Modelando Ataques de Sequestro de Repetidores

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

[1]Universidade Federal do Pará - UFPA

diego.abreu@itec.ufpa.br

Abstract. *Redes de emaranhamento quântico dependem de repetidores e de um plano de controle clássico para estabelecer pares de Bell entre nós. Embora essas redes sejam fundamentadas em princípios físicos que coíbem a observação e a cópia de estados, seu processo de controle ainda pode expor superfícies de ataque. Este trabalho discute o hijacking attack, no qual um agente malicioso redireciona requisições de emaranhamento para um nó incorreto, comprometendo o destino legítimo da comunicação. Como principal contribuição, apresentamos a modelagem desse ataque no simulador SeQUeNCe, considerando dois cenários: (i) um repetidor parcialmente comprometido, que aceita um destino falso como legítimo, e (ii) um repetidor totalmente comprometido, capaz de alterar decisões de roteamento e desviar ativamente requisições.*

1. Introdução

Redes quânticas de emaranhamento, embora baseadas em princípios físicos robustos, apresentam vulnerabilidades no plano de controle clássico, responsável por funções como roteamento, alocação de recursos e coordenação de operações (geração de entrelaçamento, purificação e *entanglement swapping*). Essas fragilidades permitem a exploração por ataques que comprometem o estabelecimento correto de pares entrelaçados, mesmo sem violar princípios fundamentais da mecânica quântica, como o teorema da não-clonagem [Smith et al. 2025b].

Dentre os ataques possíveis [Smith et al. 2025a], destaca-se o *hijacking attack*, no qual um nó malicioso manipula o processo de criação do emaranhamento, redirecionando-o para si próprio ou para nós sob seu controle [Satoh et al. 2018]. Esse ataque explora diretamente o plano de controle da rede, afetando decisões de roteamento e coordenação, podendo degradar a confiabilidade do sistema e impactar aplicações como QKD e computação quântica distribuída. Neste contexto, este trabalho propõe a modelagem do *hijacking attack* no simulador SeQUeNCe, permitindo a análise sistemática e reproduzível desse tipo de ameaça em redes de emaranhamento quântico.

2. Modelo do Ataque e Modelagem no SeQUeNCe

O *hijacking attack* considerado neste trabalho atua sobre o processo de estabelecimento de emaranhamento fim a fim. Em vez de gerar um par entrelaçado entre Alice e o Bob legítimo, a rede, sob influência do atacante, termina por estabelecer uma conexão virtual entre Alice e um nó malicioso ou incorreto.

Foram projetados dois cenários principais. No primeiro, um repetidor comprometido acredita que o atacante representa o destino legítimo e redireciona o processo de troca de emaranhamento para um *Bob falso*. No segundo, o atacante assume controle total de

(a) *Hijacker* camuflando-se como Bob. **(b) *Hijacker* controlando totalmente.**

Figura 1. Representação dos cenários de ataque *Hijacking*.

um repetidor ou do seu comportamento lógico, modificando decisões de roteamento e injetando comandos que desviam a requisição original para um destino arbitrário.

No primeiro cenário, a simulação considera que o repetidor comprometido aceita um identificador de destino incorreto e prossegue com a criação da conexão como se estivesse atendendo ao Bob legítimo. No segundo, o atacante atua diretamente sobre a lógica de encaminhamento da requisição, redirecionando o processo de *entanglement swapping* para um nó malicioso sob sua escolha.

3. Conclusão

Essa modelagem evidencia que o ataque não requer a violação direta de propriedades da mecânica quântica, como o teorema da não-clonagem, mas sim a exploração de vulnerabilidades no plano de controle clássico responsável pelo roteamento, identificação de nós e coordenação do processo de estabelecimento de emaranhamento. Dessa forma, o uso do SeQUeNCe permite analisar, em ambiente controlado, os impactos do ataque e abre caminho para a investigação de mecanismos de autenticação, verificação de rotas e detecção de anomalias em redes quânticas.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) por meio dos auxílios nº 403539/2020-0 e nº 400111/2023-3; e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), sob os auxílios 2023/00811-0, 2023/00673-7, 2021/00199-8 (CPE SMARTNESS), 2020/04031-1 e 2018/23097-3. Também contou com o apoio da Propesp/UFPA, e da Venturus e da Fundação Guamá, por meio da proposta técnica 002/2025 – CITIAMAZON.

Referências

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.

Smith, A., Abreu, D., and Abelém, A. (2025a). Ataques de repetidores em redes de entrelaçamento quântico. In *Anais do II Workshop de Redes Quânticas*, pages 13–18, Porto Alegre, RS, Brasil. SBC.

Smith, A., Abreu, D., Pimentel, A., and Abelém, A. (2025b). Redes quânticas sob ataque: Black hole repeaters. In *Anais do XLIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 266–279, Porto Alegre, RS, Brasil. SBC.