Desafios e Oportunidades rumo à Internet Quântica

Antônio J. G. Abelém[1], **Christian R. Esteve Rothenberg** [2]

[1]Universidade Federal do Pará (UFPA)
[2]Universidade Estadual de Campinas (Unicamp)
abelem@ufpa.br, chesteve@dca.fee.unicamp.br

Abstract. *To exchange data over long distances, in topologically complex networks built on heterogeneous technologies and managed by independent organizations, methods that allow quantum protocols to transparently connect to the underlying hardware implementations are required. However, quantum signals are fragile and cannot be copied or amplified. Until today, just some preliminary versions of network stacks for a quantum internet have been proposed, and only a few basic elements have been suggested. To fully realize the potentials of quantum communication, new challenges and open issues need to be addressed. This paper presents key challenges to enabling a quantum Internet and discusses possible alternatives that are being developed.*

Resumo. *Para trocar dados a longas distâncias, em redes com topologias complexas, construída com tecnologias heterogêneas e gerenciadas por organizações independentes, são necessários métodos que permitam que protocolos quânticos se conectem às implementações de hardware subjacentes de forma transparente. No entanto, os sinais quânticos são frágeis e não podem ser copiados ou amplificados. Atualmente, apenas versões preliminares de pilhas de rede para uma Internet quântica foram propostas e apenas alguns elementos básicos foram sugeridos. Para viabilizar plenamente a comunicação quântica, novos desafios e problemas em aberto precisam ser enfrentados. Este artigo apresenta os principais desafios para se viabilizar uma Internet quântica e discute possíveis alternativas que estão sendo desenvolvidas.*

1. Introdução

Conectar pessoas ou coisasé a principal motivação para a construção de redes, tanto quânticas quanto clássicas. A diferença entre elas é o tipo de dados e as operações envolvidas. Computadores quânticos e redes quânticas usam informações quânticas. O análogo do bit clássico é o bit quântico, ou qubit. Como um bit clássico, o qubit tem dois estados, mas ao contrário de um bit clássico, um qubit pode estar em uma sobreposição ponderada dos dois estados, permitindo que certas funções sejam avaliadas para ambos os valores de entrada no mesmo tempo [Nielsen 2010].

A comunicação quântica é uma maneira de transmitir sinais (quânticos ou clássicos) em distâncias usando os princípios da mecânica quântica. Esses sinais podem ser usados para tarefas que variam de criptografia a computação quântica distribuída em grande escala. Um mecanismo importante para transmitir informações quânticas é o teletransporte (*teleportation*) [Bennett et al. 1993]. A comunicação quântica oferece vantagens incomparáveis à comunicação clássica. Ela tira proveito das leis da física quântica para proteger os dados e pode fazer isso através da transferência de um estado

quântico (entrelaçado ou não), da criação de um estado entrelaçado ou do uso de um estado entrelaçado previamente estabelecido. Essas leis permitem que partículas - normalmente fótons de luz - assumam um estado especial de superposição (*superposition*), o que significa que podem representar diferentes combinações de 1 e 0 simultaneamente [Nielsen 2010].

Apesar do tremendo progresso das tecnologias quânticas rumo à Internet Quântica [S. Wehner and Hanson 2018, Cacciapuoti et al. 2020], a distribuição eficiente de qubits entrelaçados a longa distância ainda constitui um grande desafio, devido ao decaimento exponencial da taxa de comunicação destes em função da distância. Para trocar dados a longas distâncias, em redes topologicamente complexas, construídas com tecnologias heterogêneas e gerenciadas por muitas organizações independentes, são necessários cuidados com ruído e com a perda [Abelem et al. 2020].

Para habilitar o uso amplo de aplicações de propósito geral é essencial desenvolver métodos que permitam que protocolos quânticos se conectem às implementações de hardware subjacentes de forma transparente. Classicamente, isso é alcançado por uma série de protocolos em camadas, como a pilha TCP/IP, fornecendo um conjunto de abstrações que permite que aplicações troquem dados sem precisar saber detalhes das camadas inferiores. Atualmente, apenas versões preliminares de pilha de rede para uma Internet quântica foram propostas [Cacciapuoti et al. 2020] e apenas alguns elementos básicos foram sugeridos [Caleffi and Cacciapuoti 2020]. Para viabilizar totalmente os potenciais da computação quântica, novos desafios e problemas em aberto precisam ser abordados. Diante disso, propostas de arquiteturas para viabilizar uma Internet quântica em grande escala estão em desenvolvimento [S. Wehner and Hanson 2018], paralelamente ao trabalho teórico [Kumar et al. 2019] e experimental [Chen et al. 2018] em camadas físicas e gerenciamento de erros de baixo nível e tecnologias de conexão [Chandra et al. 2018].

Este trabalho contribui com uma apresentação de desafios (Seção 2) em comunicação quântica e redes quânticas, bem como discute (Seção 3) importantes aspectos relacionados com as arquiteturas que estão sendo propostas, enfatizando interessantes oportunidades de pesquisa no tema. Finalmente, são apresentadas considerações finais (Seção 4) e uma sugestão de possíveis trabalhos futuros.

2. Rumo à Internet Quântica: Um Mar de Desafios

Explorar como construir a Internet quântica, uma inter-rede de computadores quânticos e outros dispositivos quânticos, catalisará novas tecnologias que aceleram a Internet atual, melhoram a segurança de nossas comunicações e permitem avanços importantes na computação [Caleffi and Cacciapuoti 2020]. A dificuldade de cada item no projeto de uma rede cresce à medida que a escala da rede aumenta. Isso é verdade para redes clássicas e quânticas. Os principais desafios em dimensionar redes para a escala da Internet e além são: heterogeneidade, especialmente de tecnologias implantadas e condições locais; escala absoluta, afetando roteamento e nomenclatura em particular; lidar com informações desatualizadas sobre as condições atuais da rede (por exemplo, roteamento ou congestionamento) e o sucesso ou falha das operações solicitadas; atender às necessidades das organizações participantes, como privacidade, políticas de trânsito de tráfego desejadas e gerenciamento autônomo; e lidar com nós com comportamento inadequado na rede, seja o comportamento inadequado deliberado ou acidental [Cacciapuoti et al. 2020].

A princípio, desenvolver uma Internet quântica pode parecer mais difícil do que construir um computador quântico em larga escala. Felizmente, verifica-se que muitos protocolos de rede quânticos não exigem grandes computadores quânticos. Na verdade, um dispositivo quântico com um único qubit já é suficiente para muitas aplicações. Além disso, os erros nos protocolos quânticos da Internet geralmente podem ser tratados usando a correção de erros clássica e não quântica, impondo menos demandas no controle e na qualidade dos qubits do que no caso de um computador quântico pleno [Abelem et al. 2020].

A razão pela qual os protocolos quânticos da Internet podem superar a comunicação clássica com recursos relativamente modestos é porque suas vantagens dependem essencialmente de propriedades quânticas inerentes, como o entrelaçamento quântico, que podem ser exploradas com poucos qubits. Por outro lado, um computador quântico deve apresentar mais qubits do que pode ser simulado em um computador clássico para oferecer uma vantagem computacional.

Em essência, cada nó em uma rede quântica é um pequeno computador quântico que pode armazenar e operar com alguns qubits. De acordo com a tecnologia atual, se solicitarmos nós que possam manipular e armazenar qubits, o número de qubits em cada nó será menor que 10. Isso pode parecer um número extremamente pequeno, mas é importante observar que - ao contrário do propósito da computação quântica - a maioria das aplicações de rede quântica pode ser executada usando ainda menos qubits - geralmente apenas um. No entanto, ter mais qubits em cada nó oferece a oportunidade de executar a correção de erros e será útil ao considerar os protocolos de roteamento. Além disso, para protocolos de comunicação quântica geralmente não é necessária a computação quântica universal, mas é suficiente se cada nó puder executar operações mais elementares.

Segundo [S. Wehner and Hanson 2018], uma Internet quântica precisará de três elementos de hardware quântico:

1. **Conexão física**, um canal quântico, que suporte a transmissão de qubits tais como fibras ópticas padrão ou canais de espaço livre, potencialmente via satélites.
2. **Repetidores quânticos**, nós intermediários para alcançar distâncias maiores.
3. **Nós finais**, processadores quânticos conectados à Internet quântica. Eles podem variar de nós extremamente simples, que só podem preparar e medir um único qubit, a computadores quânticos em larga escala. Os nós finais podem atuar como repetidores quânticos, embora isso não seja um requisito.

Como uma internet quântica não pretende substituir a comunicação clássica, mas complementá-la com a comunicação quântica, considera-se que todos os nós podem se comunicar classicamente - por exemplo, pela Internet clássica - para trocar informações de controle. [S. Wehner and Hanson 2018] propõem estágios de desenvolvimento em direção a uma Internet quântica completa orientados por funcionalidade. O ponto central de sua definição não é a dificuldade de alcançá-los experimentalmente, mas sim a questão essencial de qual nível de complexidade é necessário para realmente habilitar aplicações úteis. Cada estágio é diferenciado por uma funcionalidade quântica específica que é suficiente para suportar uma certa classe de protocolos e aplicações.

No contexto de uma internet quântica, a aplicação mais conhecida atualmente é a distribuição de chave quântica (QKD - *Quantum Key Distribution*) [Ekert 1991], que permite que dois nós de redes distintas estabeleçam uma chave criptográfica cuja segurança

depende apenas das leis da mecânica quântica. No entanto, muitas outras aplicações são viáveis, com vantagens impossíveis de serem alcançadas pela Internet clássica. Além da área de segurança, como acesso remoto seguro a computadores quânticos [Kimble 2008], aplicações alvo incluem aquelas que requeiram coordenação, como sincronização de relógios [Kómár et al. 2014] e escolha (eleição) de líderes, além de aplicações científicas [Gottesman et al. 2012].

O status experimental atual de redes quânticas de longa distância está no estágio mais baixo com vários sistemas comerciais para QKD no mercado. As primeiras redes estendidas de repetidores confiáveis já foram implementadas em distâncias metropolitanas, e uma implementação de longa distância foi recentemente concluída [Kumar et al. 2019]. Vários experimentos recentes demonstraram elementos pertencentes a este e a estágios superiores em distâncias curtas, sugerindo que redes de alta funcionalidade estão ao alcance [Cacciapuoti et al. 2020].

3. Oportunidades de Pesquisa para desenvolver uma Internet Quântica

A seguir elencamos algumas áreas que apresentam oportunidades de pesquisa rumo o desenvolvimento de uma Internet Quântica.

Qubits robustos. Qualquer interação de um qubit com o ambiente causa decoerência, ou seja, uma perda de informação do qubit para o ambiente com o passar do tempo, e o isolamento é difícil de realizar na prática com o estado da arte das tecnologias quânticas. Além disso, o isolamento perfeito não é desejável, uma vez que a computação e a comunicação requerem interação com os qubits, por exemplo, para operações de leitura / gravação. Embora uma diminuição gradual dos tempos de decoerência seja esperada com o progresso das tecnologias quânticas, o projeto de uma rede quântica deve considerar cuidadosamente as restrições impostas pela decoerência quântica. A decoerência não é a única fonte de erros. Erros surgem praticamente com qualquer operação em um estado quântico devido a imperfeições e flutuações aleatórias. Aqui, uma figura de mérito fundamental é a fidelidade quântica. Do ponto de vista da engenharia de comunicação, a modelagem conjunta de erros induzidos pelas operações quânticas, juntamente com aqueles induzidos pela geração / distribuição de entrelaçamento, ainda é um problema em aberto.

Correção de Erros. O Teorema da não clonagem impede a adoção em redes quânticas de técnicas clássicas de recuperação de erros, que dependem da cópia de informações, para preservar a informação quântica contra a decoerência e operações imperfeitas. Recentemente, muitas técnicas de correção de erros quânticos foram propostas como em [Chandra et al. 2018]. No entanto, mais pesquisas são necessárias, pois as técnicas de correção de erros quânticos devem lidar não apenas com erros de inversão de bits, mas também de erros de inversão de fase, bem como erros de inversão de fase e de bit simultâneos. Isso difere das redes clássicas, que só precisam considerar erros de bit.

Camada de Enlace. Uma diferença fundamental em relação às redes clássicas, onde a transmissão via difusão (*broadcast*) é amplamente explorada para implementar várias funcionalidades da camada de enlace e da camada de rede, como controle de acesso ao meio e descoberta de rota, é a impossibilidade de transmitir informações quânticas para mais de um único destino devido ao *no-broadcasting theorem* [Barnum et al. 2007], um corolário do teorema de não-clonagem. Como consequência, a camada de enlace deve ser cuidadosamente repensada e redesenhada, e técnicas de multiplexação eficazes para

redes quânticas devem ser projetadas para permitir que vários dispositivos quânticos sejam conectados a um único canal quântico (por exemplo, uma fibra). O acesso ao meio pode ser baseado, por exemplo, na divisão da frequência de fótons para a distribuição de entrelaçamento.

Roteamento. Assunto importante, pois determina a conectividade de uma rede quântica em termos de capacidade de realizar teletransporte entre dispositivos quânticos. Consequentemente, novas métricas de roteamento quântico são necessárias para garantir uma seleção de caminho ciente de entrelaçamentos que seja eficiente. Além disso, o processo de teletransporte destrói o entrelaçamento como consequência. Portanto, se qubits adicionais precisam ser teletransportados, novos pares entrelaçados precisam ser criados e distribuídos entre a origem e o destino. Esta restrição não tem contrapartida em redes clássicas e deve ser cuidadosamente considerada na camada de rede [Kumar et al. 2019].

Modelo arquitetural. Redes quânticas são sistemas de engenharia complexos e desafiadores que requerem soluções sofisticadas para suas operações e controle, com muitas dessas soluções ainda a serem desenvolvidas [Caleffi and Cacciapuoti 2020]. Na verdade, muitas das tecnologias de plano de controle em uso em redes clássicas modernas não são adequadas para o plano de dados quânticos que não podem ser submetidos à conversão O-E-O. O gerenciamento e a operação da rede quântica serão particularmente desafiadores devido à natureza quântica embutida no plano de controle e / ou no plano de dados. A tarefa é ainda mais complicada pela necessidade de redes quânticas coexistirem com redes convencionais. Além disso, o monitoramento de redes quânticas requer medições de sinais convencionais e quânticos complexos, juntamente com inferências e análises para destilar conhecimento e tomar decisões de controle [Ndousse-Fetter et al. 2019]. Nesse contexto, pode-se considerar diferentes abordagens, dependendo do objetivo da rede, entre elas utilizar princípios das redes definidas por software (SDN) para gerenciar de forma mais flexível e programável, tanto a rede clássica como a rede quântica. A flexibilidade trazida pelo paradigma SDN reduz drasticamente o esforço de integração de novos dispositivos e tecnologias na rede e permite endereçar o projeto de redes quânticas versáteis por meio do desenvolvimento de switches quânticos programáveis [Humble et al. 2018, Kozlowski et al. 2020].

Pacote quântico. Requer a integração de recursos de comunicação clássicos e quânticos. Os recursos de comunicação clássica provavelmente serão fornecidos pela integração de redes clássicas, como a Internet atual com a Internet Quântica. No entanto, atualmente, não há noção de um "Pacote Quântico" - um estado quântico fotônico junto com cabeçalhos apropriados que funcionam como uma única unidade de dados que atravessa a rede quântica. Como apenas versões preliminares de pilhas de rede existem atualmente para uma Internet quântica, isso representa um grande problema em aberto e sua solução requer um esforço multidisciplinar, abrangendo desde a teoria da comunicação e comunidades de engenharia até a de engenharia de rede.

4. Conclusões

A comunicação quântica e a Internet terão um grande impacto em nosso mundo. O objetivo de uma internet quântica é habilitar aplicações fundamentalmente fora do alcance da Internet clássica. As redes quânticas, como muitas outras inovações, que se originam da pesquisa básica na academia e laboratórios nacionais, enfrentam desafios de transferência

de tecnologia, apesar de seu enorme potencial para aumentar as capacidades de uma nação e beneficiar sua sociedade. Atentos a esta questão, os principais países do mundo têm definido como visão estratégica os esforços de P&D para avançar no desenvolvimento de bases para a Internet quântica [U. S. Quantum 2020, European Alliance 2020].

Referências

Abelem, A., Vardoyan, G., and Towsley, D. (2020). *Quantum Internet: The Future of Internetworking. In: Minicursos do 38o SBRC*. SBC.

Barnum, H., Barrett, J., Leifer, M., and Wilce, A. (2007). Generalized no-broadcasting theorem. *Physical Review Letters*, 99(24).

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895.

Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S., and Bianchi, G. (2020). Quantum internet: Networking challenges in distributed quantum computing. *IEEE Network*, 34(1):137–143.

Caleffi, M. and Cacciapuoti, A. S. (2020). Quantum switch for the quantum internet: Noiseless communications through noisy channels. *IEEE Journal on Selected Areas in Communications*, pages 1–1.

Chandra, D., Babar, Z., Nguyen, H. V., Alanis, D., Botsinis, P., Ng, S. X., and Hanzo, L. (2018). Quantum topological error correction codes: The classical-to-quantum isomorphism perspective. *IEEE Access*, 6:13729–13757.

Chen, X., Cheng, B., Li, Z., Nie, X., Yu, N., Yung, M.-H., and Peng, X. (2018). Experimental cryptographic verification for near-term quantum cloud computing.

Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663.

European Alliance, Q. I. (2020). Quantum internet alliance.

Gottesman, D., Jennewein, T., and Croke, S. (2012). Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.*, 109:070503.

Humble, T. S., Sadlier, R. J., Williams, B. P., and Prout, R. C. (2018). Software-defined quantum network switching. In *Disruptive Technologies in Information Sciences*, volume 10652, pages 72 – 79. SPIE.

Kimble, H. J. (2008). The quantum internet. *Nature*, 453(7198):1023–1030.

Kómár, P., Kessler, E. M., Bishof, M., Jiang, L., Sørensen, A. S., Ye, J., and Lukin, M. D. (2014). A quantum network of clocks. *Nature Physics*, 10(8):582–587.

Kozlowski, W., Kuipers, F., and Wehner, S. (2020). A p4 data plane for the quantum internet. *Proceedings of the 3rd P4 Workshop in Europe*.

Kumar, S., Lauk, N., and Simon, C. (2019). Towards long-distance quantum networks with superconducting processors and optical links. *Quantum Science and Technology*, 4(4):045003.

Ndousse-Fetter, T., Peters, N., Grice, W., Kumar, P., Chapuran, T., Guha, S., Hamilton, S., Monga, I., Newell, R., Nomerotski, A., Towsley, D., and Yoo, B. (2019). Quantum networks for open science.

Nielsen, Michael A.and Chuang, I. (2010). *Quantum computation and quantum information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA.

S. Wehner, D. E. and Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(1):303.

U. S. Quantum, National Office, U. S. G. (2020). A strategic vision for america's quantum networks.