Redes Quânticas Sob Ataque: Black Hole Repeaters

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

[1] Universidade Federal do Pará - UFPA

Abstract. *Quantum networks promise unparalleled security by leveraging entanglement-based protocols and trusted quantum repeaters to enable applications such as quantum key distribution and distributed quantum computing. However, as these networks evolve in complexity, they expose new operational and control vulnerabilities that can be exploited by adversaries. Among these vulnerabilities, subtle attacks on the entanglement swapping process and manipulating performance metrics pose significant challenges to network integrity and efficiency. This study delves into a relatively unexplored class of threats: the Black Hole Repeater attacks. These attacks involve malicious nodes deliberately introducing errors or falsifying metrics that undermine the success rate of quantum operations and lead to resource inefficiencies while remaining undetectable by traditional monitoring techniques such as quantum tomography. Through simulations in diverse network topologies, we demonstrate the potential impact of these attacks on key performance metrics, underscoring the need for adaptive monitoring solutions and resilient architectures to enhance the security of quantum networks.*

Resumo. *As redes quânticas oferecem uma segurança sem precedentes ao utilizarem protocolos baseados em entrelaçamento e repetidores quânticos confiáveis para viabilizar aplicações como distribuição de chaves quânticas e computação quântica distribuída. Contudo, à medida que essas redes evoluem, novas vulnerabilidades operacionais e de controle emergem, podendo ser exploradas por adversários. Entre essas vulnerabilidades, destacam-se ataques sutis ao processo de troca de entrelaçamento e a manipulação de métricas de desempenho, que representam desafios significativos para a integridade e a eficiência das redes. Este estudo explora uma classe relativamente pouco investigada de ameaças: os ataques Black Hole Repeater. Esses ataques envolvem nós maliciosos que deliberadamente introduzem erros ou falsificam métricas, comprometendo a taxa de sucesso das operações quânticas e gerando ineficiências no uso de recursos, ao mesmo tempo que permanecem indetectáveis por técnicas tradicionais de monitoramento, como a tomografia quântica. Por meio de simulações realizadas em diversas topologias de rede, demonstra-se o impacto potencial desses ataques em métricas-chave de desempenho, destacando a necessidade de soluções adaptativas de monitoramento e arquiteturas resilientes para aprimorar a segurança das redes quânticas.*

1. Introdução

A Comunicação Quântica promete transformar a segurança das redes de comunicações ao introduzir garantias baseadas nos princípios de superposição e entrelaçamento quântico [Azuma et al. 2023]. Protocolos baseados nesses princípios, como a Distribuição

Quântica de Chaves (*Quantum Key Distribution* - QKD) e a distribuição de informação quântica através do protocolo de teletransporte quântico, oferecem segurança fisicamente garantida, tornando-se uma alternativa atraente frente às vulnerabilidades da criptografia clássica, especialmente em face de adversários com acesso a computadores quânticos [Wehner et al. 2018]. No entanto, embora esses sistemas sejam quanticamente seguros, surgem desafios significativos quando analisamos ataques que exploram os elementos operacionais e de controle da rede quântica [Satoh et al. 2021].

A crescente complexidade das redes quânticas, especialmente aquelas baseadas em entrelaçamento, expõe um conjunto de novas vulnerabilidades [Suzuki and Van Meter 2015]. Operações como *entanglement swapping* (troca de entrelaçamento) dependem coordenação entre os repetidores quânticos para criar pares entrelaçados entre nós distantes [Zangi et al. 2023]. Entretanto, repetidores maliciosos podem comprometer a operação, ao manipular características internas do dispositivo e o controle clássico do mesmo. Esses cenários adversos, embora discutidos de forma preliminar em trabalhos anteriores [Satoh et al. 2018, Suzuki and Van Meter 2015], carecem de análises detalhadas que considerem o impacto em métricas críticas da rede e o contexto operacional, em frente às características dos repetidores e as abordagens atuais de monitoramento das redes quânticas [Guedes de Andrade et al. 2024].

Este artigo discute os ataques conhecidos como *Black Hole Repeaters* no contexto das redes quânticas. Esses ataques envolvem repetidores quânticos comprometidos que manipulam maliciosamente o processo de *entanglement swapping*, introduzindo erros ou fornecendo informações falsas sobre métricas de desempenho. Como resultado, esses repetidores criam falhas sistemáticas na criação de enlaces entrelaçados, comprometendo a integridade e a eficiência da rede de forma sutil e difícil de detectar. Para o melhor de nosso conhecimento, este é o primeiro estudo a analisar de forma detalhada os *Black Hole Repeaters* em redes quânticas. Embora a comunicação quântica garanta proteção dos dados transmitidos em nível físico, demonstra-se que falhas no controle operacional da rede podem ser exploradas para comprometer a funcionalidade e a eficiência do sistema, reduzindo a capacidade de atendimento das requisições da rede.

As principais contribuições deste trabalho incluem a modelagem e análise detalhada dos ataques *Black Hole Repeaters*, a avaliação do impacto desses ataques em métricas críticas de desempenho, considerando diferentes cenários e topologias de rede, e a discussão sobre a dificuldade de detecção desses ataques e suas implicações para o monitoramento e a resiliência das redes quânticas. Este artigo está estruturado da seguinte forma. Na Seção 2, é apresentada a fundamentação teórica sobre redes quânticas e mecanismos de *entanglement swapping*. A Seção 3 aborda os trabalhos relacionados, destacando os avanços e lacunas existentes. Na Seção 4, são descritos o modelo de ameaça e os cenários de ataque. Os experimentos realizados e os resultados obtidos são apresentados na Seção 5. Por fim, a Seção 6 apresenta as conclusões do trabalho, apontando direções para pesquisas futuras.

2. Fundamentação Teórica

Nesta seção, são apresentados os fundamentos teóricos que embasam o trabalho, abordando o funcionamento das redes quânticas, com ênfase no protocolo de *entanglement swapping*. Em seguida, discute-se o monitoramento das redes quânticas, destacando as

principais técnicas atuais utilizadas para verificar as métricas coletadas, bem como suas limitações frente a ataques como o *Black Hole Repeater*.

2.1. Funcionamento das Redes Quânticas

As redes quânticas são formadas por nós quânticos interligados por canais de comunicação, que possibilitam a transmissão de qubits e a criação de entrelaçamento quântico entre diferentes partes da rede [Jiang et al. 2024]. O principal objetivo desses sistemas é viabilizar aplicações como teletransporte de estados quânticos, distribuição de chaves quânticas e computação quântica distribuída [Wehner et al. 2018]. Diferentemente das redes clássicas, as redes quânticas exploram as propriedades fundamentais da mecânica quântica, como a superposição e o entrelaçamento, proporcionando vantagens em segurança e eficiência.

Em enlaces quânticos, pares entrelaçados são gerados localmente através de mecanismos de criação de entrelaçamento. No entanto, devido à atenuação em canais físicos, como fibras ópticas, a fidelidade (métrica que reflete a qualidade) do entrelaçamento diminui à medida que a distância aumenta [Azuma et al. 2023]. Isso inviabiliza a comunicação direta entre nós distantes, tornando necessário o uso de repetidores quânticos. Os repetidores possibilitam a conexão de enlaces menores e a extensão do entrelaçamento por meio de operações conhecidas como *entanglement swapping* [Salimian et al. 2023].

O *entanglement swapping* é um processo fundamental que permite o estabelecimento de entrelaçamento entre nós distantes utilizando nós intermediários. Esse procedimento depende de medições de estado de Bell (*Bell State Measurements - BSM*), realizadas nos repetidores quânticos. Durante o processo, dois pares entrelaçados (EPRs) independentes são combinados em um nó intermediário, realizando uma medição de Bell que transfere o entrelaçamento para os nós finais [Mastriani 2023]. Assim, o entrelaçamento pode ser estendido gradualmente ao longo de múltiplos enlaces.

A Figura 1 ilustra o processo sequencial de *entanglement swapping*. No instante t_0, pares entrelaçados são estabelecidos localmente entre os nós adjacentes: Alice e R_1, R_1 e R_2, R_2 e R_3, e R_3 e Bob. No instante t_1, ocorre o primeiro *entanglement swapping* no nó R_1, criando um enlace virtual entre Alice e R_2. O processo continua no instante t_2, onde ocorre um novo *entanglement swapping* no nó R_2, estendendo o enlace virtual até R_3. Finalmente, no instante t_3, um último *entanglement swapping* no nó R_3 conecta Alice e Bob, criando um enlace fim a fim entre os dois nós. Esse procedimento demonstra como o entrelaçamento é estendido progressivamente por meio de nós intermediários.

Embora o *entanglement swapping* permita a extensão do entrelaçamento, ele requer um nível significativo de confiança entre os nós repetidores. Essa confiança é necessária porque as medições *BSM* realizadas nos nós intermediários dependem de dispositivos precisos e de um controle rigoroso das operações. O sucesso do *entanglement swapping* é representado pela probabilidade P_{swap}, que depende da qualidade inicial dos pares entrelaçados e da eficiência dos dispositivos dos nós repetidores. Um repetidor comprometido pode introduzir erros no processo, reduzir a fidelidade dos enlaces ou até mesmo falsificar métricas operacionais, como a probabilidade de sucesso P_{swap}. Esses erros afetam diretamente o desempenho da rede e a qualidade do entrelaçamento fim a fim, destacando a necessidade de monitoramento robusto e de protocolos de verificação. Para garantir a confiabilidade do processo, os repetidores devem compartilhar informações so-

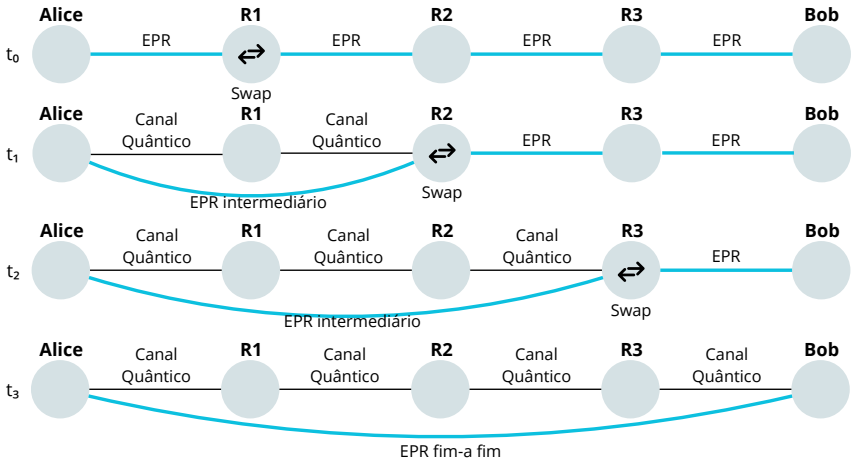


Figura 1. Processo sequencial de *entanglement swapping*. O entrelaçamento é estabelecido entre Alice e Bob por meio de operações realizadas em nós intermediários (repetidores quânticos).

bre a qualidade dos enlaces e reportar métricas precisas ao controlador da rede ou aos nós vizinhos em um cenário distribuído.

2.2. Monitoramento da Rede Quântica

O monitoramento em redes quânticas é fundamental para garantir o desempenho, a segurança e a confiabilidade das operações. Esse processo envolve a coleta e verificação de métricas essenciais, como a fidelidade dos enlaces, a fidelidade média das rotas utilizadas, a quantidade de pares EPR disponíveis ou consumidos em cada requisição, a capacidade efetiva da rede e os níveis de ruído presentes nos canais quânticos [Chehimi and Saad 2022]. A precisão dessas informações é indispensável para o controle e tomada de decisões nos nós da rede, sendo particularmente crítica em aplicações que demandam alta performance [Gyongyosi and Imre 2020].

Uma das principais técnicas utilizadas no monitoramento é a tomografia de estados quânticos (*Quantum State Tomography* - QST) [Altepeter et al. 2005]. A QST permite reconstruir a matriz densidade dos estados quânticos distribuídos entre os nós, possibilitando a avaliação da fidelidade, que quantifica o quão próximo o estado real está do estado ideal. A fidelidade é calculada com base na comparação entre o estado puro ideal, e o estado reconstruído a partir das medições tomográficas. Desvios significativos na fidelidade podem indicar a presença de ruídos, perdas ou alterações indesejadas nos estados distribuídos, comprometendo a qualidade dos enlaces e, consequentemente, o desempenho das aplicações que dependem do entrelaçamento.

A tomografia de redes quânticas (*Quantum Network Tomography* - QNT) [Guedes de Andrade et al. 2024] amplia essa abordagem ao nível da rede inteira. A QNT realiza medições exclusivamente nos nós finais, sem a necessidade de acessar diretamente os repetidores intermediários, o que a torna uma ferramenta eficiente para verificar a capacidade real dos enlaces e estimar os níveis de ruído. Comparando as métricas observadas, como a fidelidade média dos pares EPR e a capacidade efetiva dos enlaces, com as informações reportadas pelos nós intermediários, a QNT permite validar a consistência dos dados e identificar discrepâncias que possam comprometer a confiabilidade da rede

[De Andrade et al. 2022].

O monitoramento dessas métricas também desempenha um papel crucial na operação regular da rede. Quando um nó participante deseja iniciar uma aplicação, como a distribuição de chaves quânticas, ele precisa coordenar o estabelecimento de uma rota até o nó de destino. Esse processo, que pode ser gerenciado de forma centralizada ou de forma distribuída, depende das informações coletadas durante o monitoramento, como a capacidade dos enlaces e a qualidade dos pares EPR disponíveis. Essas informações embasam a tomada de decisões, como a escolha da melhor rota e de quais operações serão necessárias para o estabelecimento do EPR fim a fim. Assim, a eficiência da rede é diretamente influenciada pela qualidade e confiabilidade das informações coletadas.

3. Trabalhos Relacionados

Os avanços recentes em redes quânticas ressaltam seu potencial para comunicações seguras e eficientes, baseadas em protocolos de entrelaçamento e repetidores quânticos confiáveis. No entanto, esses avanços também trazem novos desafios, como vulnerabilidades operacionais e de controle que podem comprometer a segurança e a integridade das redes. A literatura aborda essas questões sob diversas perspectivas, desde trabalhos que focam em vulnerabilidade de protocolos específicos como o QKD [Jain et al. 2016], como uma análise mais geral acerca dos vetores de ataques possíveis nas comunicações quânticas [Satoh et al. 2021]. Nesta seção são destacados os trabalhos que focam em redes de entrelaçamento e as vulnerabilidades em repetidores quânticos.

Suzuki e Van Meter [Suzuki and Van Meter 2015] propõem uma taxonomia específica de ataques, destacando como os componentes clássicos de controle operacional dos repetidores podem comprometer o desempenho da rede. Os ataques *Black Hole Repeaters* são citados como uma potencial vulnerabilidade, porém não é feito nenhuma análise acerca desses ataques. Porém, a pespectiva de explorar o controle clássico dos repetidores é expandida por Satoh et al. [Satoh et al. 2018], que investiga ataques de sequestro de repetidores (*hijacking*), nos quais repetidores sequestrados modificam os estados quânticos distribuídos, gerando estados mistos em vez de pares de EPR ideais. Isso faz com que o EPR fim a fim seja direcionado para outro nó (que pode ser o atacante ou não) diferente do nó de destino, o qual poderá receber a informação quântica a ser transmitida pelo processo de teletransporte quântico. A detecção desses ataques é feita com processos de QNT periódicos, os quais são capazes de verificar se os pares EPRs foram distribuídos corretamente.

No entanto, mesmo quando apenas uma fração dos repetidores está comprometida e ainda não detectados, os ataques podem degradar significativamente o desempenho da rede. Harkness et al. [Harkness et al. 2024] analisam cadeias de repetidores parcialmente comprometidas, concentrando-se em cenários onde adversários controlam um subconjunto contíguo de repetidores. Os autores demonstram como atacantes podem explorar ruídos internos e limitações nos mecanismos de monitoramento para degradar o desempenho da aplicação QKD. Embora a detecção do ataque seja possível usando o próprio protocolo QKD, como os autores demonstram, ela exige o uso de recursos adicionais na rede, o que, pode criar uma vulnerabilidade adicional ao sobrecarregar a infraestrutura e ampliar o impacto adverso.

Apesar dessas contribuições, os ataques de *Black Hole Repeaters* representam uma

ameaça relativamente inexplorada. Esse tipo de ataque, que manipula de forma sutil e probabilística o processo de *entanglement swapping*, é particularmente desafiador devido à dificuldade de detecção por métodos tradicionais, como QST e QNT. Em contraste, este artigo foca em uma análise específica e aprofundada dos ataques *Black Hole Repeaters*, destacando suas características únicas e a necessidade de mecanismos mais robustos de monitoramento e mitigação. Ao oferecer uma visão detalhada de um problema ainda pouco abordado, este trabalho contribui para a compreensão das vulnerabilidades operacionais das redes quânticas e abre caminho para o desenvolvimento de soluções mais resilientes e seguras.

4. Ataque Black Hole Repeater

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.

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. A Figura 2 ilustra esse cenário, onde o atacante atua como um ponto de absorção, afetando diretamente a disponibilidade da rede e o tempo de resposta de aplicações críticas. Medidas como redundância de rotas e algoritmos de detecção de anomalias são amplamente utilizadas para mitigar tais ataques em redes tradicionais.

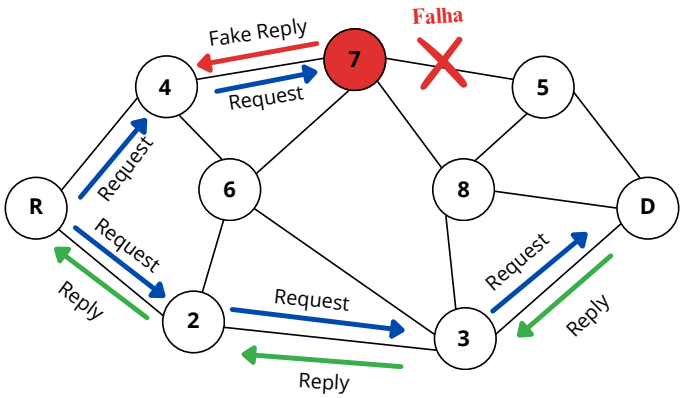


Figura 2. Ataque *Black Hole* em uma Rede Clássica.

Em redes quânticas, conforme ilustrado na Figura 3, 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

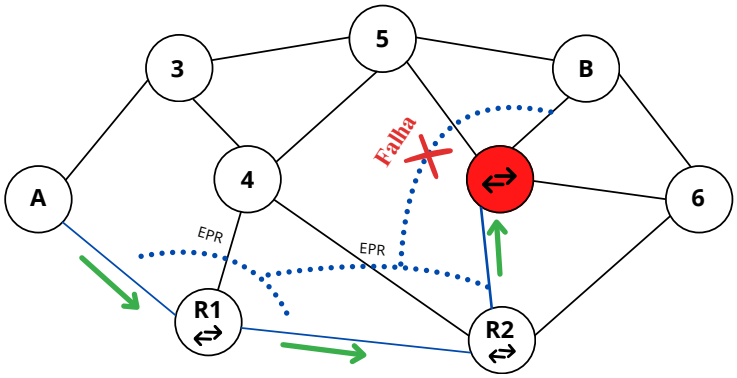


Figura 3. Ataque *Black Hole* em uma Rede Quântica.

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.

4.1. Modelo da Ameaça

Neste trabalho, consideramos um modelo de ameaça no qual um adversário controla um subconjunto dos repetidores quânticos da rede. Esses repetidores maliciosos podem manipular o processo de *entanglement swapping*, degradando deliberadamente a probabilidade de sucesso das operações ou reportando informações falsas sobre métricas de desempenho. O objetivo do adversário é prejudicar o funcionamento da rede, impactando sua eficiência, confiabilidade e o consumo de recursos.

Em condições normais, o sucesso do *entanglement swapping* depende diretamente da fidelidade dos pares entrelaçados e da eficiência dos repetidores utilizados. Contudo, em um cenário de ataque, um repetidor comprometido pode introduzir erros de maneira controlada, falhando propositalmente em realizar as operações necessárias para o estabelecimento do Par EPR fim a fim. Ao reduzir a probabilidade de sucesso, o atacante aumenta o número de operações mal-sucedidas, causando desperdício de qubits e de pares EPR, além de atrasar significativamente a conclusão das requisições.

Além de introduzir falhas operacionais, o repetidor malicioso pode também reportar informações incorretas sobre o desempenho das operações. Mesmo que uma operação de *entanglement swapping* tenha sido bem-sucedida, o repetidor pode anunciar falsamente que o processo falhou ou que a fidelidade do EPR criado é inferior à mínima necessária. Esse comportamento induz os sistemas de controle (ou os nós vizinhos em redes distribuídas) ao erro, fazendo com que sejam tomadas decisões equivocadas, como o redirecionamento de recursos para rotas menos eficientes ou a invalidação desnecessária de enlaces quânticos funcionais.

A intensidade do ataque pode ser ajustada por meio da adição progressiva de er-

ros ao processo de *entanglement swapping*, reduzindo proporcionalmente o P_{swap}. Por exemplo, se a probabilidade regular de sucesso em um enlace da rede é 0.6 (indicando que 60% das operações ocorrem com êxito), um ataque pode introduzir um incremento de 10% na taxa de erro a cada unidade de intensidade. Com intensidade 0.2, o P_{swap} seria reduzido para 40%. Essa abordagem permite ao atacante modular o impacto do ataque, evitando se destacar do comportamento esperado da rede. No entanto, quanto maior a intensidade aplicada, mais efetivo será o ataque, embora também aumente a probabilidade de detecção.

4.2. Modos de Funcionamento do Ataque

As ações do adversário podem ser aplicadas de duas formas principais. Em ataques sem alvo específico, o repetidor malicioso introduz falhas em todas as requisições de *entanglement swapping* que recebe, sem distinção do nó de origem da requisição. Em contrapartida, em ataques com alvo específico, o repetidor identifica requisições associadas a alvos específicos, e aplica suas manipulações apenas nesses casos. Isso permite que o atacante foque em nós específicos da rede. Dessa forma, o atacante maximiza o impacto do ataque, ao mesmo tempo em que mantém um comportamento regular em outras requisições.

Outra variação possível desse ataque envolve a manipulação das métricas reportadas pelo repetidor, como a fidelidade média dos enlaces ou a quantidade de pares EPR disponíveis. Ao fornecer informações falsas, o repetidor pode atrair rotas para si, tornando-se nó de preferência para as operações de *entanglement swapping*. Esse comportamento não apenas amplifica o impacto do ataque, mas também compromete a eficiência geral da rede. Apesar de ser uma ameaça relevante, ataques baseados na manipulação de métricas poderiam ser mais facilmente detectados por técnicas como QST e QNT. Essas técnicas podem verificar se a fidelidade reportada é condizente com o enlace e se a quantidade de pares EPRs é real.

Por outro lado, quando o ataque *Black Hole Repeater* é realizado exclusivamente por meio de alterações nas operações de *entanglement swapping*, ele se torna indetectável pelas técnicas de tomografia, já que a fidelidade média do canal permanece inalterada e a quantidade de qubits ou pares EPR não é diretamente impactada pela ação do atacante. Mesmo que esses parâmetros sejam verificados, eles apresentarão valores consistentes com o esperado tanto pelo QST quanto pelo QNT, dificultando significativamente a identificação do ataque.

4.3. Ataque, Falha ou Anomalia

Os ataques do tipo *Black Hole Repeater* diferenciam-se de falhas naturais ou anomalias em redes quânticas, apesar de ambos impactarem o processo de *entanglement swapping*. Enquanto falhas naturais geralmente decorrem de ruídos ou limitações operacionais e podem ser identificadas por técnicas de monitoramento como QST e QNT, ataques são projetados para emular esses ruídos de forma deliberada e sutil, dificultando sua detecção. Por exemplo, repetidores maliciosos podem manipular o *entanglement swapping*, introduzindo erros que não afetam diretamente métricas como fidelidade ou quantidade de qubits, tornando-se indetectáveis pelos métodos tradicionais. Para diferenciar esses ataques de falhas ou anomalias, é necessário adotar abordagens complementares. Um possível caminho seria uma validação cruzada entre repetidores, detecção de padrões atípicos por meio de Aprendizado de Máquina e auditorias detalhadas dos dispositivos envolvidos.

5. Experimentos e Resultados

Esta seção apresenta os experimentos realizados com os ataques *Black Hole Repeaters*. Os experimentos realizados neste estudo têm como objetivo avaliar os impactos dos ataques *Black Hole Repeaters* em diferentes cenários e topologias de redes quânticas. A análise inclui a taxa de sucesso das requisições, o consumo de pares entrelaçados e a fidelidade média das rotas utilizadas, considerando tanto ataques sem alvo específico quanto ataques direcionados. Os resultados são apresentados e discutidos nas subseções a seguir.

5.1. Configuração dos Experimentos

Para avaliar o impacto dos ataques *Black Hole Repeaters*, foi modelada uma rede quântica onde foram simuladas requisições para a criação de pares EPR fim a fim. Cada nó da rede foi associado a uma probabilidade de sucesso tanto na criação de pares entrelaçados quanto na realização do *entanglement swapping*. Os ataques foram representados como alterações dessas probabilidades em nós maliciosos, que induzem falhas deliberadas nos processos de *entanglement swapping*, afetando diretamente as rotas selecionadas para atender às requisições de criação de EPR fim a fim. Embora existam simuladores para redes quânticas [Abreu et al. 2024], nenhuma solução atual contempla a ação maliciosa dos repetidores como necessária para este experimento. Os experimentos realizados, juntamente com a modelagem detalhada da rede, estão disponíveis no repositório associado ao artigo[1].

Foram considerados dois cenários distintos. No primeiro, os ataques foram realizados de forma não-direcionada, com repetidores maliciosos introduzindo falhas em todas as requisições de *entanglement swapping* das quais participavam. No segundo cenário, os ataques foram direcionados a alvos específicos, escolhidos aleatoriamente em cada simulação. A rede quântica foi modelada com a topologia em grade, com 12 nós, todos capazes de realizar *entanglement swapping* e de enviar ou receber requisições de criação de pares EPR fim a fim. Para cada requisição, a rota foi definida utilizando o protocolo qDijkstra [Van Meter et al. 2013], que seleciona as rotas pelo menor caminho. Além disso, foram modeladas outras topologias, contendo até 100 nós, utilizando as topologias de grafos aleatórios Barabási-Albert e Erdõs-Rényi. Essa abordagem visou avaliar tanto a escalabilidade do ataque em redes de topologias complexas quanto o impacto nas principais métricas de desempenho da rede. As topologias Barabási-Albert e Erdõs-Rényi permitem representar redes com características complementares: a primeira destaca hubs altamente conectados e robustez contra falhas aleatórias, enquanto a segunda modela conexões probabilísticas com menor redundância estrutural e maior uniformidade.

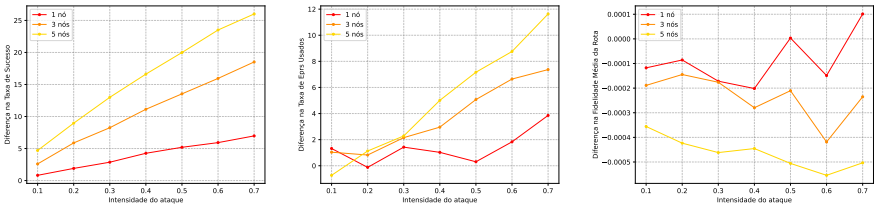
A intensidade do ataque, conforme descrito na Seção 4.1, é ajustada por meio da adição progressiva de erros ao processo de *entanglement swapping*, reduzindo proporcionalmente o P_{swap}. Nos experimentos, o P_{swap} inicial da rede foi configurado em 0.8, permitindo que a intensidade do ataque seja ajustada entre 0.1 e 0.7. Essa variação possibilita avaliar diferentes níveis de impacto na rede, desde cenários com interferência sutil até situações com degradação significativa no desempenho.

5.2. Impacto da Intensidade dos Ataques na Rede

Os impactos dos ataques *Black Hole Repeaters* foram avaliados em cenários de ataques com e sem alvo específico. As Figuras 4 e 5 ilustram o impacto desses ataques em mé-

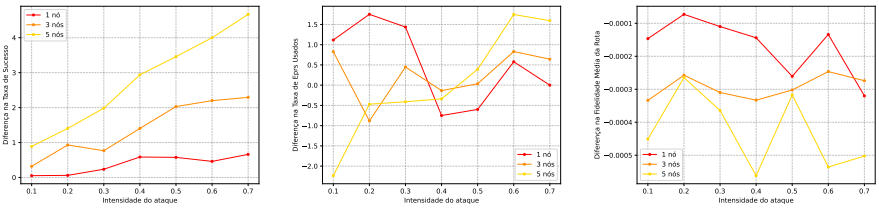
[1] `https://github.com/quantumgercom/Black-Hole-Quantum-Attack.git`

tricas como a taxa de sucesso das requisições, o consumo de pares EPRs e a fidelidade média das rotas. Os resultados levam em consideração a operação da rede com um número variado de atacantes (1,3 e 5 nós atacantes) comparando com o cenário sem ataque. Assim, é apresentado a diferença em cada métrica com a presença dos ataques.



(a) Taxa de Sucesso. (b) Consumo de EPRs. (c) Fidelidade Média.

Figura 4. Impacto da intensidade do ataque nas métricas da rede - ataque sem alvo específico.



(a) Taxa de Sucesso. (b) Consumo de EPRs. (c) Fidelidade Média.

Figura 5. Impacto da intensidade do ataque nas métricas da rede - ataque com alvo específico.

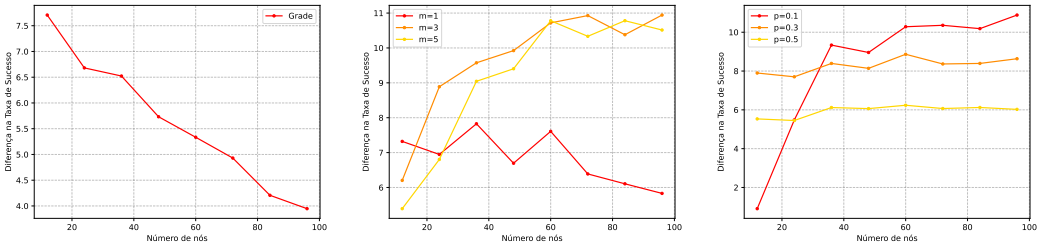
Na Figura 4, que apresenta os resultados para ataques sem alvo específico, observa-se que a intensidade do ataque tem uma relação direta com a diminuição da diferença na taxa de sucesso das requisições (Figura 4(a)). À medida que a intensidade aumenta, a diferença na taxa de sucesso entre os cenários com e sem ataque também cresce, indicando que as operações se tornam mais propensas a falhas e que o ataque está sendo efetivo. Por outro lado, o consumo de pares entrelaçados (Figura 4(b)) apresenta uma variação menos significativa. Já a fidelidade média das rotas (Figura 4(c)), apresenta pequenas variações. Isso se deve às características do ataque *Black Hole Repeater*, o qual não altera o valor da fidelidade dos pares EPRs, dificultando a sua descoberta por técnicas de tomografia.

No caso dos ataques com alvo específico (Figura 5), os resultados indicam que a diferença na Taxa de Sucesso (Figura 5(a)) aumenta com a intensidade do ataque. Contudo, como apenas as requisições específicas são afetadas, essa diferença é menos acentuada em comparação com os ataques sem alvo específico (Figura 4(a)). Da mesma forma, o impacto no consumo de pares EPR (Figura 5(b)) também se revela menos significativo, enquanto a fidelidade média das rotas (Figura 5(c)) prossegue não sendo afetada pelo ataque. Esses resultados evidenciam a sutileza do ataque *Black Hole Repeater*, tornando sua detecção especialmente desafiadora.

5.3. Análise dos ataques em diferentes topologias

A resiliência a ataques *Black Hole Repeaters* foi avaliada em diferentes topologias de rede, considerando como a estrutura da rede influencia o impacto dos ataques. Foram investigadas três topologias distintas: redes em grade, Barabási-Albert (BA) e Erdős-Rényi (ER), em cenários de ataques sem alvo específico e com alvo específico. Nessas análises, o número de ataques foi ajustado para 20% do total de nós (n), com uma intensidade de ataque de 0.4. Esse cenário permite avaliar como o ataque se comporta mesmo em redes de tamanhos crescentes, mantendo o número relativo de atacantes constante.

As topologias Barabási-Albert e Erdős-Rényi foram configuradas com parâmetros que determinam suas características estruturais. No modelo Barabási-Albert, o parâmetro m define o número de arestas que cada novo nó adiciona à rede durante o processo de construção. Um valor maior de m cria redes com hubs mais conectados, aumentando a redundância estrutural. Já no modelo Erdős-Rényi, o parâmetro p representa a probabilidade de existência de uma aresta entre dois nós quaisquer. Valores maiores de p geram redes mais densas e conectadas, enquanto valores menores resultam em redes esparsas.



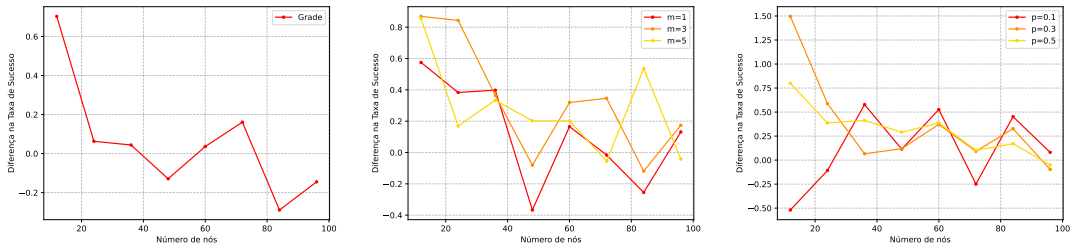
(a) Topologia em Grade. (b) Topologia Barabási-Albert. (c) Topologia Erdõs-Rényi.

Figura 6. Impacto do ataque em diferentes topologias - ataque sem alvo específico.

Na Figura 6, os resultados evidenciam o impacto dos ataques sem alvo específico. As topologias em grade (Figura 6(a)) apresentaram uma redução na diferença entre os cenários com e sem ataque. Esse comportamento é causado pelo aumento do tamanho médio das rotas à medida que o número de nós cresce, o que resulta em taxas de sucesso relativamente baixas tanto para redes atacadas quanto para as não atacadas, reduzindo assim a discrepância observada entre os dois cenários.

Em contrapartida, nas redes Barabási-Albert (Figura 6(b)), a diferença na taxa de sucesso tende a aumentar com o número de nós. Essa topologia é caracterizada pela presença de hubs, que podem ser utilizados para distribuir as rotas e minimizar os efeitos dos ataques. No entanto, quando o parâmetro m=1, a taxa de sucesso é naturalmente reduzida, dificultando uma avaliação mais precisa do desempenho. Esse efeito decorre da sobrecarga dos nós centrais, que possuem alta taxa de conexões e têm seus pares entrelaçados rapidamente exauridos, impossibilitando novas requisições de *entanglement swapping*. Além disso, o aumento no tamanho médio das rotas contribui para essa redução de eficiência. Esse cenário muda quando o fator m é aumentado, já que a maior redundância das conexões permite uma redistribuição mais eficiente das rotas e uma redução no tamanho médio das mesmas, mitigando o impacto dos ataques.

De forma semelhante às redes Barabási-Albert, as topologias Erdős–Rényi (Figura 6(c)) apresentaram um comportamento similar, mas com peculiaridades importantes. Devido à sua natureza probabilística, essas redes podem apresentar nós sem conexões, especialmente quando o parâmetro p é muito baixo. Esse comportamento é claramente evidenciado em cenários onde p e o número de nós são menores, reduzindo o número de rotas válidas e resultando em uma diferença menos pronunciada entre os cenários com e sem ataque, como observado na linha $p = 0.1$. Entretanto, conforme o número de nós aumenta, o impacto do fator p se torna mais evidente, uma vez que a baixa redundância nas rotas aumenta a probabilidade de que elas passem por nós maliciosos, amplificando o efeito dos ataques.



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

Figura 7. Impacto do ataque em diferentes topologias - ataque com alvo específico.

A Figura 7 mostra que, em todas as topologias analisadas, a variação na taxa de sucesso foi muito pequena e diminuiu com o aumento do número de nós. Esse comportamento indica que os impactos dos ataques *Black Hole Repeaters* não são facilmente distinguíveis dos erros naturais da rede, tornando o monitoramento dessa métrica pouco eficaz para a detecção desses ataques. Além disso, mesmo com um número proporcional de ataques, a semelhança entre os efeitos do ataque e os ruídos naturais reforça a dificuldade de identificação, destacando a necessidade de métodos mais avançados e direcionados para enfrentar essa ameaça.

5.4. Discussão dos Resultados

Os resultados obtidos neste estudo demonstram que os ataques *Black Hole Repeaters* têm um impacto significativo na taxa de sucesso das requisições, comprometendo a eficiência das operações da rede. Ao mesmo tempo, os ataques têm impacto pouco significativo nas métricas de fidelidade e quantidade de EPRs, as quais podem ser coletadas no monitoramento da rede. Isso ilustra a dificuldade de detecção dos ataques pelas técnicas tradicionais, como QST e QNT.

Com a redução da taxa de sucesso das requisições, seria esperado que o sistema tentasse mitigar o problema por meio de técnicas tradicionais, como a tomografia quântica. No entanto, os resultados mostram que essas técnicas não identificam variações nos repetidores atacantes. Nesse cenário, o sistema pode interpretar erroneamente que a capacidade da rede como um todo foi reduzida, levando-o a adotar medidas inadequadas.

Uma das respostas mais prováveis seria a alocação de recursos adicionais por requisição, como a tentativa de criar múltiplos pares EPR fim a fim para compensar a

aparente queda na eficiência. Essa abordagem agrava ainda mais os danos causados pelo ataque, sobrecarregando a rede, aumentando o consumo de qubits e degradando a capacidade geral de atender novas requisições. Esses resultados evidenciam a necessidade de desenvolver novas estratégias de monitoramento capazes de distinguir erros naturais de comportamentos maliciosos em redes quânticas.

6. Conclusão e Trabalhos Futuros

Neste trabalho, foi analisado o impacto dos ataques *Black Hole Repeaters* em redes quânticas, uma ameaça que explora vulnerabilidades operacionais e de controle em repetidores quânticos. Os resultados demonstraram que tanto ataques direcionados quanto não direcionados podem comprometer significativamente o desempenho das redes, reduzindo a taxa de sucesso das requisições. No entanto, esses ataques são especialmente desafiadores de detectar, pois seus efeitos frequentemente se assemelham aos erros naturais da rede, dificultando a identificação com métodos de monitoramento tradicionais.

Como trabalhos futuros, sugere-se o desenvolvimento de contramedidas que possam mitigar de maneira eficiente os impactos dos ataques *Black Hole Repeaters*. Técnicas baseadas em Aprendizado de Máquina, como modelos de detecção de anomalias, podem ser exploradas para identificar padrões atípicos nas métricas operacionais das redes quânticas. Além disso, a implementação de monitoramento distribuído, com validação cruzada das métricas reportadas por repetidores intermediários, pode aumentar a resiliência contra comportamentos maliciosos.

Além disso sugere-se o desenvolvimento de métodos para verificar as propriedades internas dos repetidores, incluindo avaliações de hardware e auditorias de segurança física. Essas medidas podem garantir que dispositivos comprometidos sejam identificados antes de entrarem em operação. Complementarmente, a implementação prática dos ataques em redes experimentais será essencial para validar modelos teóricos e compreender melhor suas características em condições reais. Essa análise experimental poderá fornecer informações para o design de arquiteturas e protocolos mais robustos, possibilitando maior segurança e confiabilidade para redes quânticas futuras.

Disponibilidade de Artefatos

Os artefatos estão disponíveis no repositório referente ao artigo [2].

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.

Referências

Abreu, D., Pimentel, A., Moraes, P., Tavares, D., Veloso, A., and Abelém, A. (2024). Multipurpose quantum network simulators: A comparative study. In *Workshop de Redes Quânticas*, pages 25–30. SBC.

[2]https://github.com/quantumgercom/Black-Hole-Quantum-Attack.git

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

Azuma, K., Economou, S. E., Elkouss, D., Hilaire, P., Jiang, L., Lo, H.-K., and Tzitrin, I. (2023). Quantum repeaters: From quantum networks to the quantum internet. *Reviews of Modern Physics*, 95(4):045006.

Chehimi, M. and Saad, W. (2022). Physics-informed quantum communication networks: A vision toward the quantum internet. *IEEE network*, 36(5):32–38.

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.

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.

Gyongyosi, L. and Imre, S. (2020). Entanglement accessibility measures for the quantum internet. *Quantum Information Processing*, 19:1–28.

Harkness, A., Krawec, W. O., and Wang, B. (2024). Security of partially corrupted quantum repeater networks. *Quantum Science and Technology*, 10(1):015005.

Jain, N., Stiller, B., Khan, I., Elser, D., Marquardt, C., and Leuchs, G. (2016). Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–387.

Jiang, J.-L., Luo, M.-X., and Ma, S.-Y. (2024). Quantum network capacity of entangled quantum internet. *IEEE Journal on Selected Areas in Communications*.

Mastriani, M. (2023). Simplified entanglement swapping protocol for the quantum internet. *Scientific Reports*, 13(1):21998.

Salimian, S., Tavassoly, M., and Ghasemi, M. (2023). Multistage entanglement swapping using superconducting qubits in the absence and presence of dissipative environment without bell state measurement. *Scientific Reports*, 13(1):16342.

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*.

Van Meter, R., Satoh, T., Ladd, T. D., Munro, W. J., and Nemoto, K. (2013). Path selection for quantum repeater networks. *Networking Science*, 3:82–95.

Wehner, S., Elkouss, D., and Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288.

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