Tandem Queue Decomposition: An Optimal Policy for QKD Networks

Krishnakumar G[*]
krishnakumar97@smail.iitm.ac.in

Shahbaz Akhtar[*]
shahbaz.pee16@iitp.ac.in

Abhishek Sinha[†]
abhishek.sinha@tifr.res.in

1 INTRODUCTION

Quantum Key Distribution allows the secure exchange of symmetric private keys between users equipped with quantum links. These keys are then used to securely encrypt the messages prior to transmission over the classical channels. The laws of quantum mechanics guarantee the unconditional security of the key exchange. The key exchange process is distance-limited (typically a few hundreds of km). As quantum repeaters (required in quantum relaying network) are not cost-effective with the present technology, we focus on the **Trusted Node** setup, where packets are sequentially encrypted and decrypted along its path by the trusted nodes on each hop. Nodes are connected by communication links equipped with a quantum channel to exchange secret keys and a classical channel to transfer encrypted messages (see Fig. 1). The messages are encrypted using standard techniques such as One-Time Pad (OTP) or AES. The key exchange process is accomplished using standard QKD protocols such as BB84, E91, and B92.

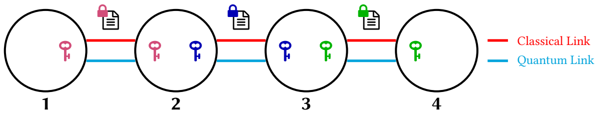

Figure 1: An example of a QKD Network with trusted nodes sharing private symmetric keys through quantum link and encrypted messages through classical link

Problem Statement: The quantum key exchange rate varies randomly due to limitations in the key generation and probable eavesdropping activities. With the limited key exchange rate and finite classical link capacity, we consider the problem of designing an optimal routing policy that securely routes packets at the maximum achievable rate. Existing policies for QKD networks allows unicast flow [4]. We propose *Tandem Queue Decomposition (TQD)*, a secure throughput-optimal policy that supports unicast, broadcast, and multicast traffic. To the best of our knowledge, no capacity-achieving policy was previously known for supporting broadcast and multicast flows in QKD networks.

2 SYSTEM MODEL

We consider an arbitrary topology network represented by a graph $\mathcal{G}(V,E)$ with $|V| = n$ nodes and $|E| = m$ edges. Each edge $e \in E$ is equipped with two links: a classical link with link capacity γ_e and a quantum link that generates keys at rate η_e[1]. The residual keys $k_e(t)$ are stored in a key bank and $\kappa_e(t) = K_e(t) + k_e(t)$. Unlike the paper [4], we do not set a hard limit on the size of the key bank since the abundance of encryption keys is always desired. To consider a general class of traffic, we group incoming packets into classes C depending on their source $s^{(c)}$ and set of destinations $d^{(c)}$. The total number of new packet arrivals to the entire network at any slot is upper bounded by A_{max}.

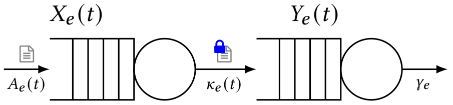

Figure 2: TQD architecture for a single link e

3 TQD POLICY

We now describe the architecture central to our proposal. We split the single data queue at each edge into two. Each edge maintains two physical queues X_e, Y_e in tandem, where packets wait for the key and the physical link capacity respectively to be available to cross the edge e. In addition, TQD maintains two virtual queues for each edge $\tilde{X}_e$ and $\tilde{Y}_e$ in tandem, corresponding to the physical queues X_e and Y_e. Our goal is to obtain a policy that stabilizes the data queues for all arrival rates within the capacity region. TQD uses UMW policy[3] on this transformed network.

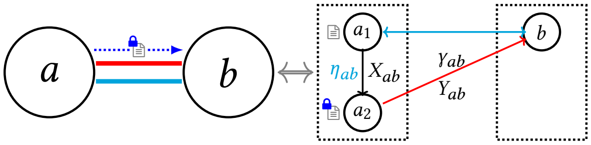

Figure 3: Secure packet transmission from Node a to b is viewed on a transformed network containing abstract nodes a_1, a_2 within node a depicting two queues X_{ab} and Y_{ab}

TQD decides the route of the packets at the source node by computing "weighted-shortest-path" in the virtual system, where the edge weight is updated as $W_e = (\tilde{X}_e + \tilde{Y}_e)$ [1]. Precedence constraints are relaxed for these virtual queues, *i.e.,* upon packet arrival, its route is computed, and all virtual queues in its route receive the packet, in contrast to the physical queues, where a packet crosses the current edge e. Packets are scheduled using **ENTO** policy [2]. Note that the policy is derived by drift-minimization of quadratic Lyapunov function $L(\tilde{Q}(t)) = \sum_{e \in E} \left(\tilde{X}_e^2(t) + \tilde{Y}_e^2(t)\right)$.

4 RESULT

Under the TQD policy, we show that the network supports any arrival rate within the secure capacity region. The stability of virtual queues is established using the standard drift comparison argument against the stationary randomized policy. By using an appropriate scheduling policy, the stability of physical queues is established. Furthermore, TQD offers loop-free routing leading to enhanced delay performance.

5 EXTENSION TO MULTICLASS SECURITY

In a heterogeneous network, some nodes lack QKD modules and will only have the Y_e queues. Also certain packets not needing encryption getting queued at X_e is a waste of resource operation. Let $E_S \subseteq E$, be the links with QKD modules. The route of packets requiring encryption is computed on the induced graph $\mathcal{G}(V, E_S)$. For all other packets, the shortest path route is computed on $\mathcal{G}(V,E)$ with $W_e = \tilde{Y}_e$. They skip X_e and join Y_e queues directly along their path. It is interesting to note that this extension does not compromise the throughput-optimality.

6 CONCLUSION/OPEN QUESTIONS

We have proposed a provably throughput-optimal centralized routing policy to improve the delay performance in QKD networks. Exploring the possibility of optimal distributed algorithms, investigating the performance advantage of one over another, extending TQD to time-varying QKD networks, and relaxing the trusted node assumption are some directions to proceed further.

REFERENCES

[1] Vishnu B and Abhishek Sinha. 2022. Fast and Secure Routing Algorithms for Quantum Key Distribution Networks. In *2022 14th International Conference on COMmunication Systems NETworkS (COMSNETS)*. 120–128.

[2] David Gamarnik. 1999. Stability of adaptive and non-adaptive packet routing policies in adversarial queueing networks. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*. 206–214.

[3] Abhishek Sinha and Eytan Modiano. 2017. Optimal control for generalized network-flow problems. *IEEE/ACM Transactions on Networking* 26, 1 (2017), 506–519.

[4] Hongyi Zhou, Kefan Lv, Longbo Huang, and Xiongfeng Ma. 2022. Quantum Network: Security Assessment and Key Management. *IEEE/ACM Transactions on Networking* (2022).

[*] Dept. of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India

[†] School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India

[1] The number of keys generated over QKD link e at slot t is $K_e(t)$