Universiteit Leiden

Master Computer Science

Title :Discovering quantum communication strategies with multi-agent reinforcement learning

Name: Athanasios Agrafiotis

Student ID: s2029413

Date:

Specialisation: Advanced Data Analytics

1st supervisor: Evert Van Nieuwenburg

2nd supervisor:

Master's Thesis in Computer Science

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden

This dissertation is submitted for the degree of
Computer Science(MSc): Advanced Data Analytics

October 2022

Acknowledgements

Abstract

Communication channel systems are easy to use; however, they are vulnerable to attacks by a third person. The third person can easily penetrate the channel and read or manipulate messages before reaching the receiver from the sender. For this purpose a number of protocols are recommended that can secure the communication between the two parties. Nowadays, quantum computing has been shown to get benefit from such scenarios and introduces protocols that can encrypt and decrypt a message. One of those protocols is the protocol of Bemett and Brassard. The purpose of this Master thesis is to present a simulation of a quantum communication channel using reinforcement learning algorithms. In more details it describes in details how the sender and the receiver exchange messages and how they verify the security of the channel with a secret key.

The main goal of this Master thesis is to simulate a Quantum key distribution process using artificial intelligence environment. In each episode the two agents are using a communication channel. The first agent reads a message and then sends it to second agent , the receiver verify the message correctness. In case the message has been transferred successful, the episode ends with the maximum reward in the other cases the reward is negative.

A number of reinforcement learning algorithms are implemented during the Master thesis project. Namely a Q-learning, deep q learning approach that solves artificial environment with optimal solutions. As a result the agent performs that actions that is required to communicate with each other avoiding any mistakes.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

The current project has as a main goal to simulate an artificial environment of quantum key Distribution. The process that describes a communication between two artificial agents that takes place in a quantum channel. For reasons of security, the channel uses a protocol that encrypts And decrypts the messages with some error. Next, the sender and the receiver communicate with a classical to channel to compare the message and to evaluate the protocol key's. The quantum Channels use quantum gates as key that produce a small amount of error. In the artificial environment, each of the two agents can make at least ten actions until the episode ends and communication to finish. In case each of the agents makes the required actions the episode finishes earlier and gives a positive reward to the agent. The communication channel generates a message that the sender will read it, next will send it to receiver that he will compare both messages and saves the key.
To solve the environment, it is a proposed reinforcement learning algorithm. Algorithms can explore the environment until to find an optimal solution playing a large number of episodes.
The project focuses on the following research questions:
Does the reinforcement learning environment simulate a Quantum key distribution?
Is the communication of a quantum channel that implements the BB84 protocol secure?
Is the protocol efficient?
To sum, the project deploys an artificial environment that represents as states the encryption/decryption between messages of two parties. The implementation of a software that takes as an input a plain text(cipher-text) encrypts the message and decrypts it. The implementation includes the quantum polarization base of each bit. An error analysis and the parameters that have been used during the simulation such as bitstream length, error correction, number of iterations will determine the key quality.

Chapter 2

Background

2.1 Example

2.2 Quantum Key distribution Related Work

The related work et al [] it presents how to ensure risk management despite attacks on communication protocol. Current state-of-the-art-key distribution and management processes face constraints and challenges such as managing numerous encryption keys. The model demonstrates the BB84 (QKD) protocol with two scenarios; the first is without eavesdropper and the second is with eavesdropper via the interception-resend attack model. The simulation is highly dependent on a communication over a quantum channel for polarized transmission. The cryptographic part relies on three components. First, the plain text that will be encrypted, key used for the encryption; at last the output (cipher-text) encrypted message. The number of keys is two; one of the keys is public (encryption key) and the private key(decryption key). Two parties communicate with each other , the party A, and party B. The simulation is based on the communication of the two parties and in case the party A wants to send a message to party B is using the Party B's public key for the encryption and Party's B private key for the decryption. The procedure of simulation uses quantum blocks, the Party's A QB transmitter, Party's B QB receiver, and at last the Eve's QB non-authorized access to the quantum channel. The paper concludes that the error is detectable with error correction rate 0.24% and 0.26% with eavesdropper, so the key has improved after each message exchange until to reach the paper's proposed threshold 0.11. Finally, the paper mentions that comparison of two scenarios with and with eavesdroppers is complicated to compare to previous work, as their analysis does not clearly state their parameters and the error.

Chapter 3

Methods & Data

Chapter 4

Results

Chapter 5

Discussion

Chapter 6

Conclusion

Chapter 7

Software

References