Инженерный вестник Дона, №7 (2024)
ivdon.ru/ru/magazine/archive/n7y2024/9347

Обзор методов оптимизации топологии сетей квантового распределения ключей

Е.С. Раздьяконов

Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: В настоящий момент технология квантового распределения ключей (КРК) гарантирует наивысший уровень безопасности обмена данными, что делает сети КРК одним из самых перспективных направлений в области компьютерной безопасности. К сожалению, проблема оптимизации топологии при планировании и расширении сетей КРК не привлекла достаточного внимания. В данной работе проводится обзор исследований, использующих аналитические модели, в задаче оптимизации топологии сетей квантового распределения ключей. Рассматриваются методы, решающие задачи максимизации пропускной способности и безопасности при минимальных затратах, описываются используемые алгоритмы, а также делаются выводы о возможных дальнейших исследованиях в данной области.
Ключевые слова: квантовое распределение ключей, математическое моделирование, топология сети, аналитическое моделирование, оптимизация топологии.

Введение

Безопасный обмен криптографическими ключами является одной из фундаментальных задач в области криптографии. Большинство существующих подходов предполагают, что для успешной атаки злоумышленник должен располагать большим количеством вычислительных мощностей. Несмотря на то, что взлом таких криптографических алгоритмов сложен, он не является теоретически невозможным. Учитывая современные темпы роста вычислительных мощностей и возможность появления доступных квантовых компьютеров в будущем, традиционные методы защиты информации могут оказаться под угрозой.

Технология квантового распределения ключей (КРК) делает процесс обмена ключами теоретико-информационно безопасным, то есть независимым от вычислительных ресурсов злоумышленника [1]. Это делает КРК перспективной технологией из области компьютерной безопасности.

Тем не менее, у сетей квантового распределения ключей имеется ряд отличий от классических коммуникационных сетей. Наиболее

существенными являются ограниченная скорость генерации и передачи ключей, зависящая от длины соединения [2], отсутствие квантовых повторителей на практике [3] и необходимость передачи ключей только в соединениях точка-точка [4]. Эти ограничения делают эффективность сетей КРК сильно зависимыми от топологии. Таким образом, при планировании сети очевидна потребность в более точной оценке топологии для максимизации безопасности и производительности, а также минимизации затрат.

В данной работе будут рассмотрены существующие методы оптимизации топологий сетей квантового распределения ключей, основанные на аналитических моделях.

Методы оптимизации топологии сетей КРК

Процесс анализа топологий компьютерных сетей подразумевает собой построение математических моделей. Несмотря на то, что в данный момент в области математического моделирования сетей КРК преобладают работы, посвященные имитационным моделям, аналитические модели могут оказаться полезными благодаря скорости и упрощенному поиску глобального экстремума.

Задача минимизации стоимости при заданных требованиях к производительности сети КРК была поставлена в [5]. В данной работе был представлен ряд аналитических моделей для оптимизации расположения узлов и соединений сети КРК, включая одномерную линейную топологию и произвольную двумерную топологию, распределение пользователей в которой описывается процессом Пуассона. Для двумерных сетей также исследуется возможность использования магистральной сети КРК.

В работе задаются целевые функции стоимости для различных топологий, зависящие от скорости передачи данных и длины соединения. В случае с двумерной топологией без магистральной сети, функция стоимости

представляет из себя сумму стоимостей линейных сетей между парами пользователей. При использовании магистральной сети оценивается как сама топология магистральной сети, так и расположение пользователей относительно ее узлов.

В результате исследования были приведены модели для оптимизации стоимости сетей КРК, а также описаны условия, при которых использование магистральных сетей оказывается выгодным. Наиболее оптимальными в рамках эффективности и стоимости оказались сети с длинами соединений, близкими к фиксированной оптимальной длине, определяемой свойствами оптического канала.

Иной метод оценки топологии сетей КРК предложен в [6]. В данной работе решается обобщение задачи о максимальном потоке на случай с несколькими источниками и стоками, поэтому классические алгоритмы решения не могут быть применены напрямую. Сеть представляется в виде взвешенного графа, где веса вычисляются в соответствии с теорией [7].

Для численной оценки качества топологии сети авторами вводится метрика, информационно-теоретическая безопасная граница связи (information-theoretic secure communication bound), учитывающая как пропускную способность квантового соединения, так и скорость генерации ключей на узлах. Для ее вычисления задача о максимальном потоке сводится к линейной и применяется алгоритм целочисленного линейного программирования.

Полученная модель была протестирована в двух экспериментах, отражающих типичные задачи при планировании топологий. В первом эксперименте оценивалось, на каком ребре сети эффективнее всего разместить КРК-систему. Во втором эксперименте оценивалось, где лучше добавить дополнительные узлы для увеличения производительности.

В обоих экспериментах оптимальная топология выбиралась путем вычисления оценки для каждого из возможных вариантов и выбора конфигурации, для которой метрика оказывалась максимальной.

В [8] была рассмотрена задача оптимизации топологии гибридных сетей КРК, использующих несколько видов квантовых устройств и протоколов одновременно.

Целью работы являлось нахождение оптимального размещения доверенных и недоверенных узлов КРК, а также соединений типа клиент-клиент и клиент-сервер-клиент на основе существующей классической сети. В качестве показателей эффективности использовались схожие метрики, что и в [6].

Так, с учетом топологии существующей сети, допустимых размещений узлов и ребер различных типов, а также ограничения на суммарную стоимость оборудования, метод сводится к решению задачи целочисленного линейного программирования.

Были проведены эксперименты со случайно сгенерированными и существующими топологиями, показавшие преимущества использования гибридных сетей квантового распределения ключей.

Работа [9] посвящена оптимизации сети в соответствии с требованиями по пропускной способности, зависящей от расстояния между узлами в пространстве, и безопасности, зависящей от топологии, а именно от количества промежуточных узлов между парой пользователей.

На основе пропускной способности квантового соединения, описанной в [10], и предположения о безопасности [11], согласно которому промежуточные узлы сети квантового распределения ключей, в отличие от соединений, являются безопасными только с некоторой вероятностью.

Таким образом, наиболее безопасной сетью является сеть с минимальным количеством узлов в соединениях между клиентами, а сеть с

минимальной длиной соединения между узлами обладает наибольшей пропускной способностью. Авторы вводят метрику коммуникационной эффективности с дополнительным параметром α, позволяющим пользователю задать приоритет либо безопасности ($\alpha = 1$), либо пропускной способности ($\alpha = 0$).

Имея данные о расположении узлов на плоскости и допуская, что между каждой парой узлов можно проложить соединение, то есть граф всех возможных соединений является полным, оптимальный путь между парой узлов является путем с максимальной коммуникационной эффективностью. При $\alpha \to 1$ оптимальный путь представляет собой прямое соединение между конечными узлами, а при $\alpha \to 0$ путь проходит между множеством ближайших промежуточных узлов. Глобальная эффективность сети является средним значением эффективности путей между всеми парами узлов.

Оптимальная сеть между множеством узлов на плоскости является объединением оптимальных путей между всеми парами узлов в полном графе. Так как в задаче поиска оптимального пути для сети КРК неприменимы методы на основе динамического программирования, авторами была разработана модификация алгоритма Поллака [12]. В работе был проведен анализ полученных оптимальных топологий сетей с использованием численных и аналитических методов.

Несмотря на то, что результатом работы данного метода является глобально-оптимальная топология сети, в случае с большим количеством узлов такой подход потребует значительного времени выполнения.

Выводы

В данной работе был проведен обзор существующих методов оптимизации топологии сетей квантового распределения ключей. В отличие от классических телекоммуникационных сетей, область оптимизации топологии сетей КРК все еще недостаточно исследована.

В ходе обзора были выделены возможные направления для исследований в данной области:

- Разработка методов оптимизации для оптимального размещения промежуточных узлов на основе информации о конечных узлах;
- Использование метаэвристических алгоритмов оптимизации для поиска приближенных решений, что может оказаться эффективным в случае большого количества узлов;
- Оптимизация топологии сети для параллельной передачи данных между двумя узлами по нескольким каналам.

Литература

1. Габдулхаков И.М., Морозов О.Г. Построение многоканальной системы квантового распределения ключей с частотным кодированием // Инженерный вестник Дона, 2020, №. 5. URL: ivdon.ru/ru/magazine/archive/N5y2020/6438

2. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., Voznak M. Quantum key distribution: a networking perspective //ACM Computing Surveys (CSUR). – 2020. – Vol. 53. – №. 5. – pp. 1-41.

3. Salvail L., Peev M., Diamanti E., Alléaume R., Lütkenhaus N., Länger T. Security of trusted repeater quantum key distribution networks //Journal of Computer Security. – 2010. – Vol. 18. – №. 1. – pp. 61-87.

4. Peev M., Poppe A., Maurhart O., Lorunser T., Langer T., Pacher C. The SECOQC quantum key distribution network in Vienna //New Journal of Physics. – 2009. – Vol. 11. – №. 7. – p. 075001.

5. Alleaume R., Roueff F., Diamanti E., Lütkenhaus N. Topological optimization of quantum key distribution networks //New Journal of Physics. – 2009. – Vol. 11. – №. 7. – p. 075002.

6. Li Q., Wang Y., Mao H., Yao J., Han Q. Mathematical model and topology evaluation of quantum key distribution network //Optics Express. – 2020. – Vol. 28. – №. 7. – pp. 9419-9434.

7. Gottesman D., Lo H. K., Lütkenhaus N., Preskill J. Security of quantum key distribution with imperfect devices //International Symposium on Information Theory, 2004. ISIT 2004. Proceedings. – IEEE, 2004. – p. 136.

8. Wang Y., Li Q., Mao H., Han Q., Huang F., Xu H. Topological optimization of hybrid quantum key distribution networks //Optics Express. – 2020. – Vol. 28. – №. 18. – pp. 26348-26358.

9. Cirigliano L., Brosco V., Castellano C., Conti C., Pilozzi L. Optimal quantum key distribution networks: capacitance versus security //npj Quantum Information. – 2024. – Vol. 10. – №. 1. – p. 44.

10. Pirandola S., Laurenza R., Ottaviani C., Banchi L. Fundamental limits of repeaterless quantum communications //Nature communications. – 2017. – Vol. 8. – №. 1. – pp. 1-15.

11. Solomons N. R., Fletcher A. I., Aktas D., Venkatachalam N., Wengerowsky S., Lončarić M., Neumann S. P., Liu B., Samec Ž., Stipčević M. Scalable authentication and optimal flooding in a quantum network //PRX quantum. – 2022. – Vol. 3. – №. 2. – pp. 020311.

12. Pollack M. The maximum capacity through a network //Operations Research. – 1960. – Vol. 8. – №. 5. – pp. 733-736.

References

1. Gabdulhakov I.M., Morozov O.G. Inzhenernyj vestnik Dona, 2020, №. 5. URL: ivdon.ru/ru/magazine/archive/N5y2020/6438

2. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., Voznak M. ACM Computing Surveys (CSUR). 2020. Vol. 53. №. 5. pp. 1-41.

3. Salvail L., Peev M., Diamanti E., Alléaume R., Lütkenhaus N., Länger T. Journal of Computer Security. 2010. Vol. 18. №. 1. pp. 61-87.

4. Peev M., Poppe A., Maurhart O., Lorunser T., Langer T., Pacher C. New Journal of Physics. 2009. Vol. 11. №. 7. p. 075001.

5. Alleaume R., Roueff F., Diamanti E., Lütkenhaus N. New Journal of Physics. 2009. Vol. 11. №. 7. p. 075002.

6. Li Q., Wang Y., Mao H., Yao J., Han Q. Optics Express. 2020. Vol. 28. №. 7. pp. 9419-9434.

7. Gottesman D., Lo H. K., Lütkenhaus N., Preskill J. International Symposium on Information Theory, 2004. ISIT 2004. Proceedings. IEEE, 2004. p. 136.

8. Wang Y., Li Q., Mao H., Han Q., Huang F., Xu H. Optics Express. 2020. Vol. 28. №. 18. pp. 26348-26358.

9. Cirigliano L., Brosco V., Castellano C., Conti C., Pilozzi L. npj Quantum Information. 2024. Vol. 10. №. 1. p. 44.

10. Pirandola S., Laurenza R., Ottaviani C., Banchi L. Nature communications. 2017. Vol. 8. №. 1. pp. 1-15.

11. Solomons N. R., Fletcher A. I., Aktas D., Venkatachalam N., Wengerowsky S., Lončarić M., Neumann S. P., Liu B., Samec Ž., Stipčević M. PRX quantum. 2022. Vol. 3. №. 2. pp. 020311.

12. Pollack M. Operations Research. 1960. Vol. 8. №. 5. pp. 733-736.

Дата поступления: 13.05.2024
Дата публикации: 22.06.2024