PBRU SCIENCE JOURNAL
2023.20(1) : 97-110

Simulating Network Management System for Quantum Key Distribution Based on Rural and Remote Broadband in Thailand

Piya Techateerawat

Department of Electrical and Computer Engineering Faculty of Engineering, Thammasat University Khlongluang, Pathumthani, Thailand

***Corresponding author; E-mail:** tpiya@engr.tu.ac.th

Received: 14 November 2022 /Revised: 10 January 2023 /Accepted: 11 January 2023

Abstract

Quantum Key Distribution (QKD) is developed to improve the security network in key exchange field. There is several success network equipment in implement QKD. However, the key distribution is limited to use in point-to-point scope. In this paper, a network in quantum cryptography network is simulated based on actual Thailand broadband services that will extend the ability of number of users in present quantum cryptography network from point-to-point to multi-user network and sustain the security of the network. The developed system is implemented based on the existing quantum cryptography by managing the pairs joining of QKD system and real data of last-mile infrastructure and services of rural and remote broadband development in Thailand. The result of simulation is proven the feasibility to implement the proposed concept in real implementation.

Keywords: Quantum Key Distribution, QKD, Network Management, Network Management Simulation, Cryptography and Security, Thailand broadband.

Introduction

The key distribution is an initial step in several security protocols that provide the key to the specific host securely. Currently, cryptography is used to assure the confidentiality and integrity of key distribution. Therefore, all key distribution is based on mathematical cryptography[1]. However, there is a proposed alternative key distribution by using quantum cryptography. This can ensure the confidentiality in transmitted key by relying on the properties of quantum. Since quantum information cannot be sniffed nor recreated, key distribution adapted this feature to develop Quantum Key Distribution (QKD)[2,3]

The quantum communication network system's channel is divided into two channels:

the public channel and the quantum channel. The public channel is used to exchange the encrypted data, and the quantum channel is used to transmit the keys, or QKD, as shown in Figure 1. The limitation of QKD is strictly transferred only two nodes or point-to-point connection. Currently, there is research that offers several methods but mainly focuses on the physical layer, for example, a quantum router, which can route the quantum signal but has challenges with data loss, connectivity, and distance.[4, 5]

Hence, our objective is to develop a network management system for QKD based on the actual infrastructure that provides the extended ability of using QKD as a network as well as convenient management and relatively low cost.

Background

a) Quantum Cryptography

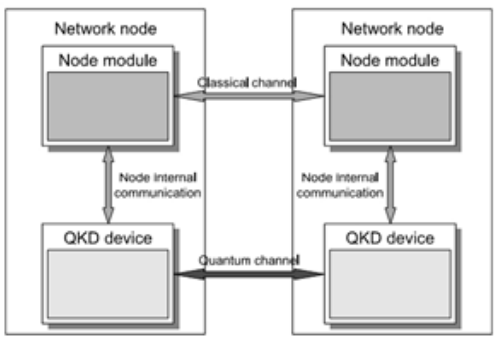


Figure 1. Data Communication in QKD System.

Quantum cryptography contains a key distribution system that uses the laws of quantum mechanics to guarantee secure communication. The crucial element of quantum mechanics, such as Heisenberg's uncertainty principle prevents anyone from directly measuring the bit value without introducing errors that can be detected. A single photon is indivisible which means that an eavesdropper cannot split the quantum signal to make measurements covertly. Quantum cryptography has a quantum no-cloning theory. This theory shows that it is not possible to receive a single photon and duplicate the photon without giving notice to others. There are two dominant schemes for quantum key distribution protocols which are the BB84 protocol and the B92 protocol[6-8].

BB84 protocol is the first quantum cryptography protocol which was proposed by Bennett and Brassard in 1984 [2]. This protocol employs two polarization bases for a single photon; rectilinear basis and diagonal basis. The single photon may be polarized in four states: horizontal |h>, vertical |v>, left circle polarized |lcp>, and right circle polarized |rcp>. Polarization state horizontal |h> and left circle polarized |lcp> represent a '0'. The polarization states of vertical |v> and right circle polarized |rcp> represent a '1'.

B92protocol is proposed by Bennett and Brassard in 1992 [9], similar to BB84 protocol but uses only two non-orthogonal quantum state |h>

represent a '0' and |rcp> represent a '1', half of the BB84 protocol to transmit the key.

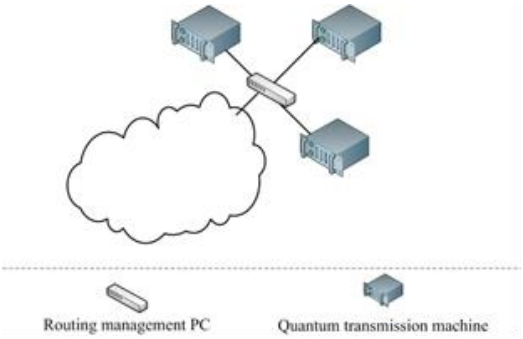
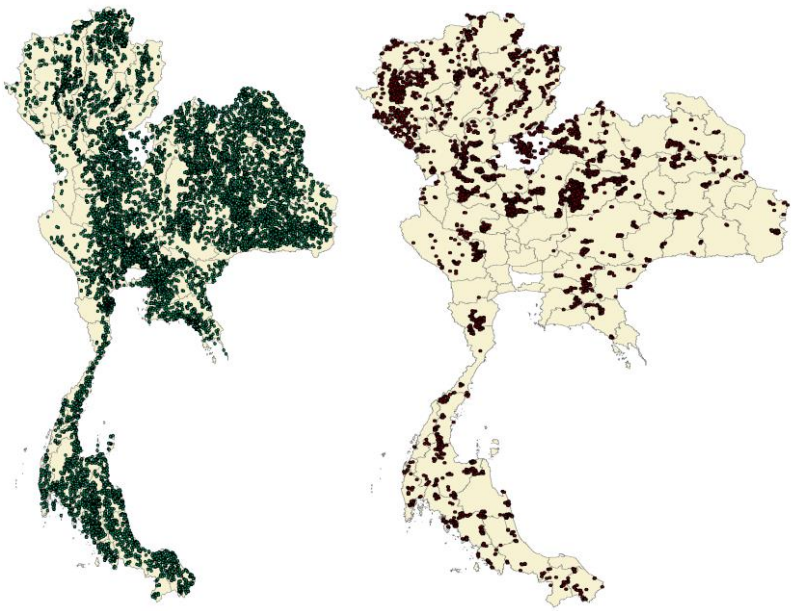


Figure 2. System Design

b) Rural and remote broadband in Thailand

In this paper, simulation is based on the real infrastructure of rural broadband in Thailand providing last-mile technologies for 15,732 rural villages (Zone C) and 3,920 remote villages (Zone C+) implemented by National Broadcasting and Telecommunications Commission (NBTC). This paper illustrates new tailored last-mile technologies that are suitable for these types of areas. The technologies are aimed to be the base on which to construct a regional system for distribution of broadband accesses at 15,732 rural villages and broadband/mobile accesses at 3,920 remote sites locating around the country as shown in Figure 3. It is noted that Ministry of Digital Economy and Society (MDES) is responsible for the broadband implementation of remaining rural villages (24,700 rural villages).

The broadband data presented in this paper is the last-mile implementation for the 3,920 remote villages in Thailand served by NBTC. This broadband development and implementation are to: 1) provide high-speed broadband internet services in the areas; 2) extend infrastructures and services to the areas so that remote people will have equal access to digital technology and information; 3) create the so-called "digital economy and society" in the areas; and 4) leverage digital technologies and services for the areas. The 3,920 remote villages implemented are in all remote areas of Thailand, as shown in Figure 3. Most of them are in the north of Thailand, a mountainous area where there are parallel high mountains with steep river valleys and high-hill areas that surround the central plain. While the 15,732 rural villages (details are shown in Table 1) are more widely distributed nationwide and most of them are easier to access compared to the remote areas, However, approximately 20–30% of the areas have the same constraints as the remote.



Zone C Zone C+

Figure 3. Broadband infrastructure (color dots): rural villages (Zone C) and remote villages (Zone C+)

Table 1. Descriptive Information of the rural villages in Thailand (Archived from NBTC survey information)

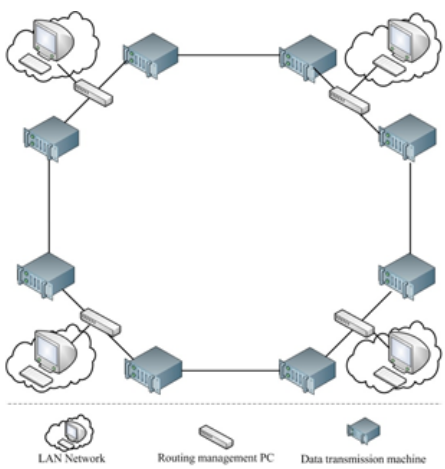
Area: Zone C	Targeted villages	Approximate population	Average population per village	no. of Teachers	no. of Students
North	4,140	2,460,432	594	19,716	241,340
South	2,052	1,713,722	835	14,288	182,610
Central and East	3,367	2,202,084	654	18,489	239,028
North-East	6,173	3,823,091	619	29,559	392,074
Total	15,732	10,199,329	648	82,052	1,055,052
North	2,027	868,041	428	11,351	148,760
South	459	239,526	522	2,757	33,919
Central and East	349	182,122	522	1,755	27,237
North-East	1,085	534,209	492	5,120	66,473
Total	3,920	1,823,898	465	20,983	276,389

Management system for quantum distribution (QKD)

Our system is designed at application layer to support connectivity, convenience, and cost. We assume that each QKD machine is a trusted host and our system has physical protection from anonymous which is based on structured network[10,11]. Quantum transmission machine uses BB84 for default protocol.

A. Hardware

From the physical connection, there are 3 main parts: 1.) Group of Network; 2.) Routing Management PC; 3.) Data Transmission Machine, as shown in Figure 2. In our system, we use encryption hardware and a quantum key distribution hardware, so each group of networks is connected to Routing Management PC then connected to Data Transmission Machine as shown in the Figure 4. For packet routing part, we design and develop our system by using open-source software and necessary library and install to Routing Management PC.



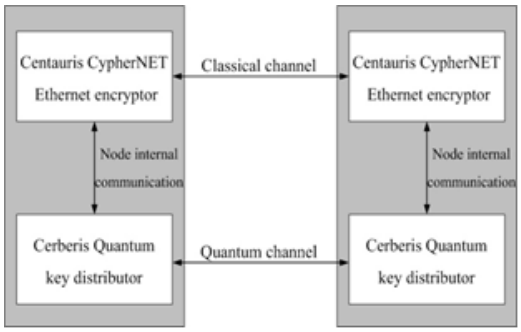


Figure 4. Network Connectivity in Testing & Structure of Data Transmission path.

B. Software

In our system, management software is deployed on Routing Management PC. The routing decision software is developed on Linux Ubuntu 9.04, Netbeans IDE 6.7.1, JNetPCap library and iproute2.

There are two main parts of the control software: 1.) Path selection software; 2.) routing software the path selection software is the first part where packets are filtered. It screens only secured packets are travelled through the QKD system and also verifies that secured packets are passed from the appropriated interface. The key method is to split secured packets to the QKD system and let the non-secure packets go to the general network, as shown in Figure 6. The routing software is the inner part of the QKD system. This is involved only selected secured packets which travelled in QKD system. The main

operation is to route secured packets and manage the queue and buffer.

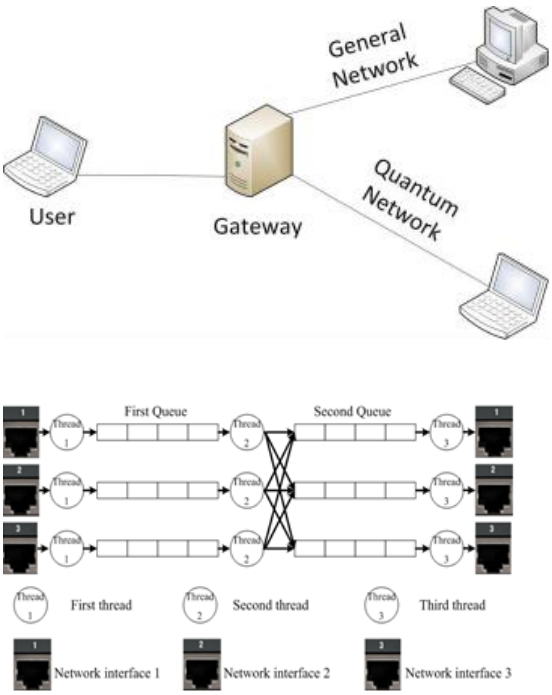


Figure 5 Packet Screening for QKD System & Queuing and Buffer System.

C. Operation

The operation of system on Routing Management PC is filtering and routing packet to the appropriated destination. In the system, each job is separated into threads. In each thread, queues are created to support storing and queuing with First-in First-out System (FIFO) as shown in figure 6 and the pseudo code is shown in figure 7.

This system requires the packet to encapsulate with a new header for two main benefits in our QKD system. The first benefit is to use this new header for support our QKD network, routing can redirect quicker in our designated network. The second benefit is to guarantee that the secured packets are only travelled in our secured QKD network.

Queues are created to support each interface separately. There are two parts of queue in our system and each queue has its own duty. The first queue is the buffer for receiving packets. The second queue is the buffer for sending packets.

The thread of the management system is separated into three parts based on the job. The first thread handles incoming packets from its own interface and puts captured packets into the first queue. The second thread removes packets from the first queue, finds their destination, and then replaces the Ethernet header with an appropriate header and inserts the modified packet into the second queue. The third thread removes packets from the second queue and transmits the packets to the corresponding interface.

Broadband Implementation and services

For the remote villages, most of the villages are on the mountains or surrounded by mountains. From Table 1, there are approximately the total of 1,823,898 populations with the average of 465 people per village. Household locations are scattered and unevenly. Some of them can be found as a group of 20 to 30 average households. In the rural area, as shown in Table 1, there are approximately 10,199,329 populations, with an average of 648 people per village. In summary, the remote villages are the areas with very low density, while the rural villages are the areas with sparse residential density, as shown in figures 7 and 8, respectively. In the last mile of implementation for both types of areas, descriptive rural and remote locations can have a relatively higher total cost of ownership in terms of transportation and maintenance, including labour and construction costs, even though prices for hardware and software are dropping.

Figure 7. A remote village in the north of Thailand

Non-availability of reliable power supply

The reliable grid power supply in Thailand has not been developed as fast as the spread of telecommunication and broadband infrastructure, especially in the remote areas. About 5-10% of the 3,920 villages do not have any electricity or do have insufficient power source. In this case, optional power supply such as solar power is considered to be a self-sustainable and capable power to broadband and mobile equipment. Nonetheless, according to our survey information, there is only 1-2% of the rural area with such power constraints.

Infrastructure issues

As seen, the growth of broadband penetration in remote areas is one of the challenges since there is insufficient infrastructure or backhaul. Implementing a broadband or

mobile infrastructure in the remote area needs more specialists and higher cost of ownership for which private network operators find it unlikely to justify the investment over that long-distance network with low population density[12]. Therefore, last-mile implementation should be reliable, affordable, scalable and financial viability. Various technologies may be suitable for last-mile broadband implementation as the backhaul in the remote areas such as fiber (Passive Optical network: GPON), satellite or microwave. Each of these technologies has its benefits and drawbacks in terms of affordability, performance and total cost of ownership (TCO). As a result, no single technology solution can fit all scenarios in remote areas. About 60% of the 3,920 villages do not have any existing internet access (no available network connectivity previously). However, according to our survey information, there are no such obstacle for most of the rural area where internet accesses thru public and/or private network providers already exist.

Broadband model in simulation

With the mentioned technical constraints in the previous section, for broadband implementation, there are two main considerations needed to find solutions for the remote area. Since in the rural area there already has been existing network infrastructure and access, the second solution is the only aware. The use of geographical distribution is derived into a development plan with clustering techniques such as K-means Clustering or Self-Organizing Map[13]. With these clustering approaches, the broadband infrastructure can divide the remote villages into several clusters in terms of infrastructure issues and a lack of knowledge. In order to achieve economic constraint, an optimal location in a cluster is determined by solving an optimization problem:

Maximize utility functions U = Sum (w*f(x)),

Subject to g(x) $\leq$ 0,

h(x) = 0, (1),

where x = considered factors shown in Table 2, g(x) is inequality constraints and h(x) is equality constraints.

Table 2. Considered factors in the optimization problem

Factors	Description
Users	Stakeholders, Gender, Age, Internet experience, Self-efficacy, Education
Physical	Location, geographic limitation, Accessibility, Landmarks) School, Temple, Hospital, etc
Social	Usages, Activities, federal, state, and local agencies
Facility	Electricity, Water, Energy
Infrastructure and Communication	Current Broadband and mobile service
Cost	Implementation and Maintenance

As a result, the broadband implementation solution provides two layers of services: 1) network infrastructure (backhaul) and 2) digital services and applications via Wi-Fi technology and a learning center. For the remote villages, first, if applicable, the fiber (Passive Optical Network: GPON) technology is exploited with an optical line termination (OLT) that is installed at the optimal location in a cluster as shown in Figure 8. There are a total of 881 OLTs to support 4,760 services (customer-premises equipment (CPE) or optical network units (ONUs)) in the 1,909 remote villages (previously, there was no existing internet infrastructure). This technology can support high-speed internet access with more than 30/10 Mbps data rate (download/upload) per service point (ONU). In case of geographic limitation over too long distance for the fiber technology in terms of technical and cost limitations, the broadband satellite capacity can be exploited to provide an internet backhaul for broadband services with more than 30/5 Mbps data rate (Download/Upload) per a service point (CPE) at remote sites.

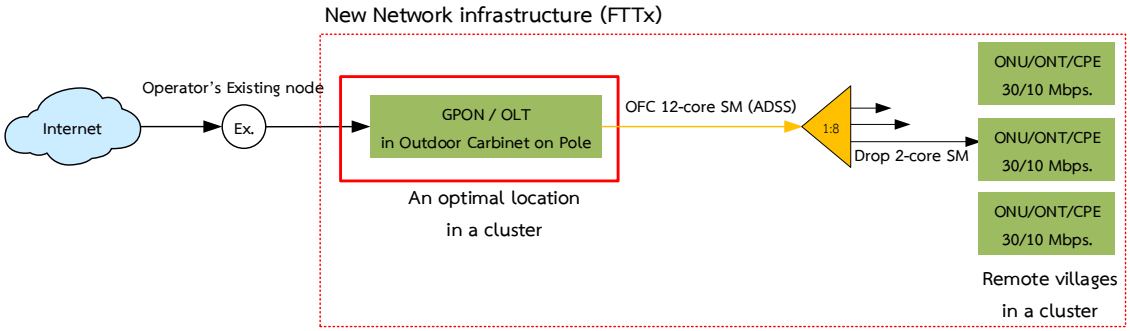


Figure 8. GPON network infrastructure (backhaul)

Discussion

The simulation is to verify the concept algorithm from three main perspectives: 1.) Data Transmission: To verify an end-to-end connection is feasible for the actual implementation. 2.) Security: to verify that system does not expose the information to the outside network. 3.) Performance: to compare with general Ethernet network in high and low traffic scenarios.

```
Construct Thread1, Thread2, Thread3
Construct Queue1[ ], Queue2[ ]
 THREAD1( )
  int_Name ← get available interface number
  Pkt_cap ← capture packets from int_Name
  Insert pkt_cap to Queue1[int_Name]
   THREAD2( )
REPEAT WHILE true
  IF Queue1 is not empty
    THEN
    Pkt_Queue1 ← packet removed from Queue1
    Proper_Int ← find proper interface for send
                 packet from Queue1
    pkt_Edited ← replace a new Ethernet header
                 of pkt_Queue1
    put pkt_Edited into Queue2[Proper_Int]
  ENDIF
END REPEAT
THREAD3( )
  REPEAT WHILE true
    IF Queue2 is not null
      THEN IF Queue2 is not empty
                THEN
                  Remove packet from Queue2
                  Send the packet off
              ENDIF
    ENDIF
END REPEAT
```

Figure 9. Algorithm of Queuing System for QKD system

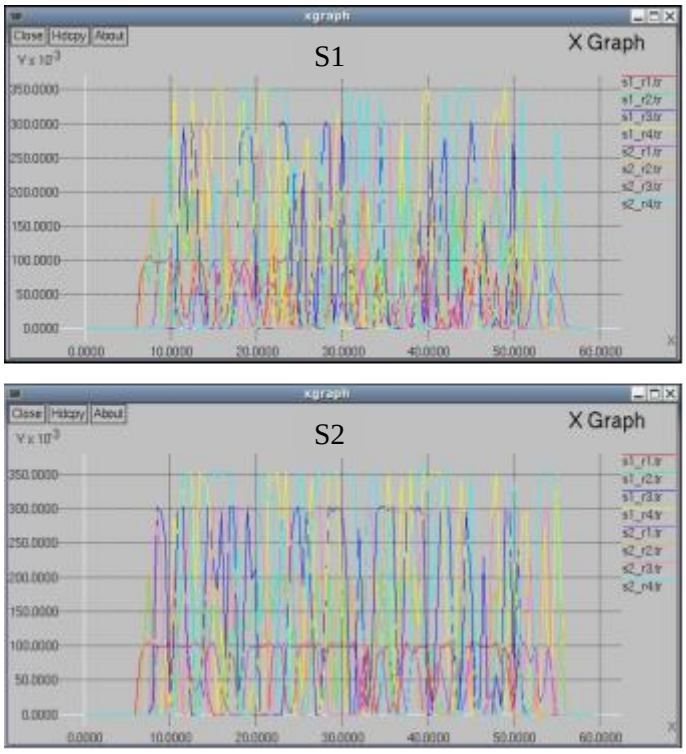


Figure 10. Graphs show a comparison of network throughput between the QKD system (s1) and normal traffic (s2) in high traffic situation

A. Data Transmission

The result from the system is shown that all connected QKD system is able to exchange the data in the shortest path appropriately. The queue is required to be prepared on a large scale in case high traffic is generated; otherwise, it may cause packet loss. During the simulation on a large scale, at least 100 MB is recommended for a buffer in case high traffic occurs.

B. Security

Key is relied on QKD system which is distributed by Quantum channel so sniffer cannot trap the distributed key. In the case that the sniffer traps the key, the QKD system is detected, and the key is ignored and resent. If the attacker attempts to trap and recreate the key, QKD can detect this key as an error because of the quantum property in BB84. Therefore, the key transmission can be trusted with the system. However, the transmission and queuing system is required to be trusted; otherwise, it can be manipulated or attacked by the intruder.

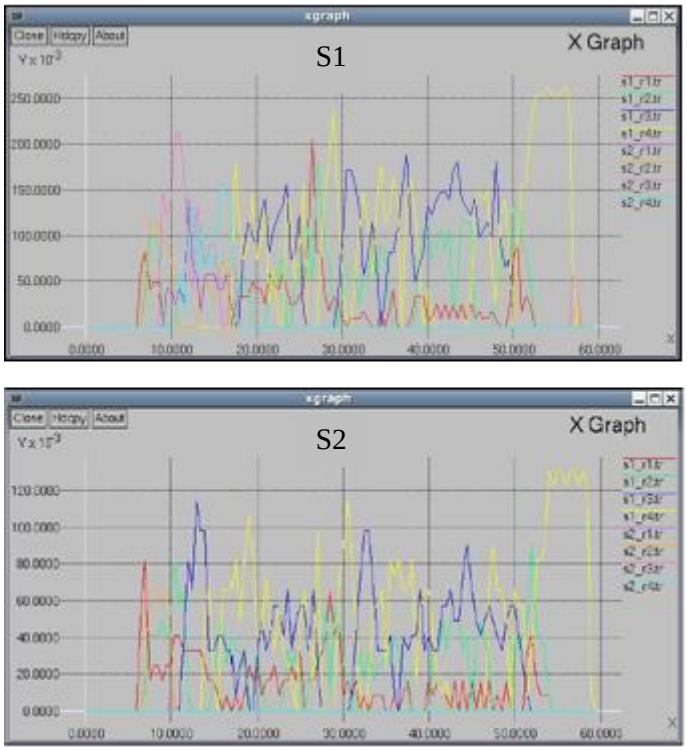


Figure 11. The comparison of network throughput between QKD system (s1) and normal traffic (s2) in low traffic situation

C. Performance

We compare the general network using Ethernet LAN and our QKD system by using NS-2 simulation. The simulation uses the actual delay and behaviour that has been recorded from the real hardware (Ceberis) as well as the packet encrypter (Centauris CypherNet).

Figure 10 shows the comparison of network throughput between QKD system (s1) and normal LAN (s2) in high traffic situation. The raw data result shows that QKD system has lower throughput than general normal network approximately 12%. This is caused by the delay of key distribution and packet application (e.g., video conference), which impacts to the total time of large file transfers (e.g., 4 GB file size). As a result, a complex network structure with high traffic may need an improved concept of QKD system.

Figure 11 shows the comparison of network throughput between QKD system (s1) and Ethernet LAN (s2) in low traffic situation. The raw data result shows that QKD system does not has lower throughput than general

normal network on average. As a result, the QKD system with mixed contents in low volume does not impact the throughput performance when compared with normal network. Therefore, as a secure channel with low volume, QKD system has a sufficient performance to operate.

Conclusion

In this article, we propose a network management system for QKD. This system is using the high security of a point-to-point quantum channel to connect a network based on actual broadband infrastructure in Thailand. The objective of the system is to provide connectivity, convenience, and low cost at the application level.

Since the quantum protocol can provide the strong security shown in BB84 and B92, key distribution is used in this secured channel. Quantum cryptography can provide the feature that guarantees no sniffer. Once the sniffer traps the quantum message, the QKD system can be detected. Also, the recreated or cloned quantum message is infeasible with current technology. Then, quantum channel provides the strong security for our QKD system.

Our QKD system is designed by using routing management PC and data transmission machine. The design is based on the assumption that quantum channels are trusted hosts and physical protection is provided for the machine. These two devices are designed to connect the quantum channel as a network as well as filter and routing packet.

The simulation in our system uses the actual data from Ceberis and Centauris CypherNet and actual infrastructure of Thailand's broadband infrastructure. The result shows that QKD system provides connectivity, security and performance in low volume scenarios. However, during the high traffic is generated the delay from encrypter and key distribution is impacted the result by approximately 12% compared to normal network and recommend at least 100 MB channel for QKD system. Therefore, QKD system is acceptable and feasible in secure network for low volume from our simulation. In case of high usage, the results are recommended for at least 100 MB bandwidth channel for QKD specifically.

Acknowledgment

For this paper, we would like to thank faculty of Engineering Thammasat University, Thammasat University.

This research was based on by the National Broadcasting and Telecommunications Commission (NBTC) project consulted by Thammasat University. The authors gratefully acknowledge the support of NBTC. Any opinions,

findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the view of NBTC.

Reference

1. Denning DE. Cryptography and Data Security. Purdue University. USA: Addison-Wesley Publisher Company; 1945.
2. Bennett CH, Brassard G. Quantum cryptography. Public key distribution and coin tossing. Proceedings of IEEE Int. Conf. Computers, Systems, and Signal Processing; Dec 91-2, Bangalore, India; 1984. p.175-9.
3. Elliott C, Pearson D, Troxel G. Quantum cryptography in practice. Proceedings of ACM SIGCOMM 2003; Karlsruhe. Germany. Aug. 2003:227-38.
4. Norbert L. Quantum key distribution, Institute for Quantum Computing University of Waterloo:1-10.
5. Zhang T, Aheng-Fu H, Xiao-Fan M, Guang-Can-G. Extensible router for multi-user quantum key distribution network. arXiv:quant-ph/0608238 2006;1-3.
6. Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik 1927;43:172-98.
7. Eli B, Shamir A. Differential cryptanalysis of the data encryption standard. Springer Verlag; 1993.
8. Ferguson N, Schroeppel R, Whiting D. A simple algebraic representation of Rijndael. Proceedings of Selected Areas in Cryptography. Lecture Notes in Computer Science. Springer-Verlag. 2001:103-11. Simple algebraic representation of Rijndael. In Selected areas in cryptography SAC 01, LNCS 2259 (pp. 103-111)
9. Bennet H, Brassard G. Quantum cryptography using any two non-orthogonal states. Phys Rev Lett 1992;68:3121-4.
10. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum crytography. Rev Mod Phys. 2002;74:145-95
11. Steenstrup E. Routing in communications networks. Englewood. United State: Prentice Hall; 1995.
12. Hollifield A, Donnermeyer F. Creating demand: Influencing information technology diffusion in rural communities. Gov Inf Q 2003;20:135-50.
13. Kanungo T, Mount M, Netanyahu S, Piatko D, Silverman R, Wu Y. An efficient k-means clustering algorithm: analysis and implementation. IEEE Trans. Pattern Anal Mach Intell 2002;24:881-92.