Síntese - Designing a Quantum Network Protocol

Autor
José Lira de Oliveira Junior

2022

Designing a Quantum Network Protocol - Kozlowski

O artigo apresenta um protocolo de redes quânticas com o intuito de permitir comunicação quântica de ponta a ponta.

Um dos principais desafios na tecnologia quântica no curto prazo é a decoerência - o decaimento gradual da informação quântica, que coloca limites nno tempo de armazenamento.

A ideia é que as redes quânticas melhorem redes clássicas e ainda executem protocolos que são impossíveis classicamente.

Principais aplicações

- comunicação quântica segura;
- computação quântica distribuída;
- computação quântica segura na nuvem;
- sincronização de clock;
- redes de medição melhoradas quanticamente aprimoradas;
- distribuição de chaves quânticas (QKD).

Principais desafios na implementação de redes de longas distâncias

- perdas na transmissão;
- decoerência (o típico tempo de vida de memórias é de alguns microsegundos a pouco mais de um segundo);
- teorema da não-clonagem (estados quânticos arbitrários não podem ser copiados).

Por conta do teorema da não-clonagem, é impossível utilizar técnicas clássicas de amplificação ou retransmissão de dados para compensar perdas.

Correção quântica de erros existe, mas ainda é inviável por questão de recursos, provavelmente só será possível em algumas décadas.

Emaranhamento

O **emaranhamento quântico** é a chave para comunicação a longas distâncias, pois pode-se utilizar um par de qubits emaranhados para transmitir dados arbitrários. Assim, pode-se 'escapar' dos problemas de perdas e do teorema da não-clonagem. Os qubits emaranhados podem ser facilmente reconstruídos se perdido, já que só precisam ser entregues em um dos poucos estados particulares, chamados de estados de Bell.

Tendo em vista as novas possibilidades trazidas pelo emaranhamento quântico, é possível realizar a operação conhecida como '*entanglement swapping*', ou troca de emaranhamento, para realizar comunicação de longas distâncias. Neste processo, 'liga-se' pares de curtas distâncias juntos de forma que se cria, no fim, um emaranhamento de longa distância.

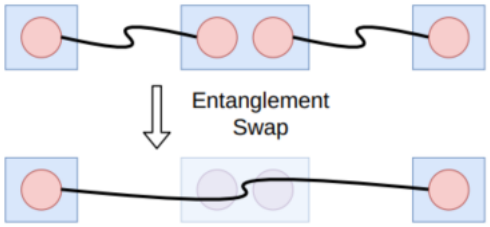

Figura 1: Entanglement swapping

Sobre o artigo

De acordo com os autores, as principais contribuições do trabalho são:

1. projeta-se um protocolo para gerar pares emaranhados de ponta a ponta, em face da decoerência, que cumpre o papel de uma camada de rede quântica.

2. traça-se a arquitetura da construção de serviços de redes quânticas e o bloco construtor nesse esquema;

3. avalia-se a eficiência do protocolo proposto diante de decoerência em um simulador de redes quânticas;

4. mostra-se que permanece funcional em hardware de curto prazo extremamente limitado.

É importante destacar que diferente de redes clássicas nas quais os dados devem ser entregues livres de erro, aplicações quânticas podem operar com estados quânticos imperfeitos, desde que a fidelidade esteja acima de um limite específico por aplicação (para o QKD básico, o limite de fidelidade é cerca de 0.8).

Fidelidade

Fidelidade é uma métrica puramente quântica que quantifica a qualidade de um estado em termos de o quão 'perto' está do estado desejado, assim, uma fidelidade igual a 1 significa que o estado está exatamente igual ao desejado. Um valor abaixo de 0.5 significa que o estado não é mais útil.

A fidelidade é perdida de diversas formas em uma rede:

1. pares de curta distância gerados em um link são imperfeitos;
2. realizar o swap em pares imperfeitos resulta em um par de menor fidelidade, mesmo se as operações físicas não tiverem ruído;
3. implementações imperfeitas de portas quânticas podem reduzir fidelidade quando qualquer qubit for processado;
4. a decoerência degrada a fidelidade de um estado quântico enquanto o qubit está armazenado na memória.

O problema 2 citado acima é uma propriedade fundamental da troca de emaranhamento e a única forma boa de garantir que o estado de saída é suficientemente bom é inserir dois estados de alta qualidade no swap.

O problema 4 pode ser atacado minimizando o tempo que qubits passam inativos na memória.

A Figura 2 ilustra a pilha de uma rede quântica proposta inspirada pela pilha de protocolos TCP/IP.

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

Figura 2: Pilha de rede quântica

A pilha coordena suas ações com seus vizinhos trocando mensagens clássicas (todos os nós são conectados classicamente), como mostra a Figura 3.

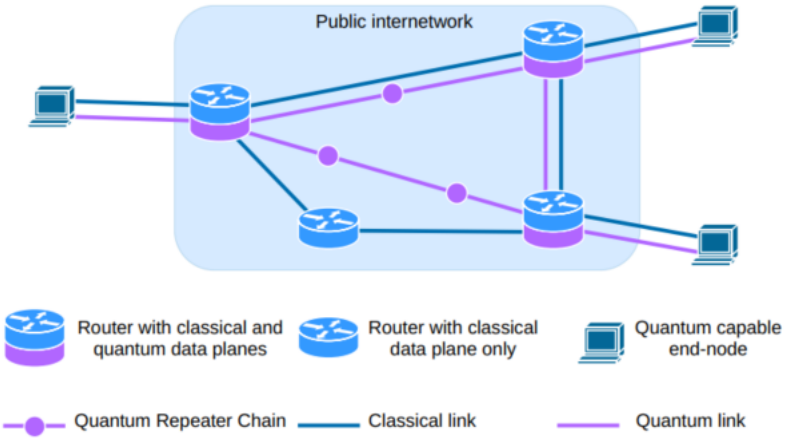

Figura 3: Arquitetura de rede quântica

Os qubits são divididos em:

- qubits de comunicação - aqueles que participam de operações de rede;
- qubits de armazenamento - qubits que guardam informação quântica, mas não podem ser utilizados para geração de emaranhamento.

Casos de uso

1. **Medido diretamente** (MD): aplicações nessa categoria são caracterizadas pelo fato de que consomem os pares entregues (medindo-os) tão logo que estão disponíveis e não os guardam. **Exemplos:** identificação segura, criptografia;
2. **Criar e guardar** (CK): aplicações nessa categoria são caracterizadas pela necessidade de armazenamento, possivemente de múltiplos pares emaranhados simultaneamente. **Exemplos:** sensores, metrologia, sistemas quânticos distribuídos.

Aspectos da rede em relação a camadas de alto nível

Logicamente, a rede entrega um par emaranhado. Fisicamente, a rede entrega um qubit emaranhado para cada um dos dois nós finais. Isso significa que a rede deve 'rastrear' os swaps e conectar os pares individuais formando um par de longa distância de forma que, no fim, seja possível identificar quais qubits pertencem ao mesmo par. Assim, a rede fornece um **identificador de par emaranhado**.

Por conta da natureza aleatória da mecânica quântica, o estado de cada par produzido pelos swaps é desconhecido, a priori, mas é revelado ao nó de troca assim que o swap é completo. A rede deve coletar esses 'anúncios', inferir o estado e entregar a informação à aplicação.

Tendo em vista que é necessário mais tempo para produzir melhores estados, algumas aplicações podem sacrificar fidelidade em troca de taxas de transmissão maiores (ou vice-versa).

Arquitetura da camada de rede

O protocolo de plano de dados quânticos proposto neste artigo requer dois serviços externos: um protocolo de sinalização e um protocolo de roteamento.

- **Protocolo de roteamento**: antes de um par emaranhado ponta-a-ponta ser gerado, o caminho ótimo deve ser determinado. No entanto, esse caminho não é computado baseando-se apenas na distância, custo e taxa de transferência, deve ser levado em conta também a fidelidade desejada ponta-a-ponta. Algoritmos de roteamento são um campo de estudo emergente em redes quânticas.

- **Protocolo de sinalização**: o papel desse protocolo será a instalação de circuitos virtuais. É similar a como RSVP-TE é usado para instalar circuitos virtuais MPLS em redes clássicas. No entanto, alocar um caminho com recursos suficientes não é o bastante. Em uma rede quãntica, os links *upstream* e *downstream* devem gerar seus pares em instantes suficientemente próximos para que a decoerência não aconteça antes do swap. Assim, a proposta é que o protocolo de sinalização seja encarregado de gerenciar o 'cronograma' (eventos).

Protocolo de plano de dados quânticos

É o componente responsável por coordenar a geração de emaranhamento a nível de link e os swaps subsequentes no caminho entre dois nós distantes enquanto minimiza as perdas por decoerência e compensa as perdas que acontecerem.

Para criar um par de longa distância, pares-link devem ser gerados ao longo de todo o caminho. A camada de rede não lida com o processo físico diretamente, ao invés disso depende de um protocolo de camada de enlace para entregar esses pares, como mostra a Figura 2. Mas é de responsabilidade da camada de rede coordenar o serviço da camada de enlace em cada nó no caminho de forma que uma quantidade suficiente de links de fidelidade adequada seja produzida.

Uma vez que os pares sejam gerados, os repetidores devem realizar trocas de emaranhamento para criar os pares de longa distância. Além disso, o protocolo também deve 'rastrear' os swaps que foram feitos no processo de cada par ponta-a-ponta. Isso deve ser feito por dois motivos: identificar corretamente quais qubits pertencem ao mesmo par ponta-a-ponta e em qual estado de Bell estão. Assim, o protocolo de rede precisa de um mecanismo para coletar as saídas das trocas de emaranhamento e entregar aos nós finais de forma que o estado de Bell final do par possa ser inferido e entregue ao receptor.

O serviço da camada de enlace

Tendo em vista que a probabilidade de sucesso em cada tentativa de gerar emaranhamento é baixa, é esperado da camada de link que haja um mecanismo de nova tentativa para aumentar confiabilidade. Assim, quatro propriedades são necessárias à camada de enlace:

1. um identificador único para cada requisição na camada de link.
2. um identificador para cada par emaranhado.
3. a camada de link deve informar à camada de rede em qual dos estados de Bell os qubits foram entregues.
4. a aplicação que está utilizando a rede deve ser capaz de especificar parâmetros relevantes de qualidade de serviço, como fidelidade mínima e restrições de tempo.

QNP - quantum network protocol

O protocolo proposto é o QNP (protocolo de rede quântica).

O QNP começa a operar uma vez que um circuito virtual (VC) é instalado em uma rede pelo protocolo de sinalização usando o caminho fornecido pelo protocolo de roteamento. O circuito é direcionado com um nó *head-end* no nó *upstream* e um nó *tail-end* no nó *downstream*. É dever do protocolo de sinalização decidir qual direção é *up* ou *downstream*. Pares emaranhados não possuem direção, mas essa distinção é útil para permitir que nós *upstream* possam iniciar atividades relacionadas aos pares, como uma geração de pares emaranhados.

- O QNP inicia com uma requisição recebida no nó *head-end*.
- Isso envia uma mensagem **FORWARD** *downstream* em direção ao nó *tail-end* iniciando a geração de par-link com um VC particular em cada link ao longo do caminho.
- Assim que dois pares-link são gerados no mesmo nó intermediário, um no link *upstream* e um no *downstream*, uma troca de emaranhamento é realizada imediatamente.
- A saída do swap é coletada por duas mensagens **TRACK**, uma indo para 'cima' e uma para 'baixo'.
- Assim que as mensagens **TRACK** chegam aos nós finais, o par é entregue à aplicação.

Registros de swap

A geração de pares-link e os swaps são paralelizáveis, assim vários links podem ser gerados simultaneamente. Já que geração de pares não é um processo necessariamente rápido, essa é uma otimização de performance, pois os qubits não precisarão esperar tanto tempo por um qubit compatível para realizar o swap, diminuindo o tempo necessário de armazenamento e minimizando a decoerência.

Tendo em vista que a ordem que os swaps acontecem não importa, uma mensagem **TRACK** pode ser pensada como uma forma de reconstruir o estado emaranhado final como se os swaps acontecessem na ordem que a mensagem coleta os registros de swap.

Assim, a mensagem TRACK efetivamente carrega informação sobre o estado de entrada do próximo swap. Quando esta coleta um novo registro de swap, usa o resultado de dois bits contidos nela para inferir o estado da entrada do próximo nó. Assim que esta chega no nó final, o "estado de entrada do próximo nó" é o estado do par emaranhado final.

Rastreamento preguiçoso de emaranhamento

Isso é chamado de rastreamento preguiçoso de emaranhamento, pois o protocolo não acompanha os pares intermediários criados durante o processo. Já que os swaps não ocorrem necessariamente na ordem que estão registrados, os registros não representam os estados intermediários. O único par que, necessariamente, é conhecido o estado é o par final. Isso permite que:

- operações quânticas ocorram não importando se as mensagens clássicas de controle foram comunicadas.
- nós individuais descartem qubits sem coerência sem que seja necessário comunicar isso ao resto do VC.

Quando um qubit é descartado, o nó deve criar um registro temporário de descarte. Quando uma mensagem de rastreamento chegar ao nó, este checará o registro de descarte se não achar o registro de swap. Se o registro de descarte estiver presente, a mensagem de rastreamento será enviada de volta à sua origem para notificar ao nó final que a cadeia foi quebrada. 7

Se circuitos são usados com reserva de recursos, haverá a alocação de uma **EER** - end-to-end rate (taxa de ponta-a-ponta) máxima, isto é, largura de banda. Assim, o QNP pode rejeitar e atrasar requisições recebidas.

Geração contínua de links

Nos estágios iniciais de redes quânticas, descartar qubits por conta da decoerência será a regra e não exceção. Portanto, a camada de enlace deve possuir um mecanismo de nova tentativa eficiente. Assim, o QNP requisita do serviço da camada de link a produção contínua de pares até que os nós finais sinalizem a conclusão da requisição.

Agregação

Pares emaranhados gerados entre os mesmos nós finais com mesmo limite de fidelidade são, para fins de aplicação, indistinguíveis. Assim, o QNP deve agregar tais requisições no mesmo VC. A agregação leva a:

- Redução da quantidade de estados que a rede precisa gerenciar, reduzindo o número total de circuitos.
- Melhora no compartilhamento de recursos em nós nos quais ocorrem swap.

Agregação significa que o VC não acompanha nenhuma requisição de informação. Assim, atribuir os pares de um circuito a requisições deve ser feito pelos nós finais. Para isso, os nós finais podem utilizar uma fila distribuída, fazer com que o nó *head-end* tome todas as decisões e as comunique pelas mensagens **TRACK** ou usar outro protocolo qualquer. O QNP só necessita que os nós 'concordem' em um método.

Mecanismos para auxiliar nesta tarefa:

1. Épocas (?): uma época é o conjunto de requisições ativas no momento. Uma nova época é criada (mas não ativada) sempre que uma requisição é recebida ou concluída. O *head-end* avança a época ativa setando o valor da próximo em cada mensagem **TRACK**. Uma vez que o par emaranhado correspondente àquela mensagem **TRACK** é entregue, a época indicada pela mensagem se torna ativa.

2. Mensagens **TRACK** carregam informação sobre qual requisição foram atribuídas pelo nó final que originou a mensagem.

Tabela de roteamento

Para comunicar todas as decisões de roteamento do protocolo de plano de dados quânticos, é necessário o registro de uma tabela de roteamento em cada nó de cada VC. Esse registro deve conter:

- o próximo nó *downstream*.
- o próximo nó *upstream*.
- a label do link *downstream*.
- a label do link *upstream*.
- a mínima fidelidade do link *downstream*.
- a máxima LPR (taxa de geração de pares-link) *downstream*.
- a EER máxima do circuito.

Deve-se notar que o limite de fidelidade para um link deve ser maior do que a fidelidade ponta-a-ponta para dar conta das perdas nos swaps e por decoerência.

Supondo ruído isotrópico (pior cenário), a fidelidade F' de um par emaranhado produzido pela combinação de dois pares com fidelidades F_1 e F_2 é dada por:

$$F' = F_1 F_2 + \frac{(1 - F_1)(1 - F_2)}{3}$$

Rodadas de teste de fidelidade

É fisicamente impossível ao protocolo ver ou medir os pares entregues para avaliar sua fidelidade. Assim, o método proposto para fornecer confiança à aplicação sobre o limite de fidelidade é utilizar rodadas de teste. Isto é, cria-se um número de pares como testes que são medidos (e consumidos). As estatísticas retiradas das medições são usadas para estimar a fidelidade dos pares realmente utilizados na aplicação.

Exemplo

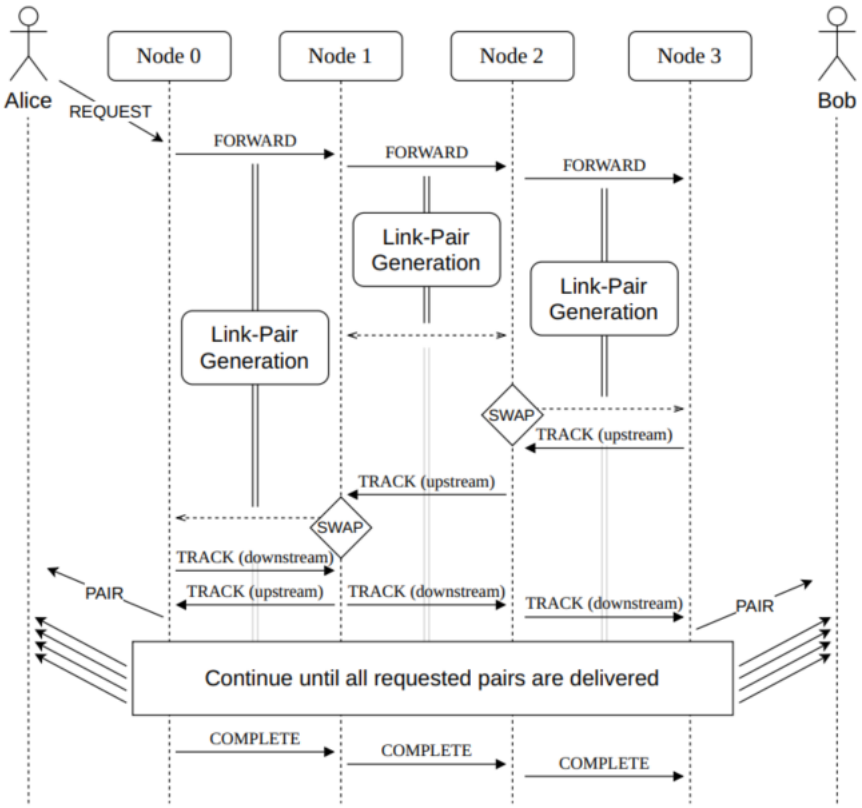

Figura 4: Exemplo de funcionamento do QNP

- Ao receber uma requisição, uma mensagem **FORWARD** é enviada ao longo do VC para iniciar a geração de pares-link;
- Swaps são executados assim que um par *upstream* e *downstream* estão disponíveis ao mesmo circuito, gerando um registro de swap na conclusão;
- Cada nó final inicia uma mensagem **TRACK** assim que os pares-link estão disponíveis.
- As mensagens **TRACK** seguem ao longo do circuito coletando registros de swap, esperando a conclusão do swap do par correspondente, se necessário.
- Quando as mensagens **TRACK** chegam ao nó final destino, o identificador final e a informação sobre o estado de Bell são entregues juntas ao próprio qubit, ou até antes.
- Assim que todos os pares são entregues, uma mensagem **COMPLETE** é enviada ao longo do circuito para finalizar ou atualizar as requisições da camada de enlace.

Destilação de emaranhamento

É um processo pelo qual dois ou mais pares imperfeitos são consumidos para produzir um par de maior fidelidade com alguma probabilidade finita. No entanto, as exigências de hardware para realizar tal processo são maiores que as exigências para o *swapping*. Assim, por ainda ser uma questão com pesquisa aberta sobre as melhores estratégias, foi decidido não incorporar a destilação de emaranhamento no protocolo.

Links

- Editar no Overleaf: `https://www.overleaf.com/5572541672rtrqcmzdnjvs`
- Visualizar no Overleaf: `https://www.overleaf.com/read/znkzgjtqqsxp`