On the Fly Dynamic Routing in Quantum Key Distribution Networks

Omar Amer[1] , Walter O. Krawec[1] and Bing Wang[1]
[1]Department of Computer Science, University of Connecticut
Storrs, CT, USA 06002
{omar.amer, walter.krawec , bing.wang}@uconn.edu

Objectives

Design efficient dynamic routing algorithms for quantum key establishment over long distance in near-term quantum networks using both quantum repeaters and trusted nodes

- Model network composed of trusted nodes (TNs) and repeaters
- Devise classical routing algorithms for routing in quantum network
- Characterize effects of network size, repeater quality, and decoherence rate
- Characterize and mitigate effect of non-ideal trusted node placement with dynamic balancing
- Focus on QKD allows for use of specialized classical/quantum tools over general entanglement networks [4][6]

Network Model:

3 Stage Model:

- First Stage - nodes attempt to establish entanglement with neighbors
- Second stage – nodes use routing algorithms to determine how to chain entanglement using bell state measurements
- Third stage – A/T/B use chained entanglement for E92 QKD protocol [1]

Loop until enough key material in network, then use max flow to push key material from A to B (XORing different keys at TNs)

Routing and Balancing:

For more details, including how these algorithms deal with non-global link level information, see paper [2] and upcoming work

- Basic routing – connect shortest A/T/B paths (based on [3][5])
- Symmetric TN placement -> key pools should be equivalent in expectation
- Asymmetric TN placement -> asymmetric key pools – inefficiency!
- Prioritize certain links to **balance** key pools
- Choose priority by finding surplus and bottleneck edges
- Incorporate priority both for global and local routing

Balancing vs. No Balancing

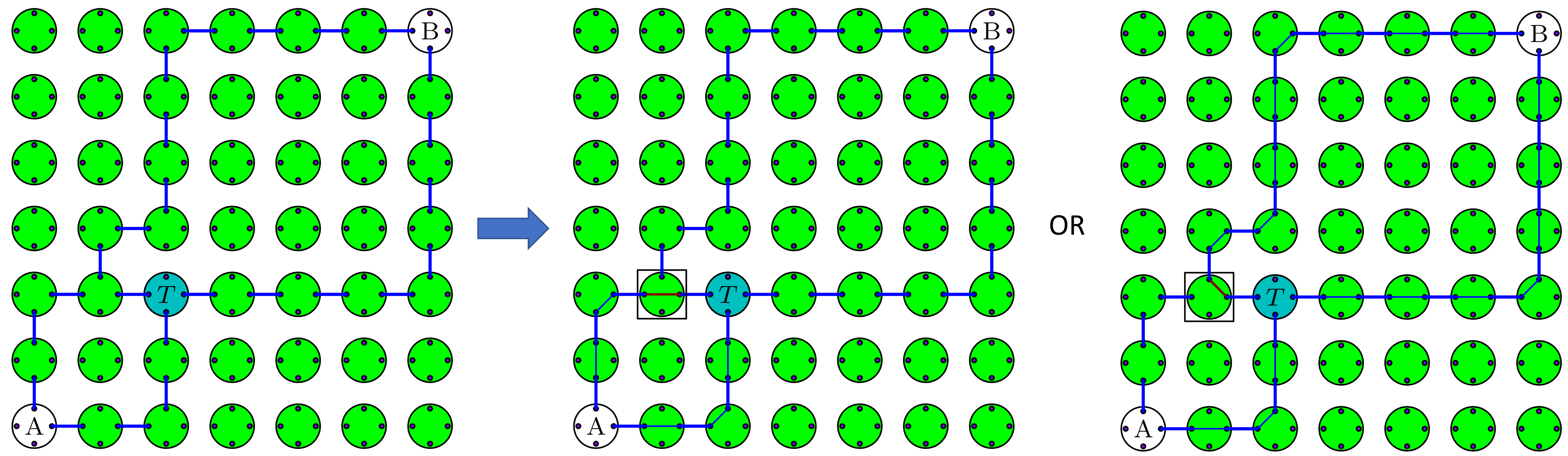

Figure 1: Possible shared entanglement graph after first stage of network with Alice, Bob, and **an asymmetrically placed trusted node.**

Figure 2: Routes chosen by our global routing algorithm **without the use of balancing** information to prioritize the T-B connection.

Figure 3 Routes chosen when **balancing information is used** – note that rather than connect A-T, the shortest options, we instead recover a longer T-B path. By making a different choice in the boxed area

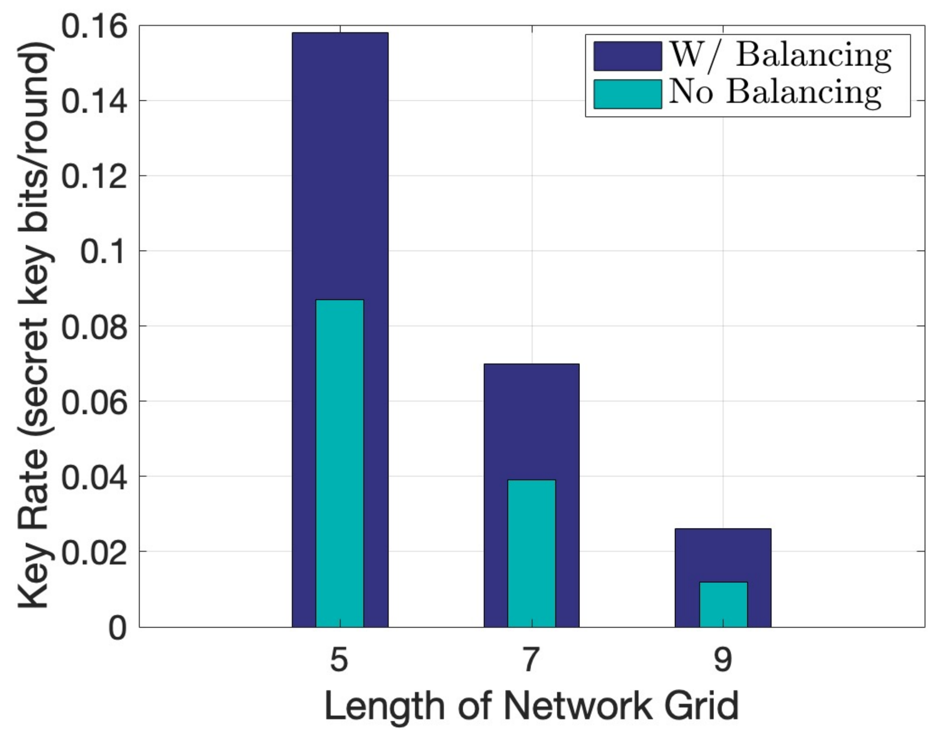

Figure 4: The relative performance of our global routing algorithm with and without balancing on different size networks with 2% decoherence on each link and 1e6 iterations. **Note that balancing results in almost twice the key rate in each case.**

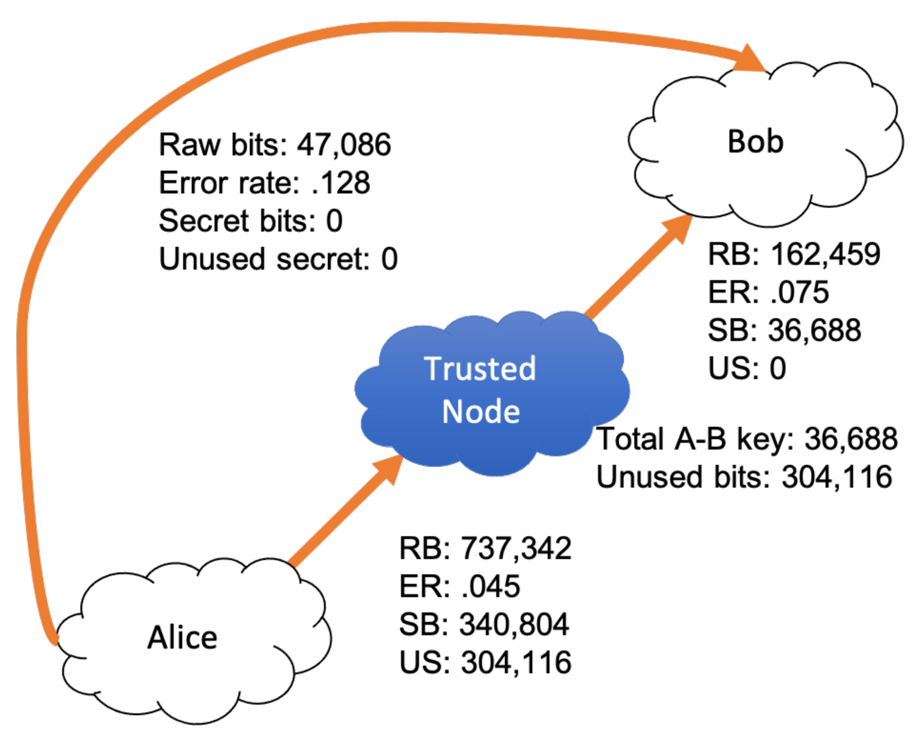

Figure 5: The size of the key pools after 1e6 iterations, showing the raw and secret key bit counts and the number of unused key bits in the network **without balancing in a** grid like Fig. 1-3, with 2% noises on each link.

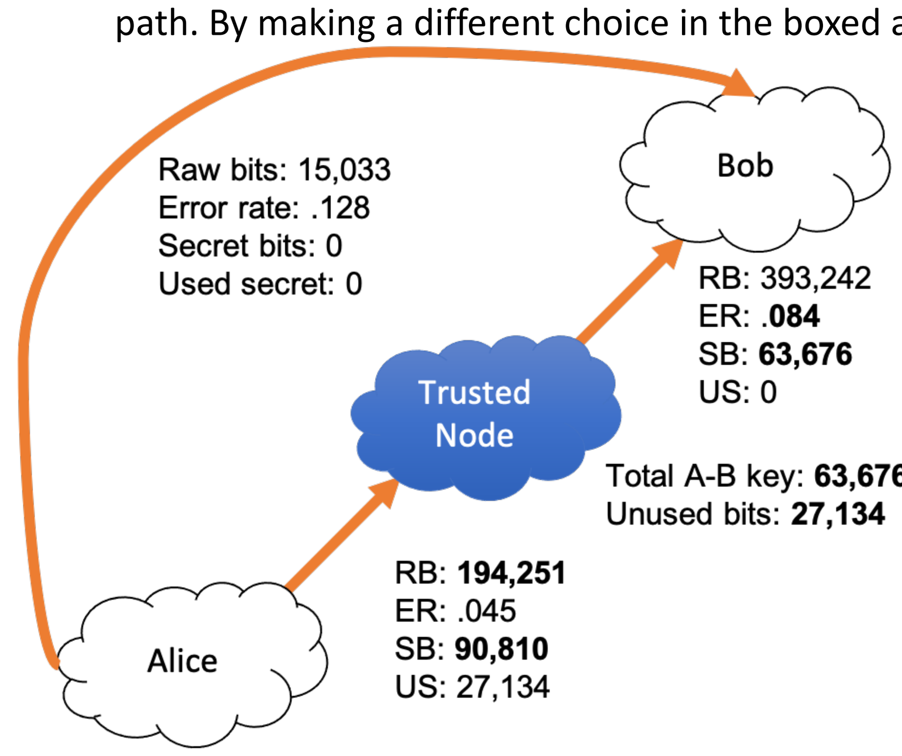

Figure 6: The results of the configuration as Fig. 5., but when **balancing** is used to prioritize the T-B path. Note the **smaller number of unused bits** and the noisier but larger key pool between T-B.

Future Work

Adapt our algorithms to be more efficient robust on a greater number of network models and scenarios

- Investigate additional classical methods of increasing key rate
- Investigate networks with heterogenous link characteristics and additional topologies
- Investigate additional topologies – including randomly generated networks

References

[1] Artur K Ekert. Quantum cryptography based on bell's theorem. Physical review letters, 67(6):661, 1991.
[2] Omar Amer, Walter O Krawec, and Bing Wang. Efficient routing for quantum key distribution networks. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE); arXiv:2005.12404, pages 137–147. IEEE, 2020.
[3] Mihir Pant, Hari Krovi, Don Towsley, Leandros Tassiulas, Liang Jiang, Prithwish Basu, Dirk Englund, and Saikat Guha. Routing entanglement in the quantum internet. npj Quantum Information, 5(1):1–9, 2019.
[4] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. Science, 362(6412), 2018.
[5] Stefano Pirandola. End-to-end capacities of a quantum communication network. Communications Physics, 2(1):1–10, 2019
[6] Kaushik Chakraborty, Filip Rozpedek, Axel Dahlberg, and Stephanie Wehner. Distributed routing in a quantum internet. arXiv preprint arXiv:1907.11630, 2019.