On the Exact Analysis of an Idealized Quantum Switch

Gayane Vardoyan
UMass Amherst

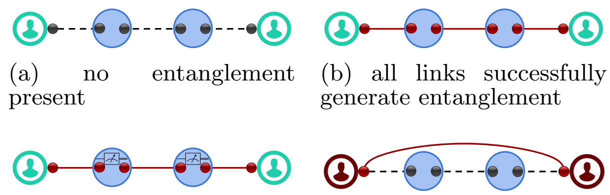
Saikat Guha
University of Arizona

Philippe Nain
Inria, France

Don Towsley
UMass Amherst

Protocols that exploit quantum communication technology offer two advantages: they can either extend or render feasible the capabilities of their classical counterparts, or they exhibit functionality entirely unachievable through classical means alone. For an example of the former, quantum key distribution protocols such as E91 [2] and BBM92 [1] can in principle yield information-theoretic security by using entanglement to generate secure key bits. These raw secret key bits can then be distilled into a one-time pad to encode messages sent between two parties. For an example of the latter, distributed quantum sensing frameworks such as [3] and [11] employ entanglement to overcome the standard quantum limit [4].

While these applications hold a tremendous amount of potential for distributed quantum communication (and even computation, see, *e.g.*, [6]), a substantial challenge is reliable generation of entanglement – an essential component for many of these tasks – especially over a large distance. This is due to the fact that there is an exponential rate-versus-distance decay for quantum state propagation both through terrestrial free-space and optical fiber channels [8, 9]. Quantum repeaters positioned between communicating nodes can overcome this fundamental rate-versus-distance tradeoff [5, 7]. The process of quantum repeater-assisted entanglement generation is illustrated at a high level in Fig. 1. Henceforth, we use the term “quantum switch” instead of “repeater” because in a more complex network than that of Fig. 1, the device will likely be connected to several nodes or users; hence it is reasonable to assume that it will be equipped with entanglement switching logic. Quantum repeaters, switches, and similar devices will serve as building blocks for large-scale quantum networks. It is natural, therefore, to ask questions about their fundamental limits from a mathematical perspective, in order to gain insight into what constitutes efficient operation for such a device, as well as to create a performance comparison basis for future protocols that will rely on these devices. To this end, we study a quantum switch that serves entangled states to pairs of users in a star topology, with the objective of determining the capacity of the switch, as well as the expected number of stored qubits in memory at the switch when it operates at capacity. We use a discrete-time Markov chain (DTMC) to construct a model that abstracts away various architecture and physical implementation details about the system, *e.g.*, the method used for entanglement generation or how



(a) no entanglement present

(b) all links successfully generate entanglement

(c) repeater nodes perform entangling measurements

(d) end nodes share an entangled state

Figure 1: Long-distance entanglement generation using quantum repeaters. The end nodes are communicating parties and the nodes between them are quantum repeaters. Dashed lines represent lack of entangled links, while solid lines represent presence of entanglement. Gray/red circles are unoccupied/occupied quantum memories, respectively.

quantum memories are realized.

We focus on the simplest variant of this problem, wherein links connecting users to the switch are identical, there is no quantum state decoherence, and the switch can store arbitrary numbers of qubits. We refer to the number of quantum memories at the switch as its *buffer size*. An unfortunate property of our DTMC model is that it is difficult to extend to model a less idealized system, *i.e.*, one with a finite buffer size, non-identical links, and non-negligible quantum state decoherence. Prior literature on quantum switch modeling utilizes continuous-time Markov chains (CTMCs) to account for these properties. Nevertheless, there is value in studying a quantum switch using a DTMC, as the system is inherently a discrete-time system, and while CTMCs have been shown to be more expressive as a modeling technique, there will undoubtedly be some differences in the resulting performance metrics. To quantify these differences, and determine whether a CTMC model provides a reasonable approximation to the original system, we compare the performance metrics obtained from both models.

Fig. 2a illustrates the problem setup: $k \geq 2$ users are connected to the quantum switch via dedicated, identical links. Time is slotted; the rest of Fig. 2 presents an example of a sequence of events that may take place in subsequent time slots. The purpose of the switch is to facilitate end-to-end entanglement generation for pairs of users that request it. The creation of an end-to-end entanglement involves two steps. First, in each time slot users attempt to generate pairwise (link-level) entanglements with the switch. A successful link-level entanglement results in a Bell state, with

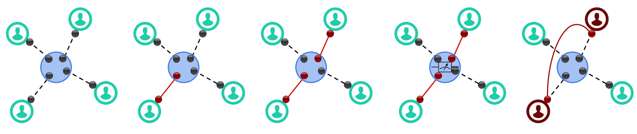


Figure 2: Example of quantum switch operation. No Bell pairs are present in **(a)**. When enough Bell pairs are successfully generated (solid lines in **(b)** and **(c)**), the switch performs a BSM **(d)**, entangling the two users' qubits **(e)**.

one qubit stored at the switch and the other stored at a user. In step two, the switch chooses two locally-held qubits, each entangled with a qubit held in a user's quantum memory, and performs a Bell state measurement (BSM). If the measurement is successful, the result is an end-to-end Bell pair between the corresponding pair of users. The switch continues to fulfill entanglement requests as long as there are available link-level Bell pairs for users who wish to communicate. At the end of the time slot, the switch may choose to store qubits from unused Bell pairs in local quantum memories until these qubits can be used in entangling measurements. This two-step process is repeated in subsequent time slots.

The capacity of a quantum switch is defined as the maximum achievable entanglement switching rate, which cannot be achieved with an arbitrary switching policy, or for an arbitrary set of user demands. To ensure that the switch operates at capacity, we allow it to perform a BSM as soon as there are at least two Bell pairs available on two distinct links, during a given time slot. This amounts to the assumption that any pair of users wish to communicate within each time slot. We also assume that the switch uses the *Oldest Link Entanglement First (OLEF)* rule when deciding which two users to pair up for an entangling measurement; *i.e.*, the switch prioritizes the oldest link-level Bell pairs for a BSM, as long as they belong to two different links. When there is more than one possible choice for such a pairing, then the switch may choose any two at random. Note that the OLEF rule does not affect the switch capacity, but it does happen to minimize the number of stored Bell pairs at the end of each time slot and thus this rule affects the qubit occupancy distribution. Finally, to ensure that the end users being serviced by the switch do not limit switch performance, we allow end nodes to have infinite and noiseless quantum storage. Following is a summary of our results:

– the DTMC is stable if and only if the number of users $k \geq 3$;
– the capacity of the switch is given by

$$C = \frac{qkp}{2},$$

where k is the number of users or links, p is the probability of successfully generating entanglement at the link level, and q is the probability of a successful BSM;
– the expected number of stored qubits is given by

$$E[Q] = \frac{1+\beta}{2(1-\beta)},$$

where Q is the number of qubits stored at the switch in steady state, across all links, and β is in the interval $(0, 1)$

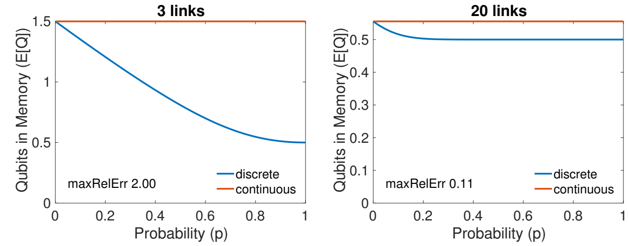


Figure 3: Comparison of the expected number of qubits in memory $E[Q]$ for the DTMC and CTMC models, for three and 20 links and for entanglement generation probabilities $p \in (0, 1)$. maxRelErr is the maximum relative error between the discrete and continuous expressions for $E[Q]$.

and is the unique solution to the following equation (where $\overline{p} \equiv 1 - p$) when $k \geq 3$:

$$(\beta p + \overline{p})^{k-1}(p + \beta\overline{p}) - \beta = 0;$$

– the expression for the capacity of the switch obtained using the DTMC matches exactly that of the CTMC model studied in [10]. On the other hand, the CTMC model overestimates the expected number of qubits in memory in steady state, but since the discrepancy is not significant (see Fig. 3), we conclude that the CTMC model is sufficiently accurate so as to be useful for exploring issues such as decoherence, link heterogeneity, and switch buffer constraints.

REFERENCES

[1] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Let.*, 1992.
[2] A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Let.*, 1991.
[3] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston, and A. V. Gorshkov. Optimal and Secure Measurement Protocols for Quantum Sensor Networks. *Phys. Rev. A*, 2018.
[4] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 2004.
[5] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel. Rate-loss analysis of an efficient quantum repeater architecture. *Phys. Rev. A*, 2015.
[6] L. Jiang, J. M. Taylor, A. S. Sørensen, and M. D. Lukin. Distributed quantum computation based on small quantum registers. *Phys. Rev. A*, 2007.
[7] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 2016.
[8] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 2017.
[9] M. Takeoka, S. Guha, and M. M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature communications*, 2014.
[10] G. Vardoyan, S. Guha, P. Nain, and D. Towsley. On the stochastic analysis of a quantum entanglement switch. *ACM SIGMETRICS Perf. Eval. Rev.*, 2019.
[11] Q. Zhuang, Z. Zhang, and J. H. Shapiro. Distributed quantum sensing using continuous-variable multipartite entanglement. *Phys. Rev. A*, 2018.
[12] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping. *Phys. Rev. Let.*, 1993.