Secure Data Transmission through IoT Devices using Quantum Key Distribution Protocol

Myat Su Win
Faculty of Computer Systems and Technologies
University of Computer Studies,
Mandalay, Myanmar
myatsuwin@ucsm.edu.mm

Khaing Khaing Wai
Department of Information Technology Support & Maintenance
University of Computer Studies,
Yangon, Myanmar
khaingkhaingwai@ucsy.edu.mm

Abstract- Information security is dominant in Internet-based IoT communication. Traditional cryptography relies upon mathematical models and the complication of calculations to determine the secret key. In recent years, it provides adequate security because the secret key is difficult and complex to compute. However, in today's Quantum age, private keys are easy to compute and have implications for system security. One of the most promising ways to provide unrestricted security is through Quantum Key Distribution (QKD). It uses the quantum property of information exchange, the so-called photons, as the information carrier of the security system. In this paper, we prove that the Quantum Key Distribution Protocol B92 is better suited for secure data transfer between IoT devices than other protocols like BB84 and BBM92 protocols using QuVis Simulators.

Keywords— **IoT, BB84, B92, BBM92, QuVis**

I. Introduction

The most important thing in Internet-based communication is information security. Internet of Things (IoT) devices have evolved into embedded systems and sensors that can connect, collect, and transmit data over the Internet. Classical cryptography relies on mathematics, and it is difficult to calculate a large number of factors [1]. The security of traditional cryptography relies on the high complication of mathematical difficulties such as the factorization of large numbers. Achieving confidentiality of information is very important in communication from the sender to the receiver. The secure data transfer takes place between them using encryption and decryption algorithms. Therefore, unauthorized persons cannot access the message, called cryptography [2]. Sending a message means that the sender and receiver are Alice and Bob, and the spy (eavesdropper) is Eve. To protect the information, encrypt the message before sending it to the receiver using a private key known to Alice and Bob involved in the communication [3]. There is no way to guarantee that key exchanges are completely secure. To overcome this problem, quantum mechanics is a way to guarantee key distribution.

II. Quantum Key Distribution

When distributing a key from a transmitter to a receiver, quantum computation creates the photon stream with four different horizontal and vertical spins, a diagonal of 45° and a diagonal of -45°, with a property called 'spin'. The horizontal direction and 45° act for the binary value **1**, and the vertical direction and -45° act for the binary value **0** respectively [4]. Fig. 1 below represents the key distribution process.

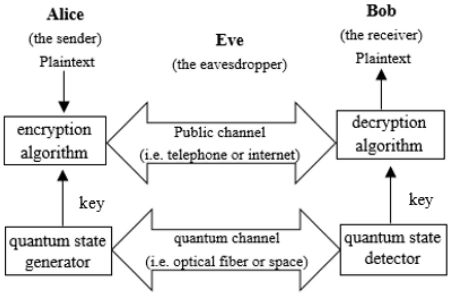


Fig. 1. Quantum Key Distribution

III. The IoT Network with B92 Protocol

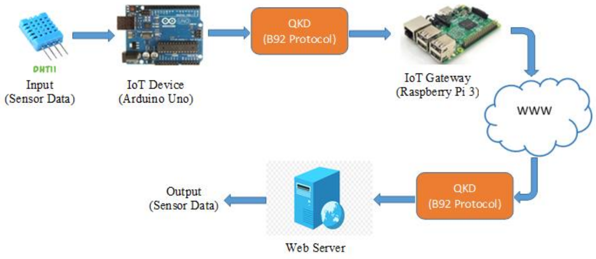
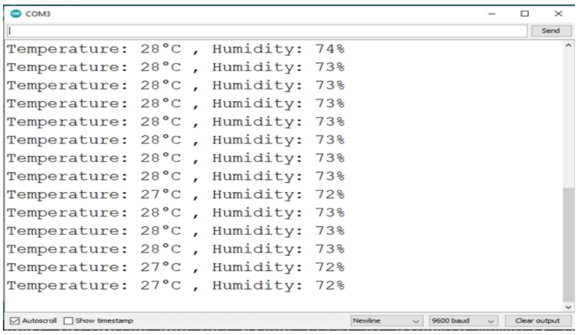


Fig. 2. Overview of the IoT network

Fig.2. represents the IoT network overview and there are two main, sending and receiving, sides. On the sending side, the IoT device accepts the sensor data and before sending the data to the IoT gateway, QKD produces the secret key that key used to encrypt the sensor data with the classical encryption method and then sends data to the IoT gateway and it sends over the Internet. On the receiving side, use the same secret key to decrypt data and send it to the server. Finally, the server shows the output of the original data. The following Fig.3. represents the sensor data output from the Arduino.



```
Temperature: 28°C , Humidity: 74%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 27°C , Humidity: 72%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 28°C , Humidity: 73%
Temperature: 27°C , Humidity: 72%
Temperature: 27°C , Humidity: 72%
```

Fig. 3. Sensor Data Output from Arduino

IV. Experimental Result

By using the QuVis simulator for test results. As part of QKD, the simulated environment consists of their three protocols, adding Eve as a spy to enhance the experience. We evaluated the BB84, B92, and BBM92 protocols' error comparison.

Alice (sender) and Bob (receiver) transmit photon polarization in each test using a random reference. Eve, the eavesdropper between Alice and Bob uses a random basis to transform the sender's basis into the receiver's basis. Send polarized photons to Bob using the 100-photon fast-forward option. In this test, we will send 4000 photons and compare the error probability ratio for each photon.

A. *Test Results for BB84 Protocol*

Fig. 4., represents the 40 testing results of the protocol. The probability error key is generated from the number of keys (N_{key}) and the number of key errors (N_{err}), the formula is:

$$P = N_{err}/N_{key} \tag{1}$$

Bob's filterable probability error key result does not surpass 0.5 (N_{tot}), the supported limit for the QuVis simulator to accurately deliver the BB84 protocol hypothesis.

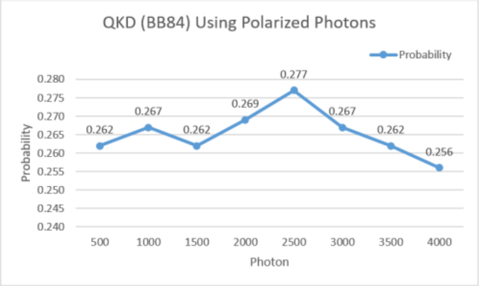


Fig. 4. Testing Result of BB84 Protocol (QuVis)

B. *Test Results for B92 Protocol*

Fig. 5., represents the 40 testing results of the protocol. The probability error keys are generated from the number of keys (**N_{key}**), and the number of key errors (**N_{err}**). Bob's filterable probability error key result does not exceed the supported limit of 0.25 (N_{tot}) for the QuVis simulator to provide an accurate hypothesis of the B92 protocol.

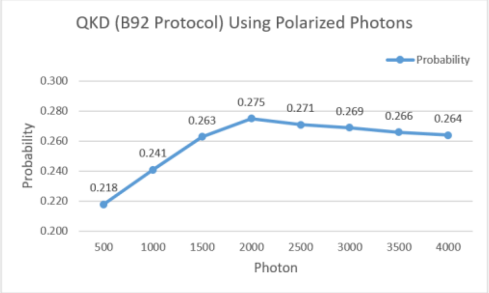


Fig. 5. Testing Result of B92 Protocol (QuVis)

C. *Test Results for BBM92 Protocol*

Test results for 40 experiments are represented in Fig. 6. The probability error key is calculated from the number of keys (**N_{key}**), and the number of key errors (**N_{err}**). Bob's filterable probabilistic error key results do not surpass the limit of 0.5 (**N_{tot}**) supported by the QuVis simulator to accurately provide the BBM92 protocol hypothesis.

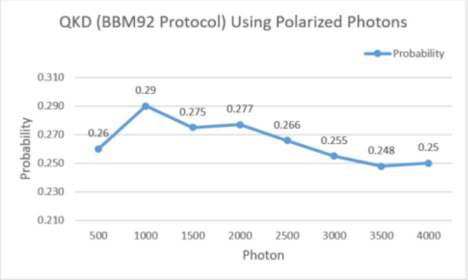


Fig. 6. Testing Result of BBM92 Protocol (QuVis)

D. *Comparative Probable Error Rates*

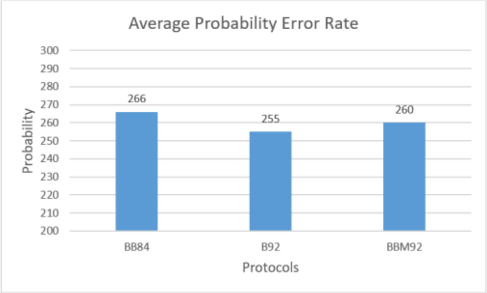


Fig. 7. Comparative Probable Error Rates of (BB84, B92, BBM92)

Fig.7. shows the average error probabilities for the BB84 protocol, the B92 protocol, and the BBM92 protocol. The results indicate that the B92 protocol has the smallest probability key error values than the BB84 and BBM92 protocols.

V. Conclusion And Future Work

We use the QKD QuVis simulation software to compare probabilities for the BB84 protocol, the B92 protocol, and the BBM92 protocol. The results indicate that the B92 protocol has the smallest probability of key failure compared to the BB84 and BBM92 protocols.

Test results indicate that the B92 protocol has a lower error rate than the other two protocols and is suitable for eavesdropping detection. Therefore, the B92 protocol is better suited for secure data transfer between IoT devices than other protocols such as the BB84 and BBM92 protocols.

In future research, we plan to implement an IoT network and use the B92 protocol for secure data transmission over the Internet.

References

[1] Hitesh Singh, D.L. Gupta, A.K Singh, "Quantum Key Distribution Protocols: A Review," Computer Engineering Journal (IOSR-JCE) 2014.

[2] Jian Zhang, Liangyi Gong, Tsinghua University, "The Current Research of IoT Security," 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC).

[3] Mhlambululi Mafu and Makhamisa Senekane, "Security of Quantum Key Distribution Protocols", Published May 30th, 2018.

[4] Brahim Ouchao, Abdeslam Jakimi, "Performance Evaluation of Secure Key Distribution Based on the B92 Protocol", International Journal of Advanced Engineering Manangement and Science (IJAEMS), vol. 4, issue. 6, 2018.