Received 20 December 2022, accepted 19 February 2023, date of publication 2 March 2023, date of current version 7 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3251649

RESEARCH ARTICLE

A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking

OMAR SHIRKO, (Graduate Student Member, IEEE), AND SHAVAN ASKAR, (Senior Member, IEEE)

Department of Information System Engineering, Erbil Polytechnic University, Erbil 44001, Iraq

Corresponding author: Shavan Askar (shavan.askar@epu.edu.iq)

ABSTRACT Quantum key distribution (QKD) is a technique for distributing symmetric encryption keys securely using quantum physics. The rate of key distribution is low and decreases exponentially with increasing distance. A classic trusted relay (CTR) uses additional keys to enhance security distance in QKD networks. In practice, the assurance of security for certain relay nodes is still lacking, despite the fact that CTR requires that all nodes be trusted. Owing to channel unreliability, system faults accumulate during the key relay, thereby increasing the probability of CTR failing to distribute the secret key. The failure of a successful key relay would then result in the subsequent destruction of all the keys involved in the process, which leads to the wasting of the quantum secret key and reduction system encryption. Hence, alleviating the effect of CTR failure for the purpose of obtaining key security distribution of distant quantum network is necessary issue to tackle. Therefore, a new scheme is needed in order to overcome the above-mentioned issues to come up with a better utilization of the generated keys. In this study, a software-defined networking (SDN) technique is introduced to circumvent this drawback by utilising the flexibility provided by the SDN paradigm for better QKD network management. In particular, a novel survivability model called software-defined quantum key relay failure (SDQKRF) is proposed in this paper in which a new function is developed and added to the SDN controller. According to the simulation results, SDN over a QKD network using the SDQKRF model is more reliable and performs better in terms of the key generation ratio, key utilisation rate, recovery after failure, avalanche effect, and service blocking rate than a regular QKD network without the SDQKRF model.

INDEX TERMS Quantum key distribution (QKD), software-defined network (SDN), survivability, classical trusted relay (CTR).

I. INTRODUCTION

It is expected that by 2023, approximately two-thirds of the world population will have Internet access, this suggests that the amount of Internet users is estimated to will increase from 3.9 billion (51% of the world population) in 2018 to 5.3 billion (66% of the world population) in 2023 [1]. The increase in internet access will lead to an increase in the number of security breaches such as eavesdropping and data interception, which consequently can result in the loss of personal information, financial losses, and significant disruptions to services [2], [3]. Therefore, cryptographic techniques became an inevitable alternative to ensure the safety of communication carried out through the internet [4]. However, one of the most essential cryptographic tasks is to establish secure cryptographic keys across untrusted networks [5]. Traditionally, encryption methods based on public-key cryptography have been used, enabling cryptographic keys to be distributed over unreliable networks. Although public-key cryptography security relies on the computational complexity

The associate editor coordinating the review of this manuscript and approving it for publication was Abderrahmane Lakas.