Optimal Remote Entanglement Distribution

Wenhan Dai, *Student Member, IEEE*, Tianyi Peng, *Student Member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

***Abstract*— Distributing entanglement between distant nodes is an essential task in quantum networks. To achieve this task, quantum repeaters have been introduced to perform entanglement swapping. This paper offers a design of remote entanglement distribution (RED) protocols that maximize the entanglement distribution rate (EDR). We introduce the concept of *enodes*, representing the entangled quantum bit (qubit) pairs in the network. This concept enables us to design the optimal RED protocols based on the solutions of some linear programming problems. Moreover, we investigate RED in a homogeneous repeater chain, which is a building block for many quantum networks. In particular, we determine the maximum EDR for homogeneous repeater chains in a closed form. Our results enable the distribution of long-distance entanglement with noisy intermediate-scale quantum (NISQ) technologies and provide insights into the design and implementation of general quantum networks.**

***Index Terms*— Quantum networks, routing, entanglement swapping, entanglement distribution, repeaters.**

I. Introduction

QUANTUM INFORMATION SCIENCE is poised to create the next technological revolution [1]–[3]. There are various quantum-enabled cutting-edge technologies in quantum communication [4]–[8], quantum computation [9]–[11], and quantum sensing [12]–[14]. Many of these technologies rely on distributing quantum entanglement [15]–[17]. For example, distributing entanglement enables quantum teleportation [18]–[20] and remote state preparation [21]–[23], sending quantum information without having to move physical particles.

The main difficulty of distributing entanglement at two distant nodes in quantum networks lies in the significant decay of communication capacity with the length of the channel. For example, the capacity of a lossy channel decays exponentially with the distance of optical fibers, thereby hindering distributing entanglement between two nodes that are far apart. To address this issue, researchers introduced quantum repeaters in the design of quantum networks. A quantum repeater is a node with quantum memory and Bell-state measurement capability. With quantum repeaters, entanglement can be distributed between distant nodes without physically sending entangled quantum bits (qubits) through the entire network [15]–[17]. The benefits of using quantum repeaters have been demonstrated in several studies [24], [25]. For example, inserting quantum repeaters between two nodes connected by optical fibers can improve the channel capacity; such capacity is determined by the maximum distance of the quantum channels divided by the quantum repeaters.

Several protocols have been proposed for entanglement distribution in quantum networks [24]–[30]. A key metric to evaluate these protocols is the entanglement distribution rate (EDR), i.e., the average amount of entanglement distributed between two specified nodes, referred to as source and sink, per time slot. Most protocols cannot provide the maximum EDR except for [24], [25], in which optimal entanglement routing protocols are proposed for basic decoherence channel models. However, the results in [24], [25] rely on the assumption of perfect quantum repeaters, i.e., the entanglement swapping can be performed with success probability of one.[1] This assumption is unlikely to hold in the foreseeable future. In [30], the scenario with imperfect quantum repeaters is considered with the constraint that entanglement swapping is successfully and simultaneously performed at all the nodes along a path connecting the source and the sink, and this leads to suboptimal protocols since the order of entanglement swapping is not optimized. Little is known about the protocols that schedule entanglement swapping optimally with imperfect quantum repeaters.

Among different quantum networks, we are particularly interested in the homogeneous repeater chain, a network that connects two distant nodes with a chain of identical and equally spaced repeaters. This is because the investigation of homogeneous repeater chains can shed light on quantum networks with general structures and lay the foundation for the study of more complicated network structures. Since the introduction of homogeneous repeater chains in [31], many protocols and EDR analyses have been provided [32]–[40]. These protocols and analyses can be categorized into two groups. The first group of work considers quantum memories that can store qubits only for a short time. Such consideration accounts for the limitation of current quantum-hardware capabilities [38]–[40]. For example in [38], entanglement-based quantum key distribution rate is determined, and different factors such as fiber loss, detector dark counts, and detector inefficiency are

Manuscript received July 15, 2019; revised December 15, 2019; accepted January 6, 2020. Date of publication January 23, 2020; date of current version April 3, 2020. This work was supported in part by the Office of Naval Research under Grant N00014-19-1-2724 and in part by the MIT Institute for Soldier Nanotechnologies. This article was presented in part at the International Conference on Computing, Networking and Communications, Big Island, Hawaii, 2020. *(Corresponding author: Moe Z. Win.)*

Wenhan Dai and Tianyi Peng are with the Wireless Information and Network Sciences Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: whdai@mit.edu; tianyi@mit.edu).

Moe Z. Win is with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: moewin@mit.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2020.2969005

[1] In the rest of this paper, "perfect/imperfect repeaters" and "perfect/imperfect entanglement swapping" are used interchangeably when clear in the context.

0733-8716 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

accounted for. However, if the quantum memory cannot store qubits for a sufficiently long time, entanglement swapping operations need to succeed simultaneously at each quantum repeater. This makes the EDR decrease exponentially with respect to the length of a repeater chain. The second group of work considers quantum memories that can store qubits for a sufficiently long time. Within this group, some studies aim at experimentation of entanglement distribution using atomic ensembles and linear optics [32]–[36]; some studies aim at the design and analysis of entanglement distribution protocols [31], [41]–[43]. Most existing protocols, e.g., in [42], assume that two neighboring quantum repeaters stop generating entanglement once an entangled qubit pair is generated between them, and this assumption may decrease the EDR. Despite the extensive entanglement distribution protocols, it still remains unclear whether the designed protocols can achieve the maximum EDR, even in the scenario that considers simple photon-loss quantum channels and probabilistic entanglement swapping.

The consideration of imperfect quantum repeaters creates a new research topic: how to design protocols that schedule entanglement swapping to maximize the EDR in a quantum network. These protocols are referred to as remote entanglement distribution (RED) protocols in this paper. Note that RED protocols differ from entanglement routing protocols [25]–[27], [30]: entanglement routing protocols find paths between two nodes and perform entanglement swapping at each node sequentially along the path, whereas RED protocols not only find the paths, but also determine the sequence of entanglement swapping. In this way, entanglement routing can be viewed as a special case of RED. To the best of the authors' knowledge, how to develop the optimal RED protocol with imperfect quantum repeaters remains unknown.

The fundamental questions related to RED in quantum networks are:

- how entanglement swapping affects the EDR in quantum networks; and
- how to exploit the structure of the homogeneous repeater chains to maximize the EDR.

The answers to these questions will enable the distribution of entanglement over long distances with noisy intermediate-scale quantum (NISQ) technologies [2] and take an essential step for the development of quantum networks.

The goal of this paper is to develop the optimal RED protocols for quantum networks. We introduce the concept of enodes, representing the entangled qubit pairs in the network. Entanglement swapping can be viewed as an operation that exchanges entangled qubit pairs among different enodes. The introduction of enodes allows us to employ techniques from linear programming and classical networks to design the RED protocols in quantum networks.

In this paper, we establish a framework of designing RED protocols for quantum networks. We transform the design of the optimal RED protocols into linear programming problems. The key contributions of this paper are as follows:

- we determine the maximum achievable EDR for quantum networks;
- we determine the structural properties of the graph corresponding to the optimal solution of the linear programming problem;
- we develop the optimal RED protocols for quantum networks based on the solution of the linear programming problem; and
- we determine the maximum EDR for homogeneous repeater chains in a closed form.

The remaining sections are organized as follows. Section II presents the system model and preliminary research results. Section III introduces the concept of enodes and derives an achievable upper bound for the maximum EDR. Section IV considers the homogeneous repeater chains and determines the maximum EDR in a closed form. The performance of the proposed protocols is presented via numerical examples in Section V. Finally, the conclusions are drawn in Section VI.

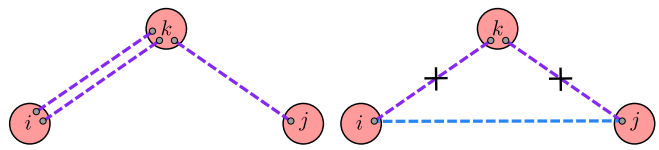
Notation: Random variables are displayed in sans serif, upright fonts; their realizations in serif, italic fonts. Vectors and matrices are denoted by bold lowercase and uppercase letters, respectively. For example, a random variable and its realization are denoted by x and x; a random vector and its realization are denoted by $\mathbf{x}$ and $\boldsymbol{x}$; a random matrix and its realization are denoted by $\mathbf{X}$ and $\boldsymbol{X}$, respectively. Sets and random sets are denoted by upright sans serif and calligraphic font, respectively. For example, a random set and its realization are denoted by X and $\mathcal{X}$, respectively. The m-by-n matrix of zeros (resp. ones) is denoted by $\mathbf{0}_{m\times n}$ (resp. $\mathbf{1}_{m\times n}$); when $n=1$, the m-dimensional vector of zeros (resp. ones) is simply denoted by $\mathbf{0}_m$ (resp. $\mathbf{1}_m$). The m-by-m identity matrix is denoted by $\boldsymbol{I}_m$: the subscript is removed when the dimension of the matrix is clear from the context. The sets of integers, even integers, odd integers, and positive integers are denoted by $\mathbb{Z}$, $\mathbb{Z}_{\mathrm{e}}$, $\mathbb{Z}_{\mathrm{o}}$, $\mathbb{N}_+$, respectively. The cardinality of a set $\mathcal{S}$ is denoted by $\mathrm{Card}(\mathcal{S})$. The set $\{m, m+1, \ldots, n\}$ is denoted by $\mathcal{K}_{m:n}$. The notation $\overset{\text{a.s.}}{=}$ denotes equal almost surely. For an edge set $\mathcal{E}$, the function $1_{\mathcal{E}}(i,j)$ is an indicator function defined to be 1 if $(i,j) \in \mathcal{E}$ and 0 otherwise. Throughout this paper, the state of a quantum system and its corresponding density matrix will be used interchangeably; the notion $\boldsymbol{\Xi}_{x,y}$ denotes a maximally entangled qubit pair between two systems x and y, each corresponding to one qubit; the notion $\boldsymbol{\Xi}_{i:j}$ denotes a maximally entangled qubit pair between two systems, where one of the systems is in node i and the other is in node j.

II. System Model

Consider a quantum network consisting of nodes equipped with quantum devices. Such a network can be abstracted by a graph consisting of nodes and edges. Let $\mathcal{N}$ and $\mathcal{E}$ denote the set of nodes and the set of edges, respectively. Each node in $\mathcal{N}$ has the capability of performing quantum measurements and storing qubits for a sufficiently long time. Consequently, each node can serve as a quantum repeater.[2] Each edge $(i,j) \in \mathcal{E}$ represents a quantum channel, and this channel can be used to generate entanglement between nodes i and j. We aim to

[2]We use "repeater" and "node" interchangeably in the rest of the paper.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.



(a) entanglement generation (b) entanglement swapping

Fig. 1. An illustration of entanglement generation and entanglement swapping. In (a), nodes i and k are connected by a quantum channel, and so are nodes k and j. Purple lines represent generated entangled qubit pairs. Entanglement can be generated between i and k. In (b), the node k performs entanglement swapping using $\boldsymbol{\Xi}_{i:k}$ and $\boldsymbol{\Xi}_{k:j}$ to distribute $\boldsymbol{\Xi}_{i:j}$. Blue lines represent distributed entangled qubit pairs.

distribute entanglement at two remote nodes with the help of quantum repeaters for general networks. Note that we are particularly interested in homogeneous repeater chains, a special case of quantum networks with desired properties, and will discuss them in Section IV.

There are two essential operations in RED: entanglement generation and entanglement swapping, as illustrated in Fig. 1.

- Entanglement generation - For $(i,k) \in \mathcal{E}$, nodes i and k are connected by a quantum channel. Nodes i and k can attempt to generate[3] entangled qubit pairs (grey dots connected by purple dashed lines in Fig. 1(a)). Entanglement generation can be implemented, for example, by locally preparing an entangled qubit pair at one of the nodes (e.g., i) and sending one entangled qubit in this pair to the other node (e.g., k) [44]. The entangled qubits are stored in the nodes for a sufficiently long time. The attempt of entanglement generation may not always succeed. If the attempt succeeds, the density matrix of the entangled qubit pair is

$$\boldsymbol{\Xi}_{i_a,k_b} := \frac{1}{2}(|00\rangle_{i_a,k_b} + |11\rangle_{i_a,k_b})(\langle 00|_{i_a,k_b} + \langle 11|_{i_a,k_b})$$

  where i_a and k_b represent physical systems in node i and k, respectively; otherwise, no entangled qubit pair is obtained.
- Entanglement swapping - Entanglement swapping [45], [46] can be seen as a special case of teleportation [18]. Suppose there are three nodes i, k, and j. Node i has one qubit, node k two, and node j one. Node i's qubit and node k's first qubit are maximally entangled, and so are node k's second qubit and node j's qubit. Node k teleports the qubit entangled with the one in node i to node j. Then, the node i's qubit is entangled with node j's even though these two nodes have never directly interacted with each other. This operation is referred to as entanglement swapping. The attempt of entanglement swapping may not always succeed. If the attempt succeeds, one entangled qubit pair $\boldsymbol{\Xi}_{i:j}$ is distributed; otherwise, no entangled qubit pair is obtained even though the two entangled qubit pairs are consumed.

[3]In this paper, we use the term "generate/generation" to describe the operation of preparing an entangled qubit pair at one node and sending one of the qubits through a quantum channel; we use the term "distribute/distribution" to describe the operation of preparing entangled qubit pairs at two nodes that are not directly connected by a quantum channel via entanglement generation and entanglement swapping. Moreover, "distribution" in entanglement distribution should not be confused with that in probability distribution.

We consider a time-slotted system in which slots are indexed by $\tau \in \mathbb{N}_+$. Each time slot is divided into two phases described below.

- Phase I: For any $(i,k) \in \mathcal{E}$, nodes i and k can make an attempt to generate an entangled qubit pair with success probability of $p_{i:k}$.[4]
- Phase II: For any $i,j,k \in \mathcal{N}$, node k can attempt to perform entanglement swapping with success probability q_k to distribute entanglement $\boldsymbol{\Xi}_{i:j}$ using $\boldsymbol{\Xi}_{i:k}$ and $\boldsymbol{\Xi}_{k:j}$.

Note that the model for entanglement generation includes the lossy optical channel, which is commonly used for quantum communication. The results presented in this paper can be extended to a general quantum channel by replacing $p_{i:j}$ with the quantum channel capacity between i and j, $\forall (i,j) \in \mathcal{E}$.

We are interested in designing efficient RED protocols for scheduling entanglement swapping in the network so that a large number of entangled qubit pairs can be distributed between a source node s and a sink node t ($s,t \in \mathcal{N}$). The node s may be remote from the node t. Once an entangled qubit pair between s and t is distributed, it is stored and will not be used for entanglement swapping. For a given network described by $\mathcal{N}$, $\mathcal{E}$, and $\{p_{i:j}\}_{(i,j)\in\mathcal{E}}$, our goal is to maximize the EDR achieved by a protocol π, i.e.,

$$\lambda^\pi = \liminf_{T\to\infty} \frac{1}{T}\sum_{\tau=1}^{T} \mathbb{E}\{\mathrm{g}^\pi_{s:t}(\tau)\} \tag{1}$$

where $\mathrm{g}^\pi_{s:t}(\tau)$ denotes the number of entangled qubit pairs (EQPs) generated and/or distributed between s and t distributed at time slot τ using an RED protocol π. The maximum EDR over all RED protocols is denoted by λ^*.

III. Imperfect Entanglement Swapping Operation

In this section, we determine the maximum EDR λ^* and design the optimal RED protocol.

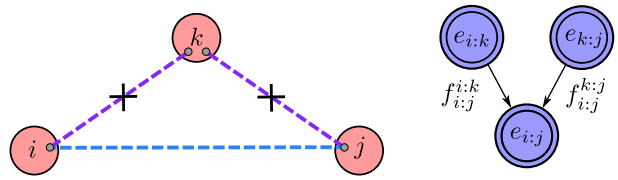
A. Optimal EDR

Analyzing entanglement swapping directly on the original network is cumbersome because the entanglement swapping operation involve pairs of nodes rather than individual nodes. Such difficulty motivates us to consider a new graph in which each node represents a pair of nodes in $\mathcal{N}$. Specifically, we introduce a directed graph $\mathcal{G}$ as described below.

- A node in $\mathcal{G}$ corresponds to a pair of nodes in $\mathcal{N}$, denoted by $e_{i:k}$ for some $i,k \in \mathcal{N}$. To distinguish the nodes in $\mathcal{G}$ from those in $\mathcal{N}$, we refer to $e_{i:k}$, $i,k \in \mathcal{N}$ in $\mathcal{G}$ as *enodes*. We do not differentiate the order of the two nodes i and k in an enode, i.e., $e_{i:k} = e_{k:i}$. These enodes represent the entangled qubit pairs.
- Let a nonnegative number $f^{i:k}_{i:j}$ denote the *eflow* from $e_{i:k}$ to $e_{i:j}$. If $f^{i:k}_{i:j} > 0$, there is a directed edge from the enode $e_{i:k}$ to the enode $e_{i:j}$. The eflow $f^{i:k}_{i:j}$ represents the amount of EQPs $\boldsymbol{\Xi}_{i:k}$ used for distributing

[4]Note that this probability does not rely on the order of i and k, i.e., $p_{i:k} = p_{k:i}$.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.



(a) entangled qubit pair $\Xi_{i:j}$ (b) enodes and eflow

Fig. 2. An illustration of enodes and eflows. In (a), the node k performs entanglement swapping using $\Xi_{i:k}$ and $\Xi_{k:j}$ to distribute $\Xi_{i:j}$. Correspondingly, in (b), the enodes $e_{i:k}$ and $e_{k:j}$ contribute eflows to $e_{i:j}$ with $f_{i:j}^{i:k}$ and $f_{i:j}^{k:j}$, respectively.

$\Xi_{i:j}$ via entanglement swapping. Since the order of the two nodes in an enode is not differentiated, we have $f_{i:j}^{i:k} = f_{i:j}^{k:i} = f_{j:i}^{i:k} = f_{j:i}^{k:i}$. However, $f_{i:k}^{i:j}$ is not necessarily equal to $f_{i:j}^{i:k}$.

An illustration of the enode and eflow is depicted in Fig. 2. The next theorem provides an upper bound for the optimal EDR. This upper bound is based on an optimization problem, where the variables are the eflows.

Theorem 1: For a given graph with node set $\mathcal{N}$, edge set $\mathcal{E}$, entanglement generation success probability $\{p_{i:j} : (i,j) \in \mathcal{E}\}$, and entanglement swapping success probability $\{q_k : k \in \mathcal{N}\}$, the optimal EDR is upper-bounded by the optimal value of the following problem $\mathscr{P}$:

$$\begin{aligned}
\mathscr{P}: \quad & \underset{\{f_{i:j}^{i:k}: i,j,k\in\mathcal{N}\}}{\text{maximize}} \quad I(s,t) \\
& \text{subject to} \quad I(i,j) \geq \sum_{k\in\mathcal{N}\setminus\{i,j\}} (f_{i:k}^{i:j} + f_{k:j}^{i:j}), \\
& \qquad i,j \in \mathcal{N}, \qquad \{i,j\} \neq \{s,t\} \quad (2) \\
& \qquad f_{i:j}^{i:k} = f_{i:j}^{k:j} \geq 0, \quad i,j,k \in \mathcal{N} \quad (3) \\
& \qquad f_{s:k}^{s:t} = f_{k:t}^{s:t} = 0, \quad k \in \mathcal{N} \quad (4)
\end{aligned}$$

where for $i,j \in \mathcal{N}$,

$$I(i,j) = p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \frac{f_{i:j}^{i:k} + f_{i:j}^{k:j}}{2}.$$

Proof: See Appendix I. □

Remark 1: The objective function and the constrains of $\mathscr{P}$ can be interpreted as follows. The objective function $I(s,t)$ represents the amount of $\Xi_{s:t}$ generated/distributed between the source node and the sink node. The constraint (2) represents the entanglement balance corresponding to an arbitrary enode $e_{i:j}$. In particular, the left hand side of (2) represents the amount of $\Xi_{s:t}$ generated/distributed between node i and node j; the right hand side of (2) represents the amount of $\Xi_{i:j}$ that is used for distributing other entanglement. The constraint (3) represents the symmetry in entanglement swapping. In particular, in entanglement swapping, the amount of $\Xi_{i:k}$ and $\Xi_{k:j}$ consumed to distribute $\Xi_{i:j}$ needs to be the same. The constraint (4) represents the requirement that the entanglement $\Xi_{s:t}$ is not used for entanglement swapping.

Remark 2: The problem $\mathscr{P}$ is a linear programming problem. The computational complexity of $\mathscr{P}$ depends on the numbers of variables and constraints, and both numbers are $\text{poly}(\text{Card}(\mathcal{N}))$ [47]–[50]. Therefore, the optimal solution of the problem $\mathscr{P}$ can be obtained efficiently by standard linear optimization algorithms. Note that optimization techniques have been used to solve problems on quantum information science [51]–[54].

We next determine some structural properties of a graph that corresponds to an optimal solution of $\mathscr{P}$.

B. Structural Properties

Definition 1 (Directed acyclic graph): A directed acyclic graph (DAG) is a directed graph with no directed cycle.

Proposition 1: There exists an optimal solution of $\mathscr{P}$ such that the graph $\mathcal{G}$ corresponding to this solution is a DAG.

Proof: See Appendix II. □

There are some standard concepts such as isolated node, parent, child, ancestor, and descendant for DAGs and we can employ them in the graph consisting of enodes.

Definition 2 (Efficiency): A directed graph consisting of enodes is efficient if for every enode $e_{i:j}$ except for $e_{s:t}$, either $e_{i:j}$ is isolated or $e_{i:j}$ is an ancestor of $e_{s:t}$.

Proposition 2: There exists an optimal solution of $\mathscr{P}$ such that the graph corresponding to this solution is acyclic and efficient.

Proof: See Appendix III. □

The constraint (2) in the problem $\mathscr{P}$ can be interpreted as follows: the incoming flow into the enode $e_{i:j}$ is no less than the outgoing flow. If the equality does not hold, some of the entanglement will be wasted. To reduce such waste, we introduce *control variables* $\{u_{i:j} : (i,j) \in \mathcal{E}\}$ for limiting the number of generated EQPs, which induces the following problem $\mathscr{P}_{\text{s}}$:

$$\begin{aligned}
\mathscr{P}_{\text{s}}: \quad & \underset{\substack{\{f_{i:j}^{i:k}: i,j,k\in\mathcal{N}\} \\ \{u_{i:j}:(i,j)\in\mathcal{E}\}}}{\text{maximize}} \quad I(s,t) \\
& \text{subject to} \quad u_{i:j} p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \frac{f_{i:j}^{i:k} + f_{i:j}^{k:j}}{2} \\
& \qquad = \sum_{k\in\mathcal{N}\setminus\{i,j\}} (f_{i:k}^{i:j} + f_{k:j}^{i:j}), \\
& \qquad i,j \in \mathcal{N}, \qquad \{i,j\} \neq \{s,t\} \quad (5) \\
& \qquad f_{i:j}^{i:k} = f_{i:j}^{k:j} \geq 0, \quad i,j,k \in \mathcal{N} \quad (6) \\
& \qquad f_{s:i}^{s:t} = f_{t:i}^{s:t} = 0, \quad i \in \mathcal{N} \quad (7) \\
& \qquad 0 \leq u_{i:j} \leq 1, \quad (i,j) \in \mathcal{E}. \quad (8)
\end{aligned}$$

Evidently, if $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ is an optimal solution of $\mathscr{P}_{\text{s}}$, then $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ is a feasible solution of $\mathscr{P}$. The next theorem implies that $\mathscr{P}$ and $\mathscr{P}_{\text{s}}$ are equivalent.

Theorem 2: The optimal value of $\mathscr{P}_{\text{s}}$ is the same as that of $\mathscr{P}$. Moreover, there exists an optimal solution of $\mathscr{P}_{\text{s}}$ such that the graph corresponding to this solution is acyclic and efficient.

Proof: See Appendix IV. □

Theorems 1 and 2 show that the optimal value of $\mathscr{P}_{\text{s}}$ is an upper bound for the EDR. Next we will show that this bound is tight; in particular, we will design an RED protocol

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

that achieves this bound. The RED protocol will employ the optimal solution of $\mathscr{P}_{\rm s}$.

C. Stationary Protocol

By Theorem 2, we can consider an optimal solution $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ of $\mathscr{P}_{\rm s}$ such that the graph corresponding to this solution is acyclic and efficient. This solution will be used to develop the RED protocol. Note that topological ordering is possible for a DAG consisting of enodes, and we can find a linear ordering of all the enodes, such that if $f_{i:j}^{i:k} > 0$, the enode $e_{i:k}$ precedes the enode $e_{i:j}$ in the ordering.

For each enode $e_{i:k}$ that has a descendant $e_{s:t}$ in $\mathcal{G}$, we consider a set $\mathcal{M}_{i:k}$, consisting of the EQPs between i and k; we also consider a collection of sets, denoted as $\mathcal{F}_{i:j}^{i:k}$ and $\mathcal{F}_{j:k}^{i:k}$, $j \in \mathcal{N}\setminus\{i,k\}$, consisting of the EQPs between i and k that will be used for distributing $\boldsymbol{\Xi}_{i:j}$ and $\boldsymbol{\Xi}_{j:k}$, respectively. This stationary protocol, denoted by $\mathring{\pi}$, is described below.

- In Phase I,
  - For any $(i,k) \in \mathcal{E}$, nodes i and k attempt to generate an entangled qubit pair $\boldsymbol{\Xi}_{i:k}$ with the probability $\mathring{u}_{i:k}$.[5] If the attempt is successful, the entangled qubit pair $\boldsymbol{\Xi}_{i:k}$ is moved to the set $\mathcal{M}_{i:k}$.
  - For every enode $e_{i:k}$, if $e_{i:k} \neq e_{s:t}$, we move each EQP $\boldsymbol{\Xi}_{i:k}$ in $\mathcal{M}_{i:k}$ to the set $\mathcal{F}_{i:j}^{i:k}$ or the set $\mathcal{F}_{j:k}^{i:k}$, $j \in \mathcal{N}\setminus\{i,k\}$ randomly. In particular,

$$\mathbb{P}\{\text{move } \boldsymbol{\Xi}_{i:k} \text{ to } \mathcal{F}_{i:j}^{i:k}\} = \frac{\mathring{f}_{i:j}^{i:k}}{\sum_{l\in\mathcal{N}\setminus\{i,k\}}(\mathring{f}_{i:l}^{i:k}+\mathring{f}_{l:k}^{i:k})} \quad (9)$$

$$\mathbb{P}\{\text{move } \boldsymbol{\Xi}_{i:k} \text{ to } \mathcal{F}_{j:k}^{i:k}\} = \frac{\mathring{f}_{j:k}^{i:k}}{\sum_{l\in\mathcal{N}\setminus\{i,k\}}(\mathring{f}_{i:l}^{i:k}+\mathring{f}_{l:k}^{i:k})}. \quad (10)$$

- In Phase II, for every $i,j,k \in \mathcal{N}$, the node k performs entanglement swapping to distribute $\boldsymbol{\Xi}_{i:j}$ using $\boldsymbol{\Xi}_{i:k}$ in $\mathcal{F}_{i:j}^{i:k}$ and $\boldsymbol{\Xi}_{k:j}$ in $\mathcal{F}_{i:j}^{k:j}$ until the set $\mathcal{F}_{i:j}^{i:k}$ or $\mathcal{F}_{i:j}^{k:j}$ is empty. The distributed EQPs between i and j are then moved to $\mathcal{M}_{i:j}$.

Note that the target entangled qubit pair $\boldsymbol{\Xi}_{s:t}$ is in $\mathcal{M}_{s:t}$. We claim that the number of entangled qubit pairs that the enode $e_{i:j}$ has accumulated after sufficiently large time slot T in $\mathcal{G}$, denoted by $\mathsf{n}_{i:j}(T)$, satisfies

$$\lim_{T\to\infty}\frac{1}{T}\mathsf{n}_{i:j}(T) \overset{\text{a.s.}}{=} u_{i:j}p_{i:j}1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \frac{\mathring{f}_{i:j}^{i:k}+\mathring{f}_{i:j}^{k:j}}{2}. \quad (11)$$

This claim can be rewritten as follows: for any $x \in \mathcal{K}_{1:\text{Card}(\mathcal{G})}$, the equation (11) holds, where $e_{i:j}$ denotes the xth enode in the topological order of $\mathcal{G}$. This claim can be proved by the strong mathematical induction on the position x of an enode in the topological order determined by $\mathcal{G}$ [55].

Base case: If $x = 1$, then $\mathring{f}_{i:j}^{i:k} = \mathring{f}_{i:j}^{k:j} = 0$ for $\forall k \in \mathcal{N}$, and by the strong law of large numbers, the number of the EQPs $\boldsymbol{\Xi}_{i:j}$ accumulated in the enode $e_{i:j}$ satisfies

$$\lim_{T\to\infty}\frac{1}{T}\mathsf{n}_{i:j}(T) \overset{\text{a.s.}}{=} u_{i:j}p_{i:j}1_{\mathcal{E}}(i,j)$$

which equals (11) with $\mathring{f}_{i:j}^{i:k} = \mathring{f}_{i:j}^{k:j} = 0$ for $\forall k \in \mathcal{N}$.

Induction step: Suppose equation (11) holds for $x = 1,2,\ldots,r$. We will prove (11) holds for $x = r+1$. For $k \in \mathcal{N}\setminus\{i,j\}$, if $\mathring{f}_{i:j}^{i:k} > 0$, then the enode $e_{i:k}$ precedes $e_{i:j}$ in the topological ordering, showing that the position of $e_{i:k}$ is less than $r+1$. By the induction hypothesis,

$$\lim_{T\to\infty}\frac{1}{T}\mathsf{n}_{i:k}(T) \overset{\text{a.s.}}{=} u_{i:k}p_{i:k}1_{\mathcal{E}}(i,k) + \sum_{l\in\mathcal{N}\setminus\{i,k\}} q_l \frac{\mathring{f}_{i:k}^{i:l}+\mathring{f}_{i:k}^{l:k}}{2}. \quad (12)$$

Consequently, the number of the EQPs $\boldsymbol{\Xi}_{i:k}$ consumed for distributing $\boldsymbol{\Xi}_{i:j}$, denoted by $\mathsf{d}_{i:j}^{i:k}(T)$, satisfies

$$\begin{aligned}\lim_{T\to\infty}\frac{1}{T}\mathsf{d}_{i:j}^{i:k}(T) &\overset{\text{a.s.}}{=} \lim_{T\to\infty}\frac{1}{T}\Big[\mathsf{n}_{i:k}(T)\,\mathbb{P}\{\text{move } \boldsymbol{\Xi}_{i:k} \text{ to } \mathcal{F}_{i:j}^{i:k}\}\Big] \\ &\overset{\text{a.s.}}{=} \mathring{f}_{i:j}^{i:k} \end{aligned} \quad (13)$$

where we have used (12) and (9) together with (5) to obtain (13). Similarly, we have

$$\lim_{T\to\infty}\frac{1}{T}\mathsf{d}_{i:j}^{k:j}(T) \overset{\text{a.s.}}{=} \mathring{f}_{i:j}^{k:j}. \quad (14)$$

Then

$$\begin{aligned}\lim_{T\to\infty}\frac{1}{T}\mathsf{n}_{i:j}(T) &\overset{\text{a.s.}}{=} u_{i:j}p_{i:j}1_{\mathcal{E}}(i,j) \\ &\quad + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \lim_{T\to\infty}\frac{1}{T}\min\{\mathsf{d}_{i:j}^{i:k}(T), \mathsf{d}_{i:j}^{k:j}(T)\} \\ &\overset{\text{a.s.}}{=} u_{i:j}p_{i:j}1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \frac{\mathring{f}_{i:j}^{i:k}+\mathring{f}_{i:j}^{k:j}}{2}\end{aligned}$$

where the summand $T\,u_{i:j}p_{i:j}1_{\mathcal{E}}(i,j)$ comes from direct entanglement generation, and the rest of the summand comes from entanglement swapping due to (13) and (14). This proves that (11) holds for $x = r+1$.

Note that

$$\begin{aligned}\lim_{T\to\infty}\mathbb{E}\Big\{\frac{1}{T}\mathsf{n}_{s:t}(T)\Big\} &= \mathbb{E}\Big\{\lim_{T\to\infty}\frac{1}{T}\mathsf{n}_{s:t}(T)\Big\} \\ &= p_{s:t}1_{\mathcal{E}}(s,t) + \sum_{k\in\mathcal{N}\setminus\{s,t\}} q_k \frac{\mathring{f}_{s:t}^{s:k}+\mathring{f}_{s:t}^{k:t}}{2} \\ &= \mathring{I}(s,t)\end{aligned}$$

where $\mathring{I}(s,t)$ denotes the optimal value of $\mathscr{P}_{\rm s}$ and the first equality is due to the dominated convergence theorem [56]. protocol $\mathring{\pi}$ is

$$\lambda^{\mathring{\pi}} = \liminf_{T\to\infty}\frac{1}{T}\mathbb{E}\{\mathsf{n}_{s:t}(T)\} = \lim_{T\to\infty}\frac{1}{T}\mathbb{E}\{\mathsf{n}_{s:t}(T)\} = \mathring{I}(s,t)$$

where the second equality is due to the existence of the limit. This shows that the protocol $\mathring{\pi}$ achieves the maximum EDR.

IV. Homogeneous Repeater Chains

In this section, we consider a special quantum network, homogeneous repeater chains, and derive the solution for $\mathscr{P}_{\rm s}$ in a closed form.

[5]The control variable $\mathring{u}_{i:k}$ is the probability of attempting to generate entanglements. Note that only if they make the attempt *and* the attempt is successful, can an entangled qubit pair be generated between nodes i and k. Hence, an entangled qubit pair can be generated with probability $\mathring{u}_{i:k}p_{i:k}$.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

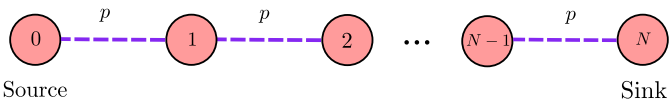


Fig. 3. Illustration of repeater chains. The purple dashed lines represent the quantum channels between neighboring nodes.

A. Network Model

The model of homogeneous repeater chains is described in several related works, e.g., [41]. A repeater chain is connected by N quantum channels as illustrated in Fig. 3. Specifically, the nodes are labeled as 0, 1, 2, ..., N and the edge set $\mathcal{E} = \{(0,1),(1,2),(2,3),\ldots,(N-1,N)\}$. Each edge $(i-1,i)$ has associated probability $p_{i-1:i}$ describing the probability of success in generating entangled qubit pair $\boldsymbol{\Xi}_{i-1:i}$. The node 0 and the node N are the source and sink nodes, respectively. The enode $e_{s:t}$ is then $e_{0:N}$. In a homogeneous repeater chain, the quantum channels between neighboring nodes are the same, i.e., $p := p_{0:1} = p_{1:2} = p_{2:3} = \ldots = p_{N-1:N}$. Furthermore, the success probability of entanglement swapping in the chain is assumed to be the same for all nodes and denoted by q.

Section III shows that designing the optimal RED protocol is equivalent to solving the optimization problem $\mathscr{P}_{\rm s}$. Here, we aim at solving $\mathscr{P}_{\rm s}$ corresponding to homogeneous repeater chains. We have the following result:

Claim 1: For homogeneous repeater chains connected by N quantum channels, the maximal EDR is

$$\frac{(N-\xi(N))\,pq^{n+1}}{2(N-2^n)+(2^{n+1}-N-\xi(N))\,q} \tag{15}$$

where $n = \lceil \log_2 N \rceil - 1$, and $\xi(N)$ is a parity indicator function of N: $\xi(N) = 1$ if N is odd, otherwise $\xi(N) = 0$.

The proof of the claim and the design of the optimal protocol will be discussed in the next subsections.

B. Scenarios With an Even N

We consider the scenario where N is even, i.e., $N \in \mathbb{Z}_{\rm e}$. We first present a solution of $\mathscr{P}_{\rm s}$, denoted by $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$, and then prove that it is the optimal solution of $\mathscr{P}_{\rm s}$.

Let $n = \lceil \log_2 N \rceil - 1$. If $N = 2^{n+1}$, the solution $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ of $\mathscr{P}_{\rm s}$ is

$$\begin{aligned} &\mathring{u}_{k:k+1} = 1, \quad k \in \mathcal{K}_{0:N-1} \\ &\mathring{f}_{2^k a:2^k a+2^{k-1}}^{2^k a:2^k a+2^k} = \mathring{f}_{2^k a:2^k a+2^k}^{2^k a+2^{k-1}:2^k a+2^k} = pq^{k-1} \end{aligned}$$

with $a = 0,1,2,\ldots,2^{n+1-k}-1$ and $k = 1,2,\ldots,n+1$.

For example, if $a = 1$ and $k = 2$, then $2^k a = 4$, $2^k a + 2^{k-1} = 6$, $2^k a + 2^k = 8$, and consequently $\mathring{f}_{4:8}^{4:6} = \mathring{f}_{4:8}^{6:8} = pq$. An illustration of this solution for $N = 8$ is given in Fig. 4. This solution corresponds to a graph with the structure of a perfect binary tree. Specifically, the entanglement swapping is first performed between the enodes $e_{2a:2a+1}$ and $e_{2a+1:2a+2}$, and this gives the EQPs corresponding to the enode $e_{2a:2a+2}$, for

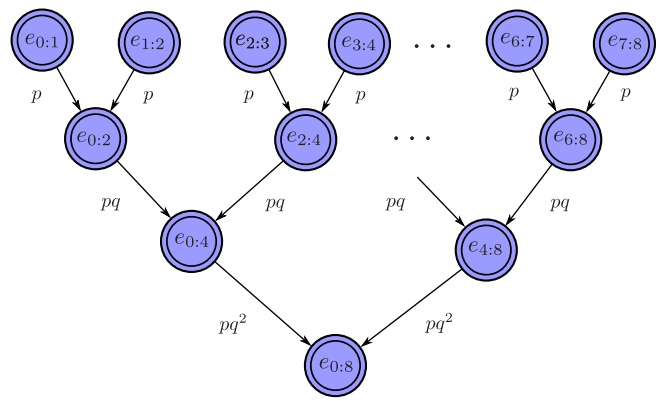


Fig. 4. Illustration of the optimal RED protocol for $N = 8 = 2^3$. The quantities near the edges represent the eflow.

$a = 0,1,2,\ldots,N/2-1$. Then the entanglement swapping is performed between $e_{4a:4a+2}$ and $e_{4a:4a+4}$, and this gives the EQPs corresponding to the enode $e_{4a:4a+4}$, for $a = 0,1,2,\ldots,N/4-1$. Such entanglement swapping can continue until the EQPs corresponding to the enode $e_{0:N}$ are obtained.

If $N < 2^{n+1}$, the solution $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ can be obtained in six steps described below.

1) $\mathring{u}_{k:k+1} = 1$, $k \in \mathcal{K}_{0:N-1}$.
2) Consider the enode: $e_{0:1}$, $e_{1:2}$, ..., $e_{N-1:N}$ and divide them into $N/2$ pairs of enodes: $e_{0:1}$ and $e_{1:2}$, $e_{2:3}$ and $e_{3:4}$, ..., $e_{N-2:N-1}$ and $e_{N-1:N}$.
3) There are $\binom{N/2}{N-2^n}$ possible ways to choose $(N-2^n)$ out of $N/2$ enode pairs. These choices are labeled as 1, 2, ..., $\binom{N/2}{N-2^n}$.
4) For the choice l, we have $(N-2^n)$ enode pairs chosen. Entanglement swapping is performed between two enodes in each chosen pair, resulting in an enode that is the common child of these two enodes; now we have a chain consisting of 2^n quantum channels and we can relabel the nodes in the chain as $\overline{0}$, $\overline{1}$, ..., $\overline{2^n}$.
5) For the newly labeled chain, determine the following eflow:

$$\begin{aligned} &\mathring{f}_{\overline{2^k a}:\overline{2^k a+2^{k-1}}}^{\overline{2^k a}:\overline{2^k a+2^k}}(l) \\ &\quad = \mathring{f}_{\overline{2^k a}:\overline{2^k a+2^k}}^{\overline{2^k a+2^{k-1}}:\overline{2^k a+2^k}}(l) \\ &\quad = \frac{1}{\binom{N/2}{N-2^n}} \frac{N/2}{N-2^n+q(2^n-N/2)}\, pq^k \end{aligned}$$

with $a = 0,1,2,\ldots,2^{n-k}-1$ and $k = 1,2,\ldots,n+1$.
6) Repeat Steps 4 and 5 until all $\binom{N/2}{N-2^n}$ combinations are iterated. Add all the eflows to obtain the optimal solution.

In Step 3, we transfer the problem from the scenario with $N \in \mathbb{Z}_{\rm e}$ to the scenario where N is a power of two. An illustration of this step is in Fig. 5. The method of determining $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ for $N = 6$ is illustrated in Fig. 6.

Remark 3: The feasibility of the $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ as a solution of $\mathscr{P}_{\rm s}$ can be verified by checking conditions (5)-(8). The value of the objective

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

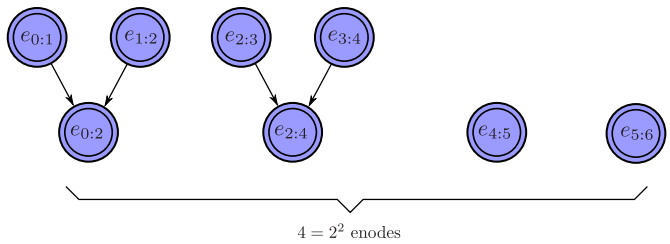


Fig. 5. Illustration of Step 3 for $N = 6$. In this case, $n = \lceil \log_2 6 \rceil - 1 = 2$. We choose $N - 2^n = 2$ pairs of enodes. In this figure, the two chosen pairs are: $e_{0:1}$ and $e_{1:2}$; $e_{2:3}$ and $e_{3:4}$. Entanglement swapping between $e_{0:1}$ and $e_{1:2}$ results in the enode $e_{0:2}$; entanglement swapping between $e_{2:3}$ and $e_{3:4}$ results in the enode $e_{2:4}$. We now have a chain consisting of $2^2 = 4$ quantum channels, separated by the repeaters 0, 2, 4, 5, and 6. These five repeaters are relabelled as $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$.

function corresponding to this solution is

$$\mathring{I}(s,t) = \frac{1}{\binom{N/2}{N-2^n}} \frac{N/2}{N - 2^n + q(2^n - N/2)} pq^{n+1} \binom{N/2}{N-2^n} = \frac{Np}{g(N)}$$

where $g(\cdot)$ is a function defined as

$$g(L) = \frac{2(L - 2^l) + q(2^{l+1} - L)}{q^{l+1}} \tag{16}$$

in which $l = \lceil \log_2 L \rceil - 1$.

We next determine an upper bound for the optimal value of $\mathscr{P}_{\mathrm{s}}$ for $N \in \mathbb{Z}_{\mathrm{e}}$. If this upper bound coincides with $\mathring{I}(s,t)$, then the optimality of $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ will be proved.

Note that the EQPs generated in Phase I correspond to the term $u_{i:j} p_{i:j} 1_{\mathcal{E}}(i,j)$ in $\mathscr{P}_{\mathrm{s}}$. These EQPs are generated directly from quantum channels instead of entanglement swapping. In the rest of the section, these EQPs are referred to as "crude entanglements." We now consider a homogeneous repeater chain with infinite quantum channels. For this chain, let $h(L)$ denote the minimum expected number of crude entanglements required to distribute one EQP shared between nodes that are connected by L quantum channels. The upper bound for the optimal value of $\mathscr{P}_{\mathrm{s}}$ relies on the lower bound for $h(L)$. The next proposition provides a lower bound for $h(L)$.

Proposition 3: For $N \in \mathbb{N}_+$, the minimum expected number of crude entanglements required to distribute one EQP shared between nodes that are connected by N quantum channels, denoted by $h(N)$, is lower bounded as

$$g(N) \le h(N) \tag{17}$$

where $g(N)$ is defined in (16).

Proof: See Appendix V. □

Theorem 3: For homogeneous repeater chains with N quantum channels, if $N \in \mathbb{Z}_{\mathrm{e}}$, the maximum EDR is

$$\lambda^* = \frac{Npq^{n+1}}{2(N - 2^n) + q(2^{n+1} - N)}$$

where $n = \lceil \log_2 N \rceil - 1$.

Proof: In the homogeneous repeater chain, the expected number of available crude entanglements generated across N quantum channels is at most pN per time slot. As a consequence, the expected number of available crude entanglements generated across N quantum channels is at most pNT after T time slots. Moreover, by definition of $h(\cdot)$, it requires $h(N)$ crude entanglements on average to obtain one EQP between nodes s and t. Therefore, the expected number of EQPs between s and t is at most $pNT/h(N)$ after T time slots. This implies for any protocol π,

$$\lambda^\pi = \liminf_{T\to\infty} \frac{1}{T} \sum_{\tau=1}^{T} \mathbb{E}\{\mathrm{g}_{s:t}^{\pi}(\tau)\} \le \liminf_{T\to\infty} \frac{1}{T} \frac{pNT}{h(N)} = \frac{Np}{h(N)}.$$

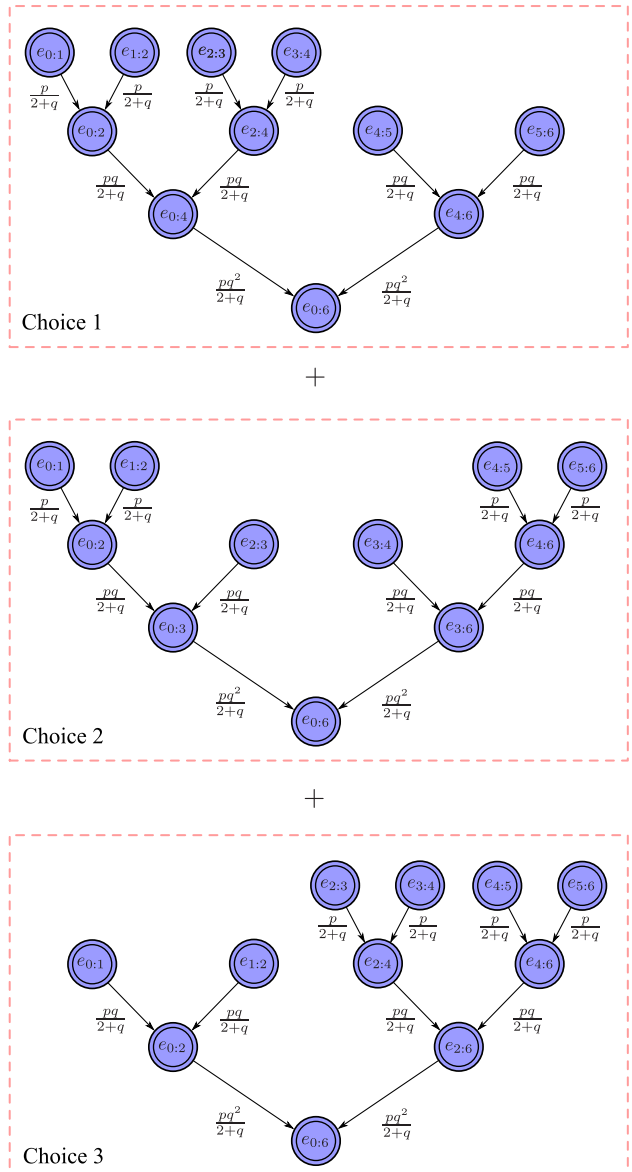


Fig. 6. An illustration of the solution for $N = 6$. The quantities near the edges represent the eflow. In this case, $n = \lceil \log_2 6 \rceil - 1 = 2$. We divide six enodes into three pairs: $e_{0:1}$ and $e_{1:2}$, $e_{2:3}$ and $e_{3:4}$, as well as $e_{4:5}$ and $e_{5:6}$. There are three possible ways of choosing $N - 2^n = 2$ out of $N/2 = 3$ pairs. The choices are labeled as 1, 2, and 3, and are shown in three red rectangles. In each rectangle, we perform the Steps 4 and 5. The eflows in three rectangles can then be added to obtain the optimal solution of $\mathscr{P}_{\mathrm{s}}$.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

Together with Proposition 3, we have the upper bound of the EDR for any protocol:

$$\lambda^{\pi} \leq \frac{Np}{g(N)} = \frac{Npq^{n+1}}{2(N-2^n)+q(2^{n+1}-N)}.$$

Note that $\mathring{I}(s,t)$ in Remark 3 coincides with the upper bound above. Therefore, $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ is the optimal solution of $\mathscr{P}_{\mathrm{s}}$, and this upper bound is indeed the maximum EDR because of Theorem 2. □

C. Scenarios With an Odd N

We consider the scenario where N is odd, i.e., $N \in \mathbb{Z}_{\mathrm{o}}$. We first present a solution of $\mathscr{P}_{\mathrm{s}}$, denoted by $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$, and then prove that it is the optimal solution of $\mathscr{P}_{\mathrm{s}}$.

Let $n = \lceil \log_2 N \rceil - 1$. The solution $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ can be obtained in six steps described below.

1) $\mathring{u}_{k:k+1} = 1$, $k \in \mathcal{K}_{0:N-2}$ and
$$\mathring{u}_{N-1:N} = q\,\frac{(N-1)}{2N-2^{n+1}+q(2^{n+1}-N-1)}.$$
2) Consider the enodes: $e_{0:1}, e_{1:2}, \ldots, e_{N-2:N-1}$ and divide them into $(N-1)/2$ pairs of enodes: $e_{0:1}$ and $e_{1:2}$, $e_{2:3}$ and $e_{3:4}$, $\ldots$, $e_{N-3:N-2}$ and $e_{N-2:N-1}$.
3) There are $\binom{(N-1)/2}{N-2^n}$ possible ways to choose $(N-2^n)$ out of $(N-1)/2$ enode pairs. These choices are labeled as 1, 2, $\ldots$, $\binom{(N-1)/2}{N-2^n}$.
4) For the choice l, we have $(N-2^n)$ enode pairs chosen. Entanglement swapping is performed between two enodes in each chosen pair, resulting in an enode that is the common child of these two enodes; now we have a chain consisting of 2^n quantum channels and we can relabel the nodes in the chain as $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{2^n}$.
5) For the newly labeled chain, determine the following eflow:
$$\begin{aligned}&\mathring{f}_{\overline{2^k a}:\overline{2^k a+2^{k-1}}}^{\overline{2^k a}:\overline{2^k a+2^k}}(l)\\ &\quad= \mathring{f}_{\overline{2^k a}:\overline{2^k a+2^k}}^{\overline{2^k a+2^{k-1}}:\overline{2^k a+2^k}}(l)\\ &\quad= \frac{1}{\binom{(N-1)/2}{N-2^n}}\,\frac{N-1}{2N-2^{n+1}+q(2^{n+1}-N-1)}\,pq^k\end{aligned}$$
with $a = 0,1,2,\ldots,2^{n-k}-1$ and $k = 1,2,\ldots,n+1$.
6) Repeat Steps 4 and 5 until all $\binom{(N-1)/2}{N-2^n}$ combinations are iterated. Add all the eflows to obtain the optimal solution.

In Step 3, we transfer the problem from the scenario with $N \in \mathbb{Z}_{\mathrm{o}}$ to the scenario where N is a power of two. The method of determining $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ is illustrated in Fig. 7.

Remark 4: The feasibility of the $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ as a solution of $\mathscr{P}_{\mathrm{s}}$ can be verified by checking conditions (5)-(8). The value of the objective function corresponding to the solution is

$$\mathring{I}(s,t) = \frac{N-1}{2N-2^{n+1}+q(2^{n+1}-N-1)}\,pq^{n+1}.$$

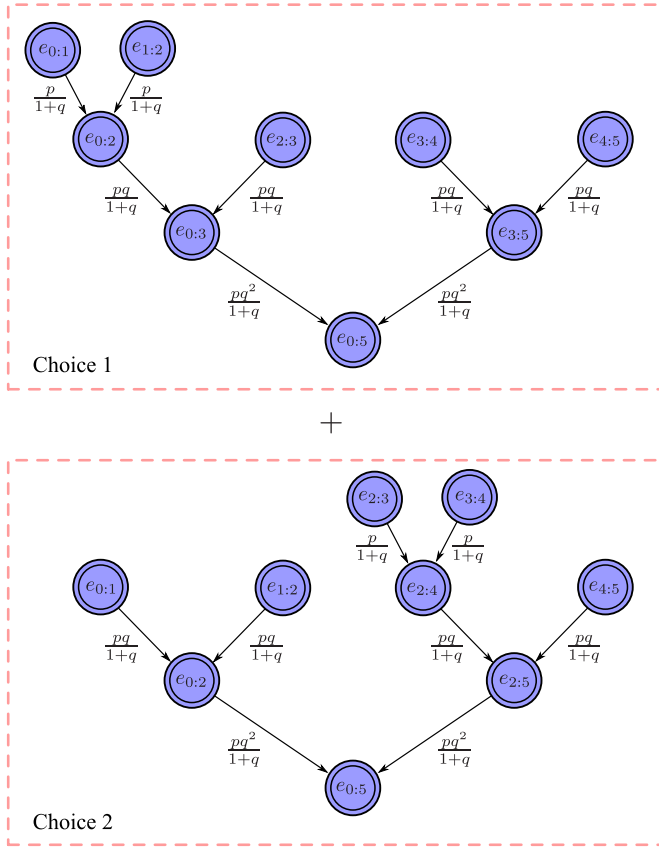


Fig. 7. An illustration of the solution for $N = 5$. The quantities near the edges represent the eflow. In this case, $n = \lceil \log_2 5 \rceil - 1 = 2$. We divide four enodes to two pairs: $e_{0:1}$ and $e_{1:2}$; as well as $e_{2:3}$ and $e_{3:4}$. There are two possible ways of choosing $N - 2^n = 1$ out of $(N-1)/2 = 2$ pairs. The choices are labeled as 1 and 2, and are shown in two red rectangles. For example in the first rectangle, the chosen pair is: $e_{0:1}$ and $e_{1:2}$. Entanglement swapping between $e_{0:1}$ and $e_{1:2}$ results in the enode $e_{0:2}$. We now have a chain consisting of $2^2 = 4$ quantum channels, separated by the repeaters 0, 2, 3, 4, and 5. These five repeaters are relabelled as $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$ and we can perform the Steps 4 and 5. After we perform the Steps 4 and 5 in each rectangle, the eflow in two rectangles can then be added to obtain the optimal solution of $\mathscr{P}_{\mathrm{s}}$.

We next determine an upper bound for the objective function of $\mathscr{P}_{\mathrm{s}}$ for $N \in \mathbb{Z}_{\mathrm{o}}$. If this upper bound coincides with $\mathring{I}(s,t)$, then the optimality of $\{\mathring{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ will be proved.

Recall that the EQPs generated in Phase I are referred to as "crude entanglements." We now refer to the crude entanglements $\Xi_{2k:2k+1}$, $k \in \mathbb{Z}$ as odd crude entanglements; analogously, we refer to the crude entanglements $\Xi_{2k-1:2k}$, $k \in \mathbb{Z}$ as even crude entanglements. We now consider a homogeneous repeater chain with infinite quantum channels. For this chain, let $h_{\mathrm{o}}(L)$ and $h_{\mathrm{e}}(L)$ denote the minimum expected number of odd crude entanglements and even crude entanglements required to distribute one entangled pair shared between nodes that are connected by L quantum channels. The upper bound for the optimal value of $\mathscr{P}_{\mathrm{s}}$ relies on the lower bounds for $h_{\mathrm{o}}(L)$ and $h_{\mathrm{e}}(L)$. The next proposition provides lower bounds for $h_{\mathrm{o}}(L)$ and $h_{\mathrm{e}}(L)$.

Proposition 4: For $N \in \mathbb{N}_+$, the minimum expected number of odd crude entanglements and even crude entanglements

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

required to distribute one entangled pair shared between nodes that are connected by N quantum channels, denoted by $h_{\rm o}(N)$ and $h_{\rm e}(N)$, respectively, satisfy the following conditions: $h_{\rm o}(1) = 1$, $h_{\rm e}(1) = 0$, if $N > 1$,

$$g_{\rm o}(N) \le h_{\rm o}(N) \text{ and } g_{\rm e}(N) \le h_{\rm e}(N)$$

where $g_{\rm o}(\cdot)$ and $g_{\rm e}(\cdot)$ are functions defined as

$$g_{\rm o}(L) = \begin{cases} \dfrac{2(L-2^l)+(2^{l+1}-L-1)\,q}{2q^{l+1}} + \dfrac{1}{q^l} & \text{if } L \in \mathbb{Z}_{\rm o} \\ \dfrac{2(L-2^l)+(2^{l+1}-L)\,q}{2q^{l+1}} & \text{if } L \in \mathbb{Z}_{\rm e} \end{cases}$$

$$g_{\rm e}(L) = \begin{cases} \dfrac{2(L-2^l)+(2^{l+1}-L-1)\,q}{2q^{l+1}} & \text{if } L \in \mathbb{Z}_{\rm o} \\ \dfrac{2(L-2^l)+(2^{l+1}-L)\,q}{2q^{l+1}} & \text{if } L \in \mathbb{Z}_{\rm e} \end{cases}$$

where $l = \lceil \log_2 L \rceil - 1$.

Proof: See Appendix VII. □

Theorem 4: For homogeneous repeater chains with N quantum channels, if $N \in \mathbb{Z}_{\rm o}$, the maximum EDR is

$$\lambda^* = \frac{(N-1)\,pq^{n+1}}{2(N-2^n)+q\,(2^{n+1}-N-1)}$$

where $n = \lceil \log_2 N \rceil - 1$.

Proof: In the homogeneous repeater chain, the expected number of the available even crude entanglements generated across N quantum channels is at most $p(N-1)/2$ per time slot. As a consequence, the expected number of available even crude entanglements generated across N quantum channels is at most $p(N-1)T/2$ after T time slots. Moreover, by definition of $h_{\rm e}(\cdot)$, it requires $h_{\rm e}(\cdot)$ even crude entanglements on average to obtain one entangled pair shared between nodes s and t. Therefore, the expected number of EQPs shared between s and t is at most $(N-1)T/(2h_{\rm e}(N))$ after T time slots. This implies for any protocol π,

$$\begin{aligned}\lambda^\pi &= \liminf_{T\to\infty} \frac{1}{T}\sum_{\tau=1}^{T} \mathbb{E}\{\mathrm{g}^\pi_{s:t}(\tau)\} \\ &\le \liminf_{T\to\infty} \frac{1}{T}\,\frac{T(N-1)\,p}{2h_{\rm e}(N)} = \frac{(N-1)\,p}{2h_{\rm e}(N)}\,.\end{aligned}$$

Together with Proposition 4, we have an upper bound of the EDR for any protocol:

$$\lambda^\pi \le \frac{(N-1)\,p}{2g_{\rm e}(N)} = \frac{(N-1)\,pq^{n+1}}{2(N-2^n)+(2^{n+1}-N-1)\,q}\,.$$

Note that $\mathring{I}(s,t)$ in Remark 4 coincides with the upper bound above. Therefore, $\{\mathring{f}^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ and $\{\mathring{u}_{i:j} : (i,j) \in \mathcal{E}\}$ is the optimal solution of $\mathscr{P}_{\rm s}$, and this upper bound is indeed the maximum EDR because of Theorem 2. □

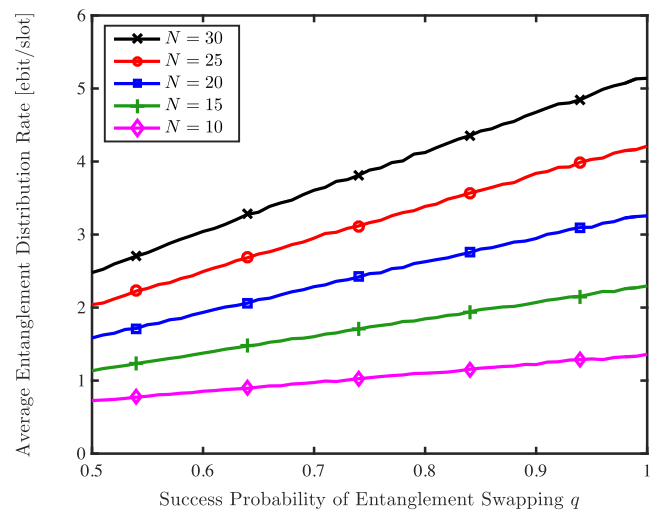


Fig. 8. The average EDR in a random network.

V. Numerical Results

This section illustrates the performance of the proposed RED protocols through numerical examples.

A. General Networks

We evaluate the maximum EDR for the following general networks. Consider a region of 60×60 km^2. The nodes are deployed in this region according to a Poisson process. Let $\mathcal{N}$ denote an instantiation of node deployment. For $i,j \in \mathcal{N}$, $(i,j) \in \mathcal{E}$ if the distance between i and j, $D_{i:j}$, is less than 30 km; the parameter $p_{i:j}$ for an edge (i,j) is

$$p_{i:j} = 10^{-\gamma D_{i:j}/10}$$

where $\gamma = 0.2$ dB/km is the loss rate [57]. The pair of source node and sink node is randomly selected with equal probability among the nodes in the network.

Consider the performance metric as the average EDR, i.e., the empirical mean of the EDR achieved by solving $\mathscr{P}_{\rm s}$ averaging over instantiations of node deployments. Fig. 8 shows the average EDR as a function of q for different values of the average node number N.[6] Theorem 2 is used to generate results in Fig. 8. First, the average EDR increases with N. For example, when $q = 0.8$, the average EDR is 1.10 ebit/slot for $N = 10$, whereas it is 4.13 ebit/slot for $N = 30$. This corresponds to an increase of 2.75 times. This is because more nodes and more edges can provide more crude entanglements for distributing the target EQP $\Xi_{s:t}$. Second, the average EDR increases with q. For example, when $N = 20$, the average EDR is 1.59 ebit/slot for $q = 0.5$, whereas it is 3.26 ebit/slot for $q = 1.0$. This corresponds to an increase of 1.05 times. This observation agrees with the intuition, since unsuccessful entanglement swapping wastes the entanglements and larger q implies less unsuccessful entanglement swapping.

We showed in Section III-C that the stationary protocol approaches the maximum EDR for large time slot T. To characterize the behavior of the stationary protocol as a function

[6]Here, the amount of entanglement is quantified by the bit of entanglement (ebit), for example, one ebit corresponds to one entangled qubit pair.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

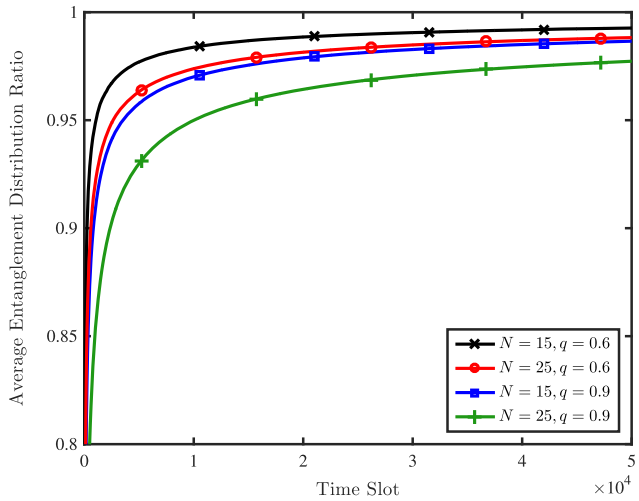


Fig. 9. The average entanglement distribution ratio in a random network.

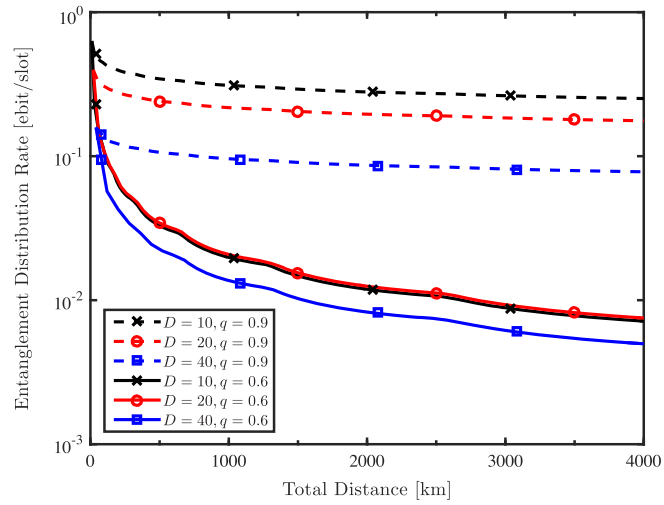


Fig. 10. The EDR in a repeater chain with $\gamma = 0.2$ dB/km.

of T, we consider the average entanglement distribution ratio at the time slot T, i.e., the empirical mean of the following random variable η_T:

$$\eta_T := \frac{\sum_{\tau=1}^{T} \mathrm{g}_{s:t}^{\mathring{\pi}}(\tau)}{T\,\lambda^*}$$

where $\mathrm{g}_{s:t}^{\mathring{\pi}}(\tau)$ is the number of EQPs at the time slot τ distributed by the stationary protocol $\mathring{\pi}$, and λ^* is the optimal value of $\mathscr{P}_{\mathrm{s}}$. The randomness of η_T originates from node deployment, parameters $p_{i:j}$, $(i,j) \in \mathcal{E}$, and the probabilistic nature of the protocol. Fig. 9 shows the average entanglement distribution ratio as a function of T for different values of N and q. First, the average entanglement distribution ratio converges to one for different values of N and q. This verifies that the proposed stationary protocol achieves the maximal EDR. Second, the convergence speed decreases with N. For example, when $q = 0.6$ and $T = 3 \cdot 10^4$, the average entanglement distribution ratio is 0.9848 for $N = 25$, whereas it is 0.9905 for $N = 15$. This is because more edges implies that there are more short paths from the source to the sink, and short paths require less entanglement swapping, so that the convergence speed can be increased.

B. Homogeneous Repeater Chains

We evaluate the maximal EDR in homogeneous repeater chains. Let D (km) denote the distance of a quantum channel in the repeater chain. Then the total distance L between the node 0 and the node N is $L = D\,N$. Let the loss rate of the channel be γ (dB/km). The parameter $p_{i:j}$ for an edge (i,j) is determined by the distance D and the loss rate γ [57]. In particular,

$$p_{i:j} = 10^{-\gamma D/10}.$$

The success probability of entanglement swapping in the network is assumed to be the same for all nodes and denoted by q. In this subsection, Claim 1 is used to generate results in the figures.

Fig. 10 shows the EDR as a function of the total distance L for $\gamma = 0.2$ dB/km. First, the EDR increases with q. This observation is consistent with the results in general networks. For example, when $D = 20$ km and $L = 1500$ km, the EDR is 0.016 ebit/slot for $q = 0.6$, whereas it is 0.205 ebit/slot for $q = 0.9$. This corresponds to an increase of 12.212 times. Second, the EDR decreases with L and the rate decreases faster with smaller q. For example, for $D = 10$, the EDR decreases 1.18 times as the total distance L increases from 1000 km to 3000 km when $q = 0.9$, whereas it decreases 2.24 times when $q = 0.6$.

We next consider the scenario where the total distance L between the source and the sink is fixed. Fig. 11 shows the EDR as a function of N for $L = 200$ km and $\gamma = 0.2$ dB/km. A key observation is that the EDR first increases dramatically and then decreases slowly as a function of N. For example, when $q = 0.6$, the EDR is 10^{-4} ebit/slot, 0.0627 ebit/slot, and 0.0288 ebit/slot for $N = 1$, $N = 21$, and $N = 100$, respectively. This corresponds to an increase of 626 times from $N = 1$ to $N = 21$, and a decrease of 54.1% from $N = 21$ to $N = 100$. The EDR first increases with N because the two neighboring quantum repeaters are far apart for a small N, and increasing N can significantly decrease D; the EDR then decreases with N because for a large N, increasing N does not significantly reduce D, and the imperfectness of quantum repeaters becomes the bottleneck of EDR. Therefore, more repeaters may not necessarily increase the EDR. The results in Fig. 11 provide guidance to the choice of repeater density in a chain and can offer insights into the design and implementation of general quantum networks.

VI. Conclusion

In this paper, we established a framework of designing RED protocols. We developed the RED protocols that achieve the maximum EDR for general quantum networks based on the solutions of the linear programming problem. Moreover, we determine the maximum EDR in a closed form for homogeneous repeater chains. The new vision developed in this paper is the introduction of enodes and eflows. RED can be seen as procedures that determine the eflows of EQPs among different enodes. We transform the RED problem into linear

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

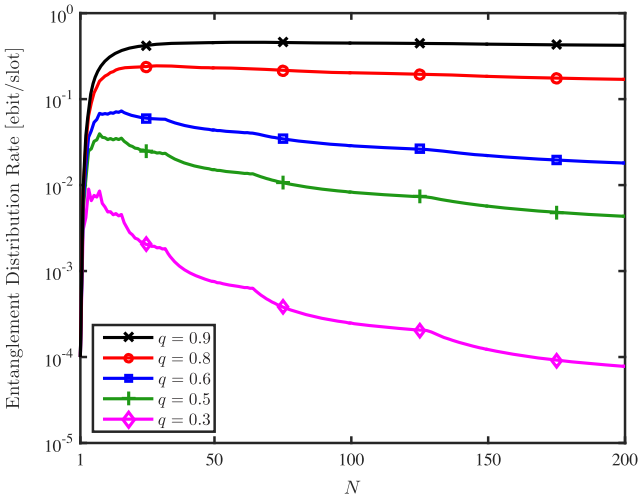


Fig. 11. The EDR in a repeater chain with N quantum channels. The total distance $L = 200$ km is fixed.

programming and employ concepts and methods from the graph theory and classical flow networks. The performance of the proposed protocols is evaluated by numerical examples. The results for homogeneous repeater chains demonstrate that the issue of significant decay of communication capacity can be essentially solved by properly deploying quantum repeaters, even if the quantum repeaters are imperfect. Our results enable the distribution of entanglement over long distances with NISQ technologies and provide insights into the design and implementation of quantum networks.

We hope that our results may incite some future work. For example, one may be interested in designing a protocol that converges to the maximum EDR faster than the protocol proposed in this paper. It may also be worth investigating quantum networks in addition to the homogeneous repeater chains and trying to determine a closed-form maximum EDR. It is also interesting to see how to extend the results in this paper to other models. For example, the parameters $p_{i:j}$ and q_k may vary over time; moreover, the entanglement generated or distributed may not be perfect. One may wonder how to determine the maximum EDR and how to obtain optimal protocol in these scenarios.

Appendix I
Proof of Theorem 1

Consider the RED protocol π^* that achieves the optimal entanglement rate. Let $\mathsf{F}_{i:j}^{i:k}(\tau)$ and $\mathsf{F}_{i:j}^{k:j}(\tau)$ denote the number of EQPs $\boldsymbol{\Xi}_{i:k}$ and $\boldsymbol{\Xi}_{k:j}$ used for distributing $\boldsymbol{\Xi}_{i:j}$ after τ time slots, respectively; let $\mathsf{h}_{i:j}^{k}(\tau)$ denote the number of EQPs $\boldsymbol{\Xi}_{i:j}$ distributed by entanglement swapping that consumes $\boldsymbol{\Xi}_{i:k}$ and $\boldsymbol{\Xi}_{k:j}$ after τ time slots. If $(i,j) \in \mathcal{E}$, let $\mathsf{P}_{i:j}(\tau)$ denote the number of EQPs $\boldsymbol{\Xi}_{i:j}$ generated in Phase I after τ time slots. At the time slot T, since the number of EQPs $\boldsymbol{\Xi}_{i:j}$ is nonnegative, we have

$$\mathsf{P}_{i:j}(T)1_{\mathcal{E}}(i,j)+\sum_{k\in\mathcal{N}\setminus\{i,j\}}\mathsf{h}_{i:j}^{k}(T)\geq\sum_{k\in\mathcal{N}\setminus\{i,j\}}(\mathsf{F}_{i:k}^{i:j}(T)+\mathsf{F}_{k:j}^{i:j}(T)).$$

Taking the expectation on both sides and dividing them by T, we have

$$p_{i:j}1_{\mathcal{E}}(i,j)+\frac{1}{T}\sum_{k\in\mathcal{N}\setminus\{i,j\}}\mathbb{E}\{\mathsf{h}_{i:j}^{k}(T)\}\geq\frac{1}{T}\sum_{k\in\mathcal{N}\setminus\{i,j\}}\Big[\mathbb{E}\{\mathsf{F}_{i:k}^{i:j}(T)\}+\mathbb{E}\{\mathsf{F}_{k:j}^{i:j}(T)\}\Big].$$

Note that the success probability for distributing $\boldsymbol{\Xi}_{i:j}$ by using $\boldsymbol{\Xi}_{i:k}$ and $\boldsymbol{\Xi}_{k:j}$ is q_k, and $\mathsf{F}_{i:j}^{i:k}(T)=\mathsf{F}_{i:j}^{k:j}(T)$. Hence,

$$\mathbb{E}\{\mathsf{h}_{i:j}^{k}(T)\}=q_k\frac{\mathbb{E}\{\mathsf{F}_{i:j}^{i:k}(T)\}+\mathbb{E}\{\mathsf{F}_{i:j}^{k:j}(T)\}}{2}$$

and we have

$$p_{i:j}1_{\mathcal{E}}(i,j)+\sum_{k\in\mathcal{N}\setminus\{i,j\}}q_k\frac{\mathbb{E}\{\mathsf{F}_{i:j}^{i:k}(T)\}+\mathbb{E}\{\mathsf{F}_{i:j}^{k:j}(T)\}}{2T}\geq\frac{1}{T}\sum_{k\in\mathcal{N}\setminus\{i,j\}}\Big[\mathbb{E}\{\mathsf{F}_{i:k}^{i:j}(T)\}+\mathbb{E}\{\mathsf{F}_{k:j}^{i:j}(T)\}\Big].\quad(18)$$

Let

$$f_{i:j}^{i:k}=\frac{1}{T}\mathbb{E}\{\mathsf{F}_{i:j}^{i:k}(T)\}.$$

Evidently, $f_{i:j}^{i:k}$ satisfies the definition of the eflow. Moreover, $\{f_{i:j}^{i:k}:i,j,k\in\mathcal{N}\}$ defined above satisfies the constraint (2) using (18). One can also easily verify that $\{f_{i:j}^{i:k}:i,j,k\in\mathcal{N}\}$ satisfies the constraints (3)-(4). Therefore, $\{f_{i:j}^{i:k}:i,j,k\in\mathcal{N}\}$ is a feasible solution of $\mathscr{P}$.

Note that

$$\sum_{\tau=1}^{T}\mathsf{g}_{s:t}^{\pi^*}(\tau)=\mathsf{P}_{s:t}(T)1_{\mathcal{E}}(s,t)+\sum_{k\in\mathcal{N}\setminus\{s,t\}}\mathsf{h}_{s:t}^{k}(T)$$

and hence

$$\begin{aligned}&\frac{1}{T}\sum_{\tau=1}^{T}\mathbb{E}\{\mathsf{g}_{s:t}^{\pi^*}(\tau)\}\\&=\frac{1}{T}\mathbb{E}\{\mathsf{P}_{s:t}(T)\}1_{\mathcal{E}}(s,t)+\frac{1}{T}\sum_{k\in\mathcal{N}\setminus\{s,t\}}\mathbb{E}\{\mathsf{h}_{s:t}^{k}(T)\}\\&=p_{s:t}1_{\mathcal{E}}(s,t)+\frac{1}{T}\sum_{k\in\mathcal{N}\setminus\{s,t\}}q_k\frac{\mathbb{E}\{\mathsf{F}_{s:t}^{s:k}(T)\}+\mathbb{E}\{\mathsf{F}_{s:t}^{k:t}(T)\}}{2}\\&=p_{s:t}1_{\mathcal{E}}(s,t)+\sum_{k\in\mathcal{N}\setminus\{s,t\}}q_k\frac{f_{s:t}^{s:k}+f_{s:t}^{k:t}}{2}\end{aligned}$$

which is exactly the objective function of $\mathscr{P}$. Let λ^* denote the optimal value for $\mathscr{P}$. Since λ^* is the upper bound for the objective function that corresponds to a feasible solution, we have

$$\frac{1}{T}\sum_{\tau=1}^{T}\mathbb{E}\{\mathsf{g}_{s:t}^{\pi^*}(\tau)\}\leq\lambda^*$$

for all T and π^*. Taking the $\liminf$ over T on the left side, we arrive at the desired result.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

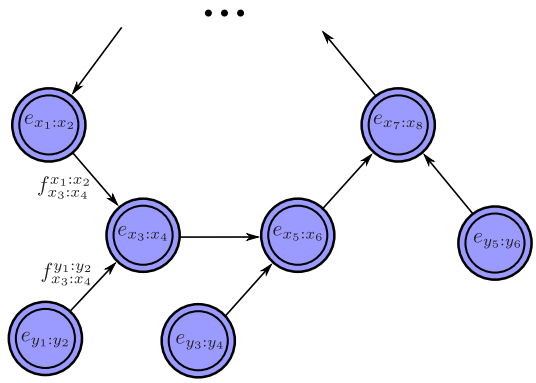


Fig. 12. One of the directed cycles in $\mathcal{G}$.

APPENDIX II
PROOF OF PROPOSITION 1

Consider the optimal solution $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ such that the graph $\mathcal{G}$ corresponding to $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ has the minimum number of edges. If the graph $\mathcal{G}$ has no directed cycles, the proof is finished. Otherwise, we will find another optimal solution of $\mathscr{P}$ and the corresponding graph of the new solution has fewer edges compared to $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$. This will lead to a contradiction and finish the proof.

Consider one of the directed cycles in $\mathcal{G}$ as in Fig. 12, consisting of nodes $e_{x_{2l-1}:x_{2l}}$, $l \in \mathcal{K}_{1:K}$, where K is the number of nodes in the cycle. For notational convenience, let $x_1 = x_{2K+1}$ and $x_2 = x_{2K+2}$. Note that the structure of entanglement swapping requires that $\text{Card}(\{x_{2l-1}, x_{2l}\} \cap \{x_{2l+1}, x_{2l+2}\}) = 1$ and $\text{Card}(\{y_{2l-1}, y_{2l}\} \cap \{x_{2l+1}, x_{2l+2}\}) = 1$, where y_{2l-1} and y_{2l} are shown in Fig. 12. From the definition of the edge, we have that $f^{x_{2l-1}:x_{2l}}_{x_{2l+1}:x_{2l+2}} > 0$, $l \in \mathcal{K}_{1:K}$.

Consider a number δ:

$$\delta = \min\left\{ f^{x_{2l-1}:x_{2l}}_{x_{2l+1}:x_{2l+2}}, l \in \mathcal{K}_{1:K} \right\}. \tag{19}$$

Evidently $\delta > 0$. We construct a solution of $\mathscr{P}$ as follows:

$$\begin{aligned}
\tilde{f}^{x_{2l-1}:x_{2l}}_{x_{2l+1}:x_{2l+2}} &= f^{x_{2l-1}:x_{2l}}_{x_{2l+1}:x_{2l+2}} - \delta, && l \in \mathcal{K}_{1:K} \\
\tilde{f}^{y_{2l-1}:y_{2l}}_{x_{2l+1}:x_{2l+2}} &= f^{y_{2l-1}:y_{2l}}_{x_{2l+1}:x_{2l+2}} - \delta, && l \in \mathcal{K}_{1:K} \\
\tilde{f}^{i:j}_{i:k} &= f^{i:j}_{i:k}, && \text{for other eflows.}
\end{aligned}$$

We next show $\{\tilde{f}^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ is an optimal solution of $\mathscr{P}$. Regarding the constraint (2), if $\{i,j\} = \{x_{2l-1}, x_{2l}\}$,

$$\begin{aligned}
&p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k \in \mathcal{N}\setminus\{i,j\}} q_k \frac{\tilde{f}^{i:k}_{i:j} + \tilde{f}^{k:j}_{i:j}}{2} \\
&= p_{i:j} 1_{\mathcal{E}}(i,j) - \delta\, q_{\{x_{2l-3},x_{2l-2}\}\cap\{x_{2l-1},x_{2l}\}} \\
&\quad + \sum_{k \in \mathcal{N}\setminus\{i,j\}} q_k \frac{f^{i:k}_{i:j} + f^{k:j}_{i:j}}{2} \\
&\geq -\delta\, q_{\{x_{2l-3},x_{2l-2}\}\cap\{x_{2l-1},x_{2l}\}} + \sum_{k \in \mathcal{N}\setminus\{i,j\}} (f^{i:j}_{i:k} + f^{i:j}_{k:j}) \\
&\geq -\delta + \sum_{k \in \mathcal{N}\setminus\{i,j\}} (f^{i:j}_{i:k} + f^{i:j}_{k:j}) \\
&= \sum_{k \in \mathcal{N}\setminus\{i,j\}} (\tilde{f}^{i:j}_{i:k} + \tilde{f}^{i:j}_{k:j})
\end{aligned}$$

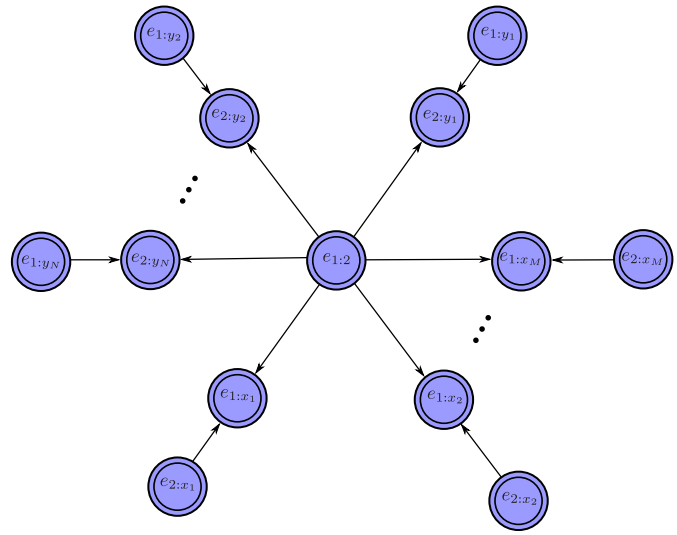


Fig. 13. Children of the non-isolated enode $e_{1:2}$.

where the first inequality is because $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ satisfies the constraint (2) and the second inequality is because $q_k \leq 1$ for all $k \in \mathcal{N}$. If $\{i,j\} = \{y_{2l-1}, y_{2l}\}$,

$$\begin{aligned}
&p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k \in \mathcal{N}\setminus\{i,j\}} q_k \frac{\tilde{f}^{i:k}_{i:j} + \tilde{f}^{k:j}_{i:j}}{2} \\
&= p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k \in \mathcal{N}\setminus\{i,j\}} q_k \frac{f^{i:k}_{i:j} + f^{k:j}_{i:j}}{2} \\
&\geq -\delta + \sum_{k \in \mathcal{N}\setminus\{i,j\}} (f^{i:j}_{i:k} + f^{i:j}_{k:j}) \\
&= \sum_{k \in \mathcal{N}\setminus\{i,j\}} (\tilde{f}^{i:j}_{i:k} + \tilde{f}^{i:j}_{k:j})
\end{aligned}$$

where the inequality is because $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ satisfies the constraint (2) and the fact $\delta > 0$. If $\{i,j\} \neq \{x_{2l-1}, x_{2l}\}$ and $\{i,j\} \neq \{y_{2l-1}, y_{2l}\}$, then the constraint (2) trivially holds. Regarding the constraint (3), since $f^{x_{2l-1}x_{2l}}_{x_{2l+1}x_{2l+2}} = f^{y_{2l-1}y_{2l}}_{x_{2l+1}x_{2l+2}} > 0$ and δ is selected according to (19), the constraint (3) holds.

The constraint (4) also trivially holds since $f^{s:t}_{i:j} = 0$ and the enode $e_{s:t}$ does not belong to the set $\{e_{x_{2l-1}:x_{2l}}, e_{y_{2l-1}:y_{2l}}, l \in \mathcal{K}_{1:K}\}$. Using the same argument, one can show that the value of the objective function remains unchanged if $f^{i:k}_{i:j}$ is replaced with $\tilde{f}^{i:k}_{i:j}$. This proves that $\{\tilde{f}^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ is an optimal solution of $\mathscr{P}$.

One can easily find that replacing $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ with $\{\tilde{f}^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ does not add additional edges in the corresponding graphs. Moreover, due to (19), at least one of the elements in $\{\tilde{f}^{x_{2l-1}:x_{2l}}_{x_{2l+1}:x_{2l+2}}, l \in \mathcal{K}_{1:K}\}$ is zero. Consequently, the graph corresponding to the optimal solution $\{\tilde{f}^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ has fewer edges than that corresponding to $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$. This gives the desired contradiction that $\{f^{i:k}_{i:j} : i,j,k \in \mathcal{N}\}$ has the minimum number of edges and finishes the proof.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

APPENDIX III
PROOF OF PROPOSITION 2

Consider the optimal solution $\{\mathring{f}_{i:j}^{i:k}\}_{i,j,k\in\mathcal{N}}$ that has the minimum number of edges. Proposition 1 shows that the associated graph is acyclic. We will prove that this optimal solution is efficient by contradiction.

Suppose there exists a non-isolated enode $e_{1:2}$ in $\mathcal{G}$ that is not an ancestor of $e_{s:t}$. Consider the children of $e_{1:2}$, denoted as $e_{1:x_1}, e_{1:x_2}, \ldots, e_{1:x_M}$, $e_{2:y_1}, e_{2:y_2}, \ldots, e_{2:y_N}$ shown in Fig. 13. We construct a solution $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ as follows:

$$\tilde{f}_{i:j}^{i:k} = \begin{cases} 0 & \text{if } e_{i:k} \text{ is a descendant of } e_{1:2} \\ 0 & \text{if } e_{i:j} \text{ is a descendant of } e_{1:2} \\ 0 & \text{if } e_{i:j} = e_{1:2} \\ f_{i:j}^{i:k} & \text{otherwise.} \end{cases}$$

Evidently, the graph $\widetilde{\mathcal{G}}$ corresponding to $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ can be obtained from $\mathcal{G}$ by removing some edges so that the enode $e_{1:2}$ does not have descendants in $\widetilde{\mathcal{G}}$. We next show that $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ is an optimal solution of $\mathscr{P}$. One can find that the constraints (2)-(4) trivially hold. Regarding the objective function, consider $f_{s:t}^{s:k}$ for some $k \in \mathcal{N}$. If $f_{s:t}^{s:k} > 0$, then $e_{s:t}$ is a descendant of $e_{s:k}$. Since $e_{s:t}$ is not a descendant of $e_{1:2}$, $e_{s:k}$ is not a descendant of $e_{1:2}$. Consequently, $\tilde{f}_{s:t}^{s:k} = f_{s:t}^{s:k}$. If $f_{s:t}^{s:k} = 0$, then $\tilde{f}_{s:t}^{s:k} = f_{s:t}^{s:k}$ trivially. This shows that $f_{s:t}^{s:k} = f_{s:t}^{s:k}$ for all $k \in \mathcal{N}$. Similarly, $\tilde{f}_{s:t}^{k:t} = f_{s:t}^{k:t}$ for all $k \in \mathcal{N}$. As a result,

$$\sum_{k\in\mathcal{N}\setminus\{s,t\}} q_k \frac{\tilde{f}_{s:t}^{s:k} + \tilde{f}_{s:t}^{k:t}}{2} = \sum_{k\in\mathcal{N}\setminus\{s,t\}} q_k \frac{f_{s:t}^{s:k} + f_{s:t}^{k:t}}{2}$$

showing that $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ is the optimal solution of $\mathscr{P}$. However, the graph $\widetilde{\mathcal{G}}$ corresponding to $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ has fewer edges than $\mathcal{G}$, leading to the desired contradiction.

APPENDIX IV
PROOF OF THEOREM 2

The proof of Proposition 1 and Proposition 2 shows that we can construct an optimal solution of $\mathscr{P}$, denoted as $\{f_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$, such that the graph $\mathcal{G}$ corresponding to $\{f_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ is acyclic and efficient. We will show that given $\{f_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$, we can provide an optimal solution of $\mathscr{P}_{\mathrm{s}}$, denoted as $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\tilde{u}_{i:j} : (i,j) \in \mathcal{E}\}$.

We will start from the solution $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\tilde{u}_{i:j} : (i,j) \in \mathcal{E}\}$, where $\tilde{f}_{i:j}^{i:k} = f_{i:j}^{i:k}$, $\forall i,j,k$ and $\tilde{u}_{i:j} = 1$, $\forall i,j$. Evidently, the solution $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ satisfies the constraints (2)-(4), but $\{\tilde{f}_{i:j}^{i:k} : i,j,k \in \mathcal{N}\}$ and $\{\tilde{u}_{i:j} : (i,j) \in \mathcal{E}\}$ may not satisfy the constraints in $\mathscr{P}_{\mathrm{s}}$. We next update each of the enodes. Here, for an enode $e_{i:j}$, updating $e_{i:j}$ means updating the incoming eflow of $e_{i:j}$ $\tilde{f}_{i:j}^{i:k}$, $k \in \mathcal{N} \setminus \{i,j\}$ and determining $\tilde{u}_{i:j}$. After updating an enode, we will make sure that three requirements are satisfied: 1) conditions (5)-(8) hold for all the updated enodes; 2) conditions (2)-(4) hold for all the nodes; and 3) the value of the objective function remains unchanged. In this way, after updating all the enodes, we will obtain a solution of $\mathscr{P}_{\mathrm{s}}$ with the same optimal value of $\mathscr{P}$.

We first update isolated enodes. If $e_{i:j}$ is an isolated enode in $\mathcal{G}$, then we set $\tilde{f}_{i:k}^{i:j} = \tilde{f}_{k:j}^{i:j} = \tilde{f}_{i:j}^{i:k} = \tilde{f}_{i:j}^{k:j} = 0$ and $\tilde{u}_{i:j} = 0$. Note that such an update satisfies the three requirements in the previous paragraph.

We then update the ancestors of $e_{s:t}$. Since $\mathcal{G}$ is acyclic, we can determine a topological ordering of $\mathcal{G}$ starting from $e_{s:t}$ and update the nodes with the order. For an enode $e_{i:j}$, since the condition (2) holds as required, we have

$$p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k \frac{\tilde{f}_{i:j}^{i:k} + \tilde{f}_{i:j}^{k:j}}{2} \geq \sum_{k\in\mathcal{N}\setminus\{i,j\}} (\tilde{f}_{i:k}^{i:j} + \tilde{f}_{k:j}^{i:j}), \quad i,j \in \mathcal{N}.$$

We then determine $\tilde{u}_{i:j}$ and update the incoming flow $\tilde{f}_{i:j}^{i:k}$ and $\tilde{f}_{i:j}^{k:j}$ as follows:

$$\varrho_{i:j} \to \frac{\sum_{k\in\mathcal{N}\setminus\{i,j\}} (\tilde{f}_{i:k}^{i:j} + \tilde{f}_{k:j}^{i:j})}{p_{i:j} 1_{\mathcal{E}}(i,j) + \sum_{k\in\mathcal{N}\setminus\{i,j\}} q_k (\tilde{f}_{i:j}^{i:k} + \tilde{f}_{i:j}^{k:j})/2}$$
$$\tilde{u}_{i:j} \to \varrho_{i:j}, \qquad \tilde{f}_{i:j}^{i:k} \to \varrho_{i:j} \tilde{f}_{i:j}^{i:k}, \qquad \tilde{f}_{i:j}^{k:j} \to \varrho_{i:j} \tilde{f}_{i:j}^{k:j}.$$

One can easily verify that such an update satisfies the three requirements. This finishes the proof.

APPENDIX V
PROOF OF PROPOSITION 3

We show that

$$h(N) \geq g(N) \tag{20}$$

for all $N \in \mathbb{N}_+$ by induction. The base case with $N = 1$ can be easily verified since $h(1) \geq 1$. For the induction step, suppose (20) holds for $N = 1, 2, \ldots, N_1$. We next show that (20) holds for $N = N_1 + 1$.

Evidently, the EQP $\boldsymbol{\Xi}_{0:N_1+1}$ is distributed based on entanglement swapping between EQPs $\boldsymbol{\Xi}_{0:a}$ and $\boldsymbol{\Xi}_{a:N_1+1}$ for some $a \in \mathcal{K}_{1:N_1}$. Let x_a denote the fraction of the EQPs $\boldsymbol{\Xi}_{0:N_1+1}$ that is distributed based on entanglement swapping between $\boldsymbol{\Xi}_{0:a}$ and $\boldsymbol{\Xi}_{a:N_1+1}$. For a fixed a, we consider the expected numbers of crude entanglements required to distribute one EQP $\boldsymbol{\Xi}_{0:a}$ and one EQP $\boldsymbol{\Xi}_{a:N_1+1}$. These two numbers can be lower-bounded by $h(a)$ and $h(N_1 + 1 - a)$. Then

$$\begin{aligned} h(N_1+1) &\geq \frac{1}{q} \sum_{a\in\mathcal{K}_{1:N_1}} x_a \big[h(a) + h(N_1+1-a)\big] \\ &\geq \frac{1}{q} \sum_{a\in\mathcal{K}_{1:N_1}} x_a \big[g(a) + g(N_1+1-a)\big] \\ &\geq \frac{1}{q} \sum_{a\in\mathcal{K}_{1:N_1}} x_a \; q \; g(N_1+1) \\ &= \sum_{a\in\mathcal{K}_{1:N_1}} x_a \; g(N_1+1) \\ &= g(N_1+1) \end{aligned}$$

where the first inequality has been explained, the second inequality is because of the induction hypothesis, the third inequality is because of Lemma 1 below, and the second

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

equality is because $\sum_{a\in\mathcal{K}_{1:N_1}} x_a = 1$. This completes the proof for (20) for all $N \in \mathbb{N}_+$.

Lemma 1: For K, $M \in \mathbb{N}_+$,

$$\frac{g(K)+g(M)}{q} \geq g(K+M). \tag{21}$$

Proof: See Appendix VI. □

Appendix VI
Proof of Lemma 1

Without loss of generality, we assume $K \leq M$. We prove (21) in three cases: $K = M$; $K = M-1$; and $K \leq M-2$.

Case 1: $K = M$.

Let $k = \lceil \log_2 K \rceil - 1$. Then

$$\begin{aligned}\frac{g(K)+g(M)}{q} &= \frac{2}{q}\, g(K)\\ &= \frac{2}{q}\,\frac{2(K-2^k)+(2^{k+1}-K)\,q}{q^{k+1}}\\ &= \frac{2(2K-2^{k+1})+(2^{k+2}-2K)\,q}{q^{k+2}}\\ &= g(2K)\\ &= g(K+M)\end{aligned}$$

where the fourth equality is because $k = \lceil \log_2 2K \rceil - 2$. Therefore, the inequality (21) holds.

Case 2: $K = M-1$.

Let $k = \lceil \log_2 K \rceil - 1$. We discuss two subcases: $K = 2^{k+1}$ and $K < 2^{k+1}$. If $K = 2^{k+1}$, then

$$\begin{aligned}\frac{g(K)+g(M)}{q} &= \frac{2(K-2^k)+(2^{k+1}-K)\,q}{q^{k+2}}\\ &\quad+\frac{2(K+1-2^{k+1})+(2^{k+2}-K-1)\,q}{q^{k+3}}\\ &= \frac{2^{k+1}}{q^{k+2}}+\frac{2+(2^{k+1}-1)\,q}{q^{k+3}}\\ &= \frac{2+(2^{k+2}-1)\,q}{q^{k+3}}\\ &= \frac{2(2K+1-2^{k+2})+(2^{k+3}-2K-1)\,q}{q^{k+3}}\\ &= g(2K+1)\\ &= g(K+M)\end{aligned}$$

where the first equality is because $k+1 = \lceil \log_2 M \rceil - 1$ and the fifth equality is because $k+2 = \lceil \log_2 (K+M) \rceil - 1$. If $K < 2^{k+1}$, then

$$\begin{aligned}\frac{g(K)+g(M)}{q} &= \frac{2(K-2^k)+(2^{k+1}-K)\,q}{q^{k+2}}\\ &\quad+\frac{2(K+1-2^{k})+(2^{k+1}-K-1)\,q}{q^{k+2}}\\ &= \frac{2(2K+1-2^{k+1})+(2^{k+2}-2K-1)\,q}{q^{k+2}}\\ &= g(2K+1)\\ &= g(K+M)\end{aligned}$$

where the third equality is because $k+1 = \lceil \log_2 (K+M) \rceil - 1$. Therefore, the inequality (21) holds.

Case 3: $K \leq M-2$.

Note that

$$\begin{aligned}g(K+1)-g(K) &= \frac{2-q}{q^{\lceil \log_2 (K+1) \rceil}}\\ &\leq \frac{2-q}{q^{\lceil \log_2 M \rceil}} = g(M)-g(M-1)\end{aligned} \tag{22}$$

where the equalities can be verified by some calculation, and the inequality is because $K+1 \leq M$ and $2-q > 0$. The inequality (22) implies

$$g(K)+g(M) \geq g(K+1)+g(M-1).$$

Similarly, we have

$$g(K+1)+g(M-1) \geq g(K+2)+g(M-2)$$

provided that $K+1 \leq (M-1)-2$. Such a process can be repeated and we will have

$$g(K)+g(M) \geq \begin{cases} 2\, g\Big(\dfrac{K+M}{2}\Big) & \text{if } K+M \in \mathbb{Z}_{\rm e}\\ g\Big(\dfrac{K+M-1}{2}\Big)+g\Big(\dfrac{K+M+1}{2}\Big) & \text{if } K+M \in \mathbb{Z}_{\rm o}.\end{cases}$$

The results from Case 1 and Case 2 show that

$$q\, g(K+M) = \begin{cases} 2\, g\Big(\dfrac{K+M}{2}\Big) & \text{if } K+M \in \mathbb{Z}_{\rm e}\\ g\Big(\dfrac{K+M-1}{2}\Big)+g\Big(\dfrac{K+M+1}{2}\Big) & \text{if } K+M \in \mathbb{Z}_{\rm o}.\end{cases}$$

Combining the results above, we have that the inequality (21) holds in Case 3.

Appendix VII
Proof of Proposition 4

We next show that

$$h_{\rm o}(N) \geq g_{\rm o}(N) \tag{23}$$

$$h_{\rm e}(N) \geq g_{\rm e}(N) \tag{24}$$

for all $N \in \mathbb{N}_+$ by induction. The base case with $N = 1$ can be easily verified since $h_{\rm o}(1) \geq 1$ and $h_{\rm e}(1) \geq 0$. For the induction step, suppose (23) and (24) hold for $N = 1, 2, \ldots, N_1$. We next show that (23) and (24) hold for $N = N_1 + 1$.

Evidently, the EQP $\boldsymbol{\Xi}_{0:N_1+1}$ is distributed based on entanglement swapping between EQPs $\boldsymbol{\Xi}_{0:a}$ and $\boldsymbol{\Xi}_{a:N_1+1}$ for some $a \in \mathcal{K}_{1:N_1}$. Let x_a denote the fraction of EQPs $\boldsymbol{\Xi}_{0:N_1+1}$ that is distributed based on entanglement swapping between $\boldsymbol{\Xi}_{0:a}$ and $\boldsymbol{\Xi}_{a:N_1+1}$. For a fixed a, we consider the expected numbers of odd crude entanglements required to distribute one entangled pair $\boldsymbol{\Xi}_{0:a}$ and one EQP $\boldsymbol{\Xi}_{a:N_1+1}$. If $a \in \mathbb{Z}_{\rm o}$, these two numbers can be lower-bounded by $h_{\rm o}(a)$ and $h_{\rm e}(N_1+1-a)$, respectively; if $a \in \mathbb{Z}_{\rm e}$, these two numbers can be lower-bounded by $h_{\rm o}(a)$ and $h_{\rm o}(N_1+1-a)$, respectively. Then

$$\begin{aligned}h_{\rm o}(N_1+1) &\geq \frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\big[h_{\rm o}(a)+h_{\rm e}(N_1+1-a)\big]\\ &\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\big[h_{\rm o}(a)+h_{\rm o}(N_1+1-a)\big]\end{aligned}$$

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

$$\begin{aligned}
&\geq \frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\big[g_{\rm o}(a)+g_{\rm e}(N_1+1-a)\big]\\
&\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\big[g_{\rm o}(a)+g_{\rm o}(N_1+1-a)\big]\\
&\geq \frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\ q\ g_{\rm o}(N_1+1)\\
&\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\ q\ g_{\rm o}(N_1+1)\\
&=\sum_{a\in\mathcal{K}_{1:N_1}} x_a g_{\rm o}(N_1+1)\\
&=g_{\rm o}(N_1+1) \qquad (25)
\end{aligned}$$

where the first inequality has been explained, the second inequality is because of the induction hypothesis, the third inequality is because of (27) and (29) in Lemma 2 below, and the last equality is because $\sum_{a\in\mathcal{K}_{1:N_1}} x_a=1$. Similarly,

$$\begin{aligned}
h_{\rm e}(N_1+1)&=\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\big[h_{\rm e}(a)+h_{\rm o}(N_1+1-a)\big]\\
&\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\big[h_{\rm e}(a)+h_{\rm e}(N_1+1-a)\big]\\
&\geq \frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\big[g_{\rm e}(a)+g_{\rm o}(N_1+1-a)\big]\\
&\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\big[g_{\rm e}(a)+g_{\rm e}(N_1+1-a)\big]\\
&\geq \frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm o}} x_a\ q\ g_{\rm e}(N_1+1)\\
&\quad+\frac{1}{q}\sum_{a\in\mathcal{K}_{1:N_1}\cap\mathbb{Z}_{\rm e}} x_a\ q\ g_{\rm e}(N_1+1)\\
&=\sum_{a\in\mathcal{K}_{1:N_1}} x_a g_{\rm e}(N_1+1)\\
&=g_{\rm e}(N_1+1). \qquad (26)
\end{aligned}$$

Equations (25) and (26) complete the proof for (23) and (24) for all $N\in\mathbb{N}_+$.

Lemma 2: For $K,M\in\mathbb{N}_+$. If $K\in\mathbb{Z}_{\rm e}$, then

$$\frac{g_{\rm o}(K)+g_{\rm o}(M)}{q}\geq g_{\rm o}(K+M) \qquad (27)$$

$$\frac{g_{\rm e}(K)+g_{\rm e}(M)}{q}\geq g_{\rm e}(K+M). \qquad (28)$$

If $K\in\mathbb{Z}_{\rm o}$, then

$$\frac{g_{\rm o}(K)+g_{\rm e}(M)}{q}\geq g_{\rm o}(K+M) \qquad (29)$$

$$\frac{g_{\rm e}(K)+g_{\rm o}(M)}{q}\geq g_{\rm e}(K+M). \qquad (30)$$

Sketch of the Proof: See Appendix VIII. □

Appendix VIII
Sketch of the Proof of Lemma 2

We only prove the first inequality (27) and the proof for the remaining inequalities is similar.

Recall that $K\in\mathbb{Z}_{\rm e}$. We prove (27) in three cases: $M\in\mathbb{Z}_{\rm e}$; $M\in\mathbb{Z}_{\rm o}$ and $K\geq M-1$; and $M\in\mathbb{Z}_{\rm o}$ and $K<M-1$.

Case 1: $M\in\mathbb{Z}_{\rm e}$.

Since $K\in\mathbb{Z}_{\rm e}$ and $M\in\mathbb{Z}_{\rm e}$, $K+M\in\mathbb{Z}_{\rm e}$. Then

$$\frac{g_{\rm o}(K)+g_{\rm o}(M)}{q}=\frac{g(K)+g(M)}{2q} \qquad (31)$$

$$\geq\frac{g(K+M)}{2}=g_{\rm o}(K+M) \qquad (32)$$

where the equalities are due to the definition of $g(\cdot)$ in (16), and the inequality is due to Lemma 1.

Case 2: $M\in\mathbb{Z}_{\rm o}$ and $K\geq M-1$.

We have that

$$\begin{aligned}
\frac{g_{\rm o}(K)+g_{\rm o}(M)}{q}&=\frac{g_{\rm o}(K)+g_{\rm o}(M+1)}{q}+\frac{q-1}{q^{m+2}}\\
&\geq g_{\rm o}(K+M+1)+\frac{q-1}{q^{m+2}}\\
&=g_{\rm o}(K+M)+\frac{1-q}{q^{\lceil\log_2(K+M)\rceil}}+\frac{q-1}{q^{m+2}}\\
&\geq g_{\rm o}(K+M)
\end{aligned}$$

where $m=\lceil\log_2 M\rceil-1$. The equalities are due to the expression of $g_{\rm o}(\cdot)$ and the fact that $M+1\in\mathbb{Z}_{\rm e}$ and $M+K\in\mathbb{Z}_{\rm o}$; the first inequality is due to the proof in Case 1; and the last inequality is because

$$\lceil\log_2(K+M)\rceil\geq\lceil\log_2(2M-1)\rceil=\lceil\log_2(2M)\rceil=m+2.$$

Case 3: $M\in\mathbb{Z}_{\rm o}$ and $K<M-1$.

Since $K\in\mathbb{Z}_{\rm e}$ and $M\in\mathbb{Z}_{\rm o}$, we have $K\leq M-3$.

$$\begin{aligned}
g_{\rm o}(K+2)-g_{\rm o}(K)&=\frac{2-q}{2q^{\lceil\log_2(K+2)\rceil}}+\frac{2-q}{2q^{\lceil\log_2(K+1)\rceil}}\\
&\leq\frac{2-q}{q^{\lceil\log_2(K+2)\rceil}}\\
&\leq\frac{2-q}{q^{\lceil\log_2(M-1)\rceil}}\\
&=\frac{2-q}{q^{\lceil\log_2(M-2)\rceil}}\\
&\leq\frac{1}{q^{\lceil\log_2 M\rceil}}+\frac{1-q}{q^{\lceil\log_2(M-2)\rceil}}\\
&=g_{\rm o}(M)-g_{\rm o}(M-2) \qquad (33)
\end{aligned}$$

where the equalities can be verified by some calculation, and the second inequality is because $K\leq M-3$ and $2-q>0$. The inequality (33) implies

$$g_{\rm o}(M)+g_{\rm o}(K)\geq g_{\rm o}(M-2)+g_{\rm o}(K+2).$$

Similarly, we have

$$g_{\rm o}(M-2)+g_{\rm o}(K+2)\geq g_{\rm o}(M-4)+g_{\rm o}(K+4)$$

provided that $K+2\leq(M-2)-3$. Such a process can be repeated and we will have

$$g_{\rm o}(M)+g_{\rm o}(K)\geq g_{\rm o}\Big(\frac{K+M-1}{2}\Big)+g_{\rm o}\Big(\frac{K+M+1}{2}\Big).$$

Since $M\in\mathbb{Z}_{\rm o}$ and $K\in\mathbb{Z}_{\rm e}$, one of $(K+M\pm1)/2$ is odd and the other is even; their difference is no more than 1. The result from Case 2 shows that

$$g_{\rm o}\Big(\frac{K+M-1}{2}\Big)+g_{\rm o}\Big(\frac{K+M+1}{2}\Big)\geq q\ g_{\rm o}(K+M)\,.$$

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

Combining the results above, we have that the inequality (27) holds in Case 3.

ACKNOWLEDGMENT

The authors wish to thank A. Conti and S. Guerrini for the helpful suggestions and careful reading of the manuscript.

REFERENCES

[1] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," *Phil. Trans. Roy. Soc. Lond. A*, vol. 361, no. 1809, pp. 1655–1674, Jun. 2003.

[2] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.

[3] *National Strategic Overview for Quantum Information Science*, Nat. Sci. Technol. Council, Washington, DC, USA, Sep. 2018.

[4] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, "Multipartite entanglement can speed up quantum key distribution in networks," *New J. Phys.*, vol. 19, no. 9, Sep. 2017, Art. no. 093012.

[5] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Channel-adapted quantum error correction for the amplitude damping channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5705–5718, Dec. 2008.

[6] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, no. 4, Apr. 2003, Art. no. 042317.

[7] S. Guerrini, M. Chiani, and A. Conti, "Secure key throughput of intermittent trusted-relay QKD protocols," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–5.

[8] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added coherent states," in *Proc. IEEE Workshop Quantum Commun. Inf. Technol. (QCIT)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–5.

[9] D. Bruß and C. Macchiavello, "Multipartite entanglement in quantum algorithms," *Phys. Rev. A*, vol. 83, no. 5, May 2011, Art. no. 052313.

[10] D. Alanis *et al.*, "Quantum-aided multi-objective routing optimization using back-tracing-aided dynamic programming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7856–7860, Aug. 2018.

[11] V. Havlíček *et al.*, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, Mar. 2019.

[12] G. M. D'Ariano, P. L. Presti, and M. G. A. Paris, "Using entanglement improves the precision of quantum measurements," *Phys. Rev. Lett.*, vol. 87, no. 27, p. 270404, Dec. 2001.

[13] P. Kömar *et al.*, "A quantum network of clocks," *Nature Phys*, vol. 10, no. 8, pp. 582–587, Aug. 2014.

[14] Z. Huang, C. Macchiavello, and L. Maccone, "Usefulness of entanglement-assisted quantum metrology," *Phys. Rev. A*, vol. 94, no. 1, Jul. 2016, Art. no. 012101.

[15] S. Khatri, C. T. Matyas, A. U. Siddiqui, and J. P. Dowling, "Practical figures of merit and thresholds for entanglement distribution in quantum networks," *Phys. Rev. Res.*, vol. 1, no. 2, Sep. 2019, Art. no. 023032.

[16] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Phys. Rev. A*, vol. 59, no. 1, pp. 169–181, Jul. 2002.

[17] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. V. Meter, and M. D. Lukin, "Quantum repeater with encoding," *Phys. Rev. A*, vol. 79, no. 3, Mar. 2009, Art. no. 032325.

[18] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Jul. 2002.

[19] L. Vaidman, "Teleportation of quantum states," *Phys. Rev. A*, vol. 49, no. 2, p. 1473, Feb. 1994.

[20] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, pp. 575–579, Dec. 1997.

[21] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," *Phys. Rev. Lett.*, vol. 87, Jul. 2001, Art. no. 077902.

[22] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, "Remote preparation of quantum states," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 56–74, Jan. 2005.

[23] W. Dai, T. Peng, and M. Z. Win, "Remote state preparation for multiple parties," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brighton, U.K., May 2019, pp. 7983–7987.

[24] S. Pirandola, "Capacities of repeater-assisted quantum communications," Jan. 2016, *arXiv:1601.00966*. [Online]. Available: https://arxiv.org/abs/1601.00966

[25] S. Pirandola, "End-to-end capacities of a quantum communication network," *Nature Commun. Phys.*, vol. 2, p. 51, May 2019.

[26] S. Bäuml, K. Azuma, G. Kato, and D. Elkouss, "Linear programs for entanglement and key distribution in the quantum Internet," Sep. 2018, *arXiv:1809.03120*. [Online]. Available: https://arxiv.org/abs/1809.03120

[27] L. Gyongyosi and S. Imre, "Decentralized base-graph routing for the quantum Internet," *Phys. Rev. A*, vol. 98, no. 2, Aug. 2018, Art. no. 022310.

[28] E. Schoute, L. Mančinska, T. Islam, I. Kerenidis, and S. Wehner, "Shortcuts to quantum network routing," Oct. 2016, *arXiv:1610.05238*. [Online]. Available: https://arxiv.org/abs/1610.05238

[29] M. Caleffi, "Optimal routing for quantum networks," *IEEE Access*, vol. 5, pp. 22299–22312, 2017.

[30] M. Pant *et al.*, "Routing entanglement in the quantum Internet," *NPJ, Quantum Inf.*, vol. 5, no. 1, pp. 1–9, Mar. 2019.

[31] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Jul. 2002.

[32] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.

[33] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, "Multiplexed memory-insensitive quantum repeaters," *Phys. Rev. Lett.*, vol. 98, Feb. 2007, Art. no. 060502.

[34] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. De Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," *Phys. Rev. A*, vol. 76, no. 5, 2007, Art. no. 050301.

[35] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, "Fault-tolerant quantum repeater with atomic ensembles and linear optics," *Phys. Rev. A*, vol. 76, no. 2, Aug. 2007, Art. no. 022329.

[36] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, pp. 33–80, Mar. 2011.

[37] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, "Design and analysis of communication protocols for quantum repeater networks," *New J. Phys.*, vol. 18, no. 8, Aug. 2016, Art. no. 083015.

[38] N. Sinclair *et al.*, "Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control," *Phys. Rev. Lett.*, vol. 113, no. 5, 2014, Art. no. 053603.

[39] S. Guha *et al.*, "Rate-loss analysis of an efficient quantum repeater architecture," *Phys. Rev. A*, vol. 92, no. 2, 2015, Art. no. 022357.

[40] X. Liu, Z.-Q. Zhou, Y.-L. Hua, C.-F. Li, and G.-C. Guo, "Semihierarchical quantum repeaters based on moderate lifetime quantum memories," *Phys. Rev. A*, vol. 95, no. 1, 2017, Art. no. 012319.

[41] E. Shchukin, F. Schmidt, and P. van Loock, "On the waiting time in quantum repeaters with probabilistic entanglement swapping," *Phys. Rev. A*, vol. 100, no. 3, 2019, Art. no. 032322.

[42] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, "Optimal approach to quantum communication using dynamic programming," *Proc. Nat. Acad. Sci. USA*, vol. 104, no. 44, pp. 17291–17296, Oct. 2007.

[43] N. K. Bernardes, L. Praxmeyer, and P. van Loock, "Rate analysis for a hybrid quantum repeater," *Phys. Rev. A*, vol. 83, no. 1, 2011, Art. no. 012323.

[44] L. Ruan, W. Dai, and M. Z. Win, "Adaptive recurrence quantum entanglement distillation for two-Kraus-operator channels," *Phys. Rev. A*, vol. 97, no. 5, May 2018, Art. no. 052332.

[45] M. Żukowski,, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event-ready-detectors' Bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, no. 26, pp. 4287–4290, Jul. 2002.

[46] B. T. Kirby, S. Santra, V. S. Malinovsky, and M. Brodsky, "Entanglement swapping of two arbitrarily degraded entangled states," *Phys. Rev. A*, vol. 94, no. 1, Jul. 2016, Art. no. 012336.

[47] D. Bertsimas and J. N. Tsitsiklis, *Introduction to Linear Optimization*, 1st ed. Belmont, MA, USA: Athena Scientific, 1997.

[48] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[49] D. G. Luenberger and Y. Ye, *Linear Nonlinear Programming*, 3rd ed. New York, NY, USA: Springer, 2008.

[50] R. J. Vanderbei, *Linear Programming: Foundations and Extensions*, 2nd ed. Norwell, MA, USA: Kluwer, 2001.

[51] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Structured near-optimal channel-adapted quantum error correction," *Phys. Rev. A*, vol. 77, no. 1, Jan. 2008, Art. no. 012320.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.

[52] S. Croke, S. M. Barnett, and G. Weir, "Optimal sequential measurements for bipartite state discrimination," *Phys. Rev. A*, vol. 95, no. 5, May 2017, Art. no. 052308.
[53] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Optimum quantum error recovery using semidefinite programming," *Phys. Rev. A*, vol. 75, no. 1, Jan. 2007, Art. no. 012338.
[54] W. Dai, T. Peng, and M. Z. Win, "Quantum queuing delay," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 605–618, Mar. 2020.
[55] D. S. Gunderson, *Handbook of Mathematical Induction: Theory and Applications*, 1st ed. Boca Raton, FL, USA: Chapman, 2010.
[56] G. B. Folland, *Real Analysis: Modern Techniques and Their Applications*, 1st ed. New York, NY, USA: Wiley, 1984.
[57] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Commun.*, vol. 8, Apr. 2017, Art. no. 15043.

Wenhan Dai (Student Member, IEEE) received the B.E. degree in electronic engineering and the B.S. degree in mathematics from Tsinghua University, Beijing, China, in 2011, and the S.M. and Ph.D. degrees in aeronautics and astronautics from the Massachusetts Institute of Technology (MIT) in 2014 and 2019, respectively.

His research interests include statistical inference, network science, communication theory, and their applications to wireless communication, network localization and navigation, quantum information science, efficient network localization, quantum network operation, and quantum sensing.

Dr. Dai was honored by the Marconi Society with the Paul Baran Young Scholar Award in 2017. He received the Student Paper Award (first place) from the IEEE CWIT in 2015, the Chinese Government Award for Outstanding Student Abroad in 2016, the first prize of the IEEE Communications Society Student Competition in 2016, and the Marconi-BISITE Best Paper Award from the IEEE ICUWB in 2017. He was recognized as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS in 2014.

Tianyi Peng (Student Member, IEEE) received the B.S. degree in computer science from Tsinghua University, China, in 2017. He is currently pursuing the master's degree with the Massachusetts Institute of Technology (MIT).

Since August 2017, he has been with the Wireless Information and Network Sciences Laboratory, MIT. He was with the Center for Quantum Information, Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, from 2015 to 2017, and the Center for Theoretical Physics (CTP), MIT, in summer 2016.

Mr. Peng received the Outstanding Thesis Award in 2017 from Tsinghua University.

Moe Z. Win (Fellow, IEEE) is a Professor at the Massachusetts Institute of Technology (MIT) and the founding director of the Wireless Information and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories and NASA Jet Propulsion Laboratory.

His research encompasses fundamental theories, algorithm design, and network experimentation for a broad range of real-world problems. His current research topics include network localization and navigation, network interference exploitation, and quantum information science. He has served the IEEE Communications Society as an elected Member-at-Large on the Board of Governors, as elected Chair of the Radio Communications Committee, and as an IEEE Distinguished Lecturer. Over the last two decades, he held various editorial positions for IEEE journals and organized numerous international conferences. Currently, he is serving on the SIAM Diversity Advisory Committee.

Dr. Win is an elected Fellow of the AAAS, the EURASIP, the IEEE, and the IET. He was honored with two IEEE Technical Field Awards: the IEEE Kiyo Tomiyasu Award (2011) and the IEEE Eric E. Sumner Award (2006, jointly with R. A. Scholtz). His publications, co-authored with students and colleagues, have received several awards. Other recognitions include the IEEE Communications Society Edwin H. Armstrong Achievement Award (2016), the International Prize for Communications Cristoforo Colombo (2013), the Copernicus Fellowship (2011) and the *Laurea Honoris Causa* (2008) from the Università degli Studi di Ferrara, and the U.S. Presidential Early Career Award for Scientists and Engineers (2004). He is an ISI Highly Cited Researcher.

Authorized licensed use limited to: MIT Libraries. Downloaded on June 09,2020 at 20:56:39 UTC from IEEE Xplore. Restrictions apply.