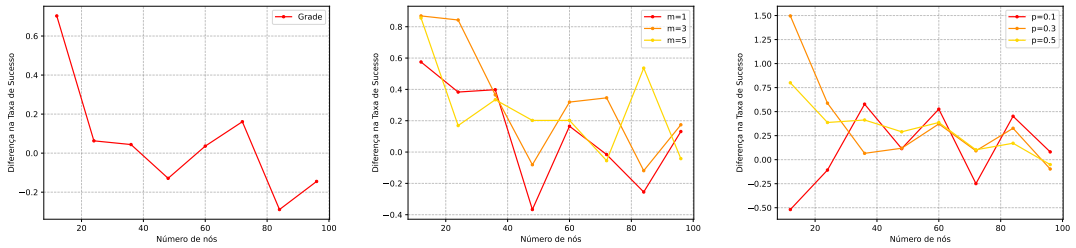
4. Estudo de Caso

Esta seção apresenta a modelagem e simulação do ataque *Black Hole Repeater* em redes quânticas. O objetivo é ilustrar seu funcionamento e caracterizar seus efeitos so-

bre métricas essenciais da rede, focalizando especificamente na taxa de sucesso das requisições. A intenção dos experimentos é evidenciar, de forma exploratória, como o ataque pode impactar negativamente a operação da rede mesmo quando os indicadores tradicionais aparentam normalidade. Os resultados obtidos não têm caráter conclusivo, mas servem para exemplificar a complexidade associada à detecção desse tipo de ataque.

A rede quântica foi modelada com suporte a requisições de criação de pares EPR fim a fim, com nós capazes de realizar *entanglement swapping*. Cada nó foi associado a probabilidades de sucesso tanto na geração de pares quanto na realização dos swaps. O ataque foi representado por repetidores que, ao serem comprometidos, deliberadamente falham nas operações de *entanglement swapping* quando há requisições provindas de um alvo específico, sem alterar diretamente outras métricas da rede.

As simulações foram realizadas em diferentes topologias, incluindo redes em grade com 12 nós e redes com até 100 nós, utilizando os modelos Barabási-Albert e Erdős-Rényi. As requisições foram roteadas utilizando o protocolo Dijkstra [Dijkstra 2022] que considera o menor caminho baseado em pesos, no caso, serão considerados a quantidade de saltos da rede. Os modelos escolhidos permitem representar diferentes estruturas de conectividade e analisar a atuação do ataque em cenários com graus variados de complexidade topológica e robustez estrutural. Sendo a diferença na taxa de sucesso dada pela fórmula: $T_s = T_p - T_a$. T_s é a diferença na taxa de sucesso, T_p é a taxa de sucesso média da rede padrão (sem ataque) e T_a representa a taxa de sucesso média de uma rede sob ataque.



(a) Topologia em Grade. (b) Topologia Barabási-Albert. (c) Topologia Erdõs-Rényi.

Figure 3. Impacto do ataque em diferentes topologias - ataque com alvo específico.

A intensidade do ataque foi ajustada com probabilidade constante de sucesso das operações de *entanglement swapping*, inicialmente configurada em 0.8. A variação do número de nós foi acompanhada da progressão dos nós maliciosos, a disposição percentual de *Black Holes* manteve-se em 20% dos nós totais da rede. Esse controle fino da quantidade de atacantes tenta sobrepor o efeito redutivo no ataque ao incrementar o número de rotas possíveis, pois o crescimento dos caminhos possíveis mitigam os danos gerados ao diminuírem o contato dos atacantes com os seus alvos.

Os gráficos resultantes ilustram o impacto do ataque sobre o desempenho da rede e a estabilidade das requisições. Observa-se que, mesmo sob condições degradadas, os indicadores globais — como fidelidade média e uso de recursos — podem permanecer dentro de faixas aceitáveis ou até vir a tornar-se irrelevante, como pode ser visto na figura 3(a) quando torna-se negativo por variações naturais da rede, o que exemplifica a dificuldade de detectar o ataque por meios tradicionais. Esses resultados reforçam a necessidade

de abordagens complementares de monitoramento e detecção, especialmente em redes quânticas sujeitas a atores maliciosos com conhecimento do funcionamento interno dos protocolos de roteamento e distribuição de entrelaçamento.

5. Conclusão

Este trabalho explorou as vulnerabilidades de redes baseadas em entrelaçamento quântico, com foco no *Quantum Black Hole Attack*, um tipo de ataque furtivo que compromete o processo de *entanglement swapping* sem alterar significativamente as métricas convencionais de monitoramento. Através da modelagem do ataque e de experimentos em uma topologia de rede em treliça, evidenciamos que os métodos tradicionais de detecção, baseados em tomografia de estado (QST) e tomografia de rede (QNT), podem falhar em identificar esse comportamento malicioso. Esses resultados reforçam o risco inerente à confiança irrestrita nos repetidores quânticos e ressaltam a necessidade de abordagens mais robustas e complementares de monitoramento em redes quânticas seguras.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pela Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), e pela 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.

References

Altepeter, J. B., Jeffrey, E. R., and Kwiat, P. G. (2005). Photonic state tomography. *Advances in atomic, molecular, and optical physics*, 52:105–159.

De Andrade, M. G., Diaz, J., Navas, J., Guha, S., Montaño, I., Smith, B., Raymer, M., and Towsley, D. (2022). Quantum network tomography with multi-party state distribution. In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 400–409. IEEE.

Dijkstra, E. W. (2022). A note on two problems in connexion with graphs. In *Edsger Wybe Dijkstra: his life, work, and legacy*, pages 287–290.

Guedes de Andrade, M., Navas, J., Guha, S., Montaño, I., Raymer, M., Smith, B., and Towsley, D. (2024). Quantum network tomography. *IEEE Network*, 38(5):114–122.

Satoh, T., Nagayama, S., Oka, T., and Van Meter, R. (2018). The network impact of hijacking a quantum repeater. *Quantum Science and Technology*, 3(3):034008.

Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M., and Van Meter, R. (2021). Attacking the quantum internet. *IEEE Transactions on Quantum Engineering*, 2:1–17.

Suzuki, S. and Van Meter, R. (2015). Classification of quantum repeater attacks. In *Proc. NDSS Workshop on Security of Emerging Technologies*.

Yuen, H. P. (2016). Security of quantum key distribution. *IEEE Access*, 4:724–749.

Zangi, S. M., Shukla, C., Ur Rahman, A., and Zheng, B. (2023). Entanglement swapping and swapped entanglement. *Entropy*, 25(3):415.