CHAPTER 1

INTRODUCTION

1.1 Background

As the network's use grows, the complexity level increases, such as an increased routing scheme. Routing is indispensable to finding the best connection between hosts who want to communicate. The best path-finding technique can be done using metrics, such as metric hop count and cost. Metric hop count uses a distance vector routing, and cost uses a link-state routing. These routines are applied to conventional networks based on software-defined networking (SDN). SDN is a concept of a separate computer network architecture approach controller with the device, so it becomes an innovation utilized in this thesis related to its ability, that is, being able to control the network centrally, programmability, and scalability. The ability to control centrally is needed in the search for the best path by condensing metric hop and cost, while programmability is related to network optimization in path search, and scalability relates to the use of resources. This thesis uses OpenDaylight as a network controller because in its application OpenDaylight has an internet protocol (IP) that is used to find out the path that connects the source with the destination and makes it easier for users to configure the switch by looking at the graphical user interface (GUI) display on the controller side.

In addition, SDN-based can be implemented in quantum networks. Quantum networks are needed to exchange quantum information. Quantum information consists of quantum bits as carriers of information called qubits, which are sent using photons. Photons are light that is not polarized but can be polarized with two rectilinear and diagonal-based filters because of the uniqueness of photons that are not easily duplicated and intercepted so that they can be used for information security. A quantum network generally consists of two channels: The classical channel and the quantum channel. Classical channels exchange and send information as in conventional networks, while quantum channels exchange and send quantum-based information. The combination of the two channels can form a quantum key distribution (QKD) channel, resulting in the exchange of secret keys.

Several related studies discuss a lot about the characteristics of the network quantum, including focusing on the distance to transmit photons, maximum generating keys, optimizing network topologies, and QKD protocol functions [1]. The research is based on the quantum network project that has been carried out by the defense advanced research projects agency (DARPA) QKD, united bold Beranek and Newman (BBN), Boston University, and Harvard University jointly completed the world's first quantum cryptographic network structure [2]. Research by [3] conducted a wavelength test based on the QKD network that uses a star topology and uses the BB84 protocol, and the BB84 decoy-state protocol [4]-[6]. This network relies on telecommunications infrastructure by demonstrating the feasibility of integrating QKD into a network based on four QKD router ports [7]. Secure communication based on quantum cryptography (SECOQC) [8] is a six-node and eight-chain QKD-based metropolitan network built in Vienna, 2010 TOSHIBA IDQ Switzerland and several Australian groups working with the QKD Tokyo network collaboration [9]. QKD network protocols used, such as BB84, SARG04, decoy-state BB84, COW, BBM92, and CV-QKD. The encryption application used is a one-time pad (OTP). Research by [10] tested the CV-QKD network with an entire mesh topology in Shanghai using gaussian modulation. This network consists of four nodes connected by six QKD links using optical fiber to provide all-to-all interconnection and does not use optical fiber by technique wavelength-division multiplexing (WDM) to demonstrate the feasibility of implementation CV-QKD. Research by [11] implemented the QKD network in Cambridge by implementing the DV-QKD network using the BB84 protocol. Which channel used is the quantum channel and the classical multiplex channel using the WDM method, so testing proves the secret key is produced at a speed of 2-3 Mbps using the advanced encryption standard (AES) cryptographic method. Research by [12] was conducted in Bristol by testing the QKD network capability on four SDN-based nodes and carrying out connectivity testing QKD-secured. Research by [13] implemented the QKD network using the BBM92 protocol to support secure connections using 28 key pairs of eight users.

Optimizing the use of keys can be overcome by implementing an SDN-based network. When a routing update occurs, the information sent is only necessarily broadcast to some network devices [14]. Therefore, network devices only need to send information to the controller. Besides that, random routing can be implemented according to the application programming interface (API), which is already available on the controller and capable of monitoring links online. Dijkstra's algorithm as a value-based

path determines the lowest cost. However, the selection of the best path with the cost is not necessarily through the route shortest based on the number of hops because it is broadcasting one data that consumes one secure key [14]. Research by [15] implemented stochastic routing based on the number of shortest hops and the remaining link locks. Stochastic routing is done with the aim that eavesdroppers do not easily find predictable paths, so the selection of hops is determined randomly by using a metric hop count, but the research is still based on a conventional network.

This thesis obtained a simulation based on SD-QKDN with the results of testing the use of keys based on the results of path selection, the routing scheme performance, and the processing time carried out on the distance vector and link state routing schemes obtained from an average of ten trials.

1.2 Problem Identification

Based on the background of this thesis, the following are some of the problems that can be identified:

1. How to test the path selection of the distance vector and link state routing schemes on the SD-QKDN.
2. How to test distance vector and link state routing schemes performance in SD-QKDN.
3. How to test the processing time of the distance vector and link state routing schemes.

1.3 Objective

The objectives obtained from this thesis are as follows:

1. Knowing path selection of the distance vector and link state routing schemes on the SD-QKDN.
2. Knowing the results of testing the distance vector and link state on the routing scheme performance.
3. Knowing processing time on the distance vector and link state routing schemes.

1.4 Scope Limitations

The problems that have been described in this thesis are limited by several things, as follows:

1. This thesis was conducted in a simulation using Ubuntu desktop 16.04 LTS.
2. This thesis focuses on discussing how distance vector and link state routing scheme performance work.
3. The routing protocol for distance vector is the routing information protocol (RIP), and the link state is an open shortest path first (OSPF).

1.5 Hypotesis

The link state routing scheme has advantages, such as cost-based path selection, where the data is arranged according to research needs. Still, the best path produced has more estimated path selection time than the routing distance vector. The distance vector routing scheme can choose a path based on the minimum hop count, so the estimated path selection time is unlike link state routing.

1. The routing scheme is adapted to the characteristics of the SD-QKDN, such as selecting the best path based on a predetermined matrix based on the test scenario. Both of these routing schemes have a goal, such as selecting paths that will reduce the use of excess keys because the use of keys is based on the results of the key generation process.
2. The minimum number of hops can also reduce the use of keys in the path selection process and have a faster time. The path selection process considers the transmission process currently running on that route.

1.6 Contribution

This thesis focuses on the routing scheme distance vector and link state performance, which are simulated on SDN-based using the OpenDaylight controller for QKD networks.

1. Evaluating routing scheme distance vector and link state performance on SD-QKDN.
2. Simulating the routing scheme based on the SD-QKDN can optimize the use of quantum keys.

1.7 Research Methodology

This thesis is divided into four work packages to produce high-quality results.

1. **Study of literature:** Search for information related to this thesis sourced from books, journals, and discussions to support the completion of this thesis.
2. **System design:** System design using Ubuntu Desktop 16.04 LTS.
3. **System analysis:** Observing the system testing results according to the scenarios and parameters, concluding the problems in this thesis.
4. **Conclusion:** Of all the steps done above with input from the supervising lecturer, conclusions can be drawn from the results that have been carried out.