УДК 530.145:535.12

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПТИМИЗАЦИИ СИСТЕМ КРКБЧ

Тупяков Д.В. (Университет ИТМО)

Научный руководитель – кандидат физико – математических наук, Киселев Ф.Д. (Университет ИТМО)

Введение. Квантовое распределение ключей (КРК) в настоящее время можно признать одной из самых многообещающих областей квантовых коммуникаций и криптографии в целом. Одним из преимуществ КРК перед классическими методами шифрования является то, что безопасность передачи данных основана на фундаментальных принципах квантовой механики. Значительный интерес вызывает возможность внедрения системы КРК в существующую волоконную оптическую линию связи (ВОЛС) на основе технологии мультиплексирования с разделением по длине волны (WDM), что обусловлено практическим удобством и экономической выгодой. Однако, это достаточно трудная задача. Во-первых, на слабый сигнал квантового канала негативно влияют гораздо более мощные информационные (классические) каналы. В результате чего шумовые сигналы, образованные в результате нелинейных эффектов в оптическом волокне, попадают в спектральную полосу квантового канала. Во-вторых, с появлением первых протоколов КРК начали развиваться и способы атаки на системы, основанные на них. Наконец, любая действующая система КРК, требует эффективного управления с обратной связью в реальном времени для поддержания стабильности системы при столкновении с помехами из внешней среды или несовершенством внутренних компонент.

В настоящее время разработано большое множество методов уменьшения негативного влияния классических каналов и предотвращения или противодействия атакам. Однако решения задач, связанных с несовершенством оборудования, все еще находятся в разработке. Система, реализующая сеанс КРК через существующую ВОЛС, является динамической, ввиду неидеальности её оставляющих, таких как детекторы, модуляторы и фильтры. Их характеристики в общем случае непостоянны, они зависят от времени и условий внешней среды, таких как температура, влажность и т. п. Так как параметры КРК выбираются, основываясь на характеристиках оборудования, так чтобы достичь наибольшей эффективности работы, необходима постоянная перенастройка параметров КРК под новые характеристики оборудования в режиме реального времени. Такая задача может быть решена классическим методом с применением алгоритма локального поиска [1] определяющего локальный экстремум функции нескольких переменных. Однако такой способ требует больших вычислительных и временных ресурсов, в связи с чем проведение настройки в режиме реального времени, основываясь на классическом методе оптимизации, не представляется возможным. В последнее время набирают популярность методы, основанные на применении машинного обучения. Возрастающий интерес к подобным подходам основан на том, что способы, основанные на машинном обучении, позволяют не только упростить процесс развертывания систем КРК в существующей ВОЛС, но и создавать практически автономные динамические системы, способные подстраиваться под изменяющиеся условия.

Основная часть. Предлагаемое решение заключается в использовании нейронной сети, основанной на методах статистики, позволяющей предсказать наиболее близкое к оптимальному значение параметров КРК, затратив намного меньшее количество временных и вычислительных ресурсов. Подобное решение уже рассматривалось для систем КРК с поляризационным кодированием BB84 [2] и не зависящих от измерительных устройств систем КРК (MDI) [3]. В этой работе будет рассмотрено применение нейронной сети для оптимизации систем на многомодовых когерентных состояниях, в частности систем КРК на боковых частотах фазомодулированного излучения (КРКБЧ) [4,5], и проведена оценка эффективности

и целесообразности такого решения. Для достижения поставленной цели выполнены следующие три этапа работы:

1) Подготовка обучающих данных, заключающихся в случайных наборах возможных параметров оборудования и соответствующих им оптимальных параметров системы, вычисленных с помощью локального поиска;
2) Разработка, обучение и оценка эффективности нейронной сети;
3) Внесение изменений в обучающие данные и в нейронную сеть для увеличения ее эффективности согласно выводам, полученным на втором этапе, повторная оценка эффективности исследуемого решения, заключение о возможности применения нейронных сетей для оптимизации систем КРКБЧ.

Выводы. Полученная на конечном этапе нейронная сеть способна за время порядка десятых долей миллисекунд с точностью порядка 98% (относительно результатов локального поиска) определять оптимальные параметры системы КРКБЧ, отталкиваясь от текущих значений характеристик оборудования. Такие показатели позволяют заключить, что применение машинного обучения в области КРК является перспективным направлением, потенциально способным справляться с задачами, требующими решения в режиме реального времени.

Список использованных источников:

1. Xu F., Xu H., Lo H.K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution // Phys. Rev. A. — 2014. — Vol. 89. — P. 052333.
2. Wang W., Lo H.K. Machine learning for optimal parameter prediction in quantum key distribution // Physical Review A. — 2019. — Vol. 100..
3. Predicting optimal parameters with random forest for quantum key distribution / Hua-Jian Ding [et al.] // Quantum Information Processing. — 2020. — Vol. 19.
4. Analysis of the chromatic dispersion effect on the subcarrier wave QKD system / F. Kiselev [et al.] // Optics Express. — 2020. — Vol. 28. — P. 28696.
5. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack / Anton Kozubov [et al.] // Optics Express. — 2018. — Vol. 26. — P. 1292–11308.