IMPLEMENTATION OF BB84 PROTOCOL ON UDP 802.11i

[1]NUR HANANI KAMARUL AIZAN, [2]ZURIATI AHMAD ZUKARNAIN, [3]HISHAMUDDIN ZAINUDDIN
[1]M.Sc, Faculty of Computer Science and Information Tech., University Putra Malaysia (UPM).
[2]Senior Lecturer, Department of Computer Networks, Faculty of Computer Science, UPM, Malaysia.
[3]Assoc. Prof., Institute for Mathematical Research, University Putra Malaysia (UPM), Malaysia.
E-mail: nur_hani10@yahoo.com[1], zuriati@fsktm.upm.edu.my[2], hisham@fsas.upm.edu.my[3]

ABSTRACT

Cryptography nowadays is looking for a secure and trusted channel especially in key distribution between two legitimate parties without being intercepted or decipher by intruders either in wireless or wired communication medium. The invention of Quantum Cryptography as part of quantum mechanics has solves the key distribution's problem in cryptosystem by providing a secure communication channel between two parties with absolute security guaranteed by the laws of physics. Quantum Key Distribution (QKD) as a new method in key distribution used to transmit secret key between two legitimate parties. This paper will discuss the implementation of BB84 protocol in UDP 802.11i Wireless Local Area Network (WLAN). WLAN as a wireless links are much noisier and less reliable in general than wired links. This type of noise will generate different numbers of key length and also different level of error rate estimation.

Keywords: *Quantum Key Distribution (QKD), Wireless Local Area Network (WLAN), User Datagram Protocol (UDP), 802.11i.*

1. INTRODUCTION

This paper carried out the research in the implementation of BB84 protocol on UDP 802.11i Wireless Local Area Network (WLAN). The objective of this work is to measure the error rate and key length in wireless environment. QKD is a solution for the classical cryptography such as DES, AES, RSA etc. It is inevitable to be cracked just in an hour by using high powerful computing [1].

The most important problem in cryptography is security and authenticity of the message send between sender and receiver. Assume that two parties which Alice and Bob are willing to communicate over insecure (public) channel to share a secret key. The potential of eavesdropper or intruder to gain the secret key is high. Thus, Quantum Key Distribution (QKD) has provided a secure channel for Alice and Bob to exchange the secret key instead of public channel. The security of QKD is guaranteed by the principle of quantum mechanics where conventional scheme of key distribution does not guarantee the secrecy of the key.

2. RELATED WORK

The related works contain of three parts. The first part explains about the wireless security, followed by User Datagram Protocol (UDP) and BB84 protocol.

2.1 Wireless Security

A. 802.11i and Quantum Cryptography

The growth of wireless devices is increasingly developed. However the constraint in wireless environment is the complexity of data processing such as that required by new and robust security protocols. The security methods become available and weaknesses become apparent. Thus, it is necessitates to have a better system to adapt to counteract security weaknesses and also provide security for users in securing their data.

IEEE 802.11i is optional amendments to IEEE 802.11 standard protocol which offer enhance security at the medium access control (MAC) layer [6]. This protocol is intended to overcome the weaknesses of previous security schemes. The wired equivalent privacy (WEP) security scheme defined in the IEEE 802.11b has been replaced by Wi-Fi protected access (WPA) which provides the temporal key integrity protocol (TKIP). This new security scheme requires the clients and access points must query an authentication server. WEP has been shown to be a weak security protocol with many flaws as follows:

- WEP uses only one secret key for both authentication and encryption. Once the security is discovered, the authentication key also will be discovered. Thus, this is not a good security strategy [5].

- RC4 stream cipher algorithm in WEP has a set of weak keys and becomes vulnerable if one part of the key is disclosed to attackers. RC4 key is concatenation of an Initialization Vector (IV) of 24 bits which is sent in plain text together with the encrypted frame. Because of IV is directly used as a part of RC4 key, passive attacks can be easily disclosure the WEP key [5].
- WEP not avoid repeated IV during the use of a given secret key**.** This will give the opportunity for attacker to gain knowledge of the key due to slow bit rate in 802.11b protocol with 11Mb/s. It requires a renewal of secret key every 8 hours which is impossible in WEP because it does not define any mechanism to establish new secret key between mobile device and access point [5].
- The implementation of CRC-32 in WEP to provide authentication seems not a good message integrity protection algorithm [5].

B. 802.11i key management

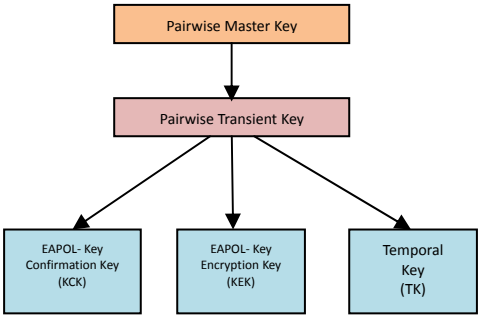


Figure 1: *Pairwise key hierarchy*

In 802.11i has many keys at different levels, which becoming a hierarchy as shown in Fig. 1 [5],[8]. Pairwise master key located at the top level which is used to derive the other keys.

While, at the second level in the hierarchy is a pairwise transient key (PTK). It is created between the access point and the mobile terminal during the connection establishment.

Furthermore, PTK is split into three final temporal keys know as key confirmation key (KCK), key encryption key (KEK) and temporal key (TK) [5],[8].

C. Quantum Cryptography – QKD

Quantum cryptography or quantum key distribution (QKD) is a new method for key distribution to solve the flaws in the conventional cryptography. This method utilizes the principle of quantum mechanics to guarantee secure communication. It enables two legitimate parties shared a random secret key which only known to them to encrypt and decrypt the message [2].

The unique property in quantum cryptography is the ability to detect the presence of Eavesdropper or any third party that trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics, where the process of measuring a quantum system in general disturbs the system. If a third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies.

By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. The communication is aborted and no secret key can be produced when the level of eavesdropping has reach or higher the certain threshold, otherwise if the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure[5].

Quantum cryptography is used to produce and distribute the key and not to use in transmitting any message data. The produced key can be used with any chosen symmetric classical cryptography to encrypt and decrypt the message, which can be transmitted over a standard communication channel which called as public channel.

While, in free space QKD uses the air as the medium in transmit the photons or bits between sender and receiver. The feasibility of QKD over the air is considered problematic because of unreliable medium and high error rate. For the limited distance and indoor environment, the quantum channel would be realized at the reasonable level.

2.1 User Datagram Protocol (UDP)

This project has implemented QKD on UDP protocol which are connectionless and unreliable transport protocol. The two ports serve to identify the end points within the Alice and Bob as a sender and receiver and no formal handshaking is required for connection establishment and it is what we call as connectionless.

User Datagram Protocol is used, in place of TCP, when a reliable delivery is not required. UDP does not maintain connection state includes receive and send buffers, congestion control parameters, and sequence and acknowledgment number parameters.

Thus, for this reason, a server devoted to a particular application can typically support many more active clients when the application runs over UDP rather than TCP. This will give a good affect to the process of QKD in getting the secret key, where the communication is still in process and continue even if some of the segment had lost that may cause of the interruption by Eavesdropper or noise during the communication

occurs.

UDP packet's called as user datagram with 8 bytes header. A format of user datagram is shown in Fig. 2[11]. In the user datagram first 8 bytes contains header information and the remaining byte contains data.

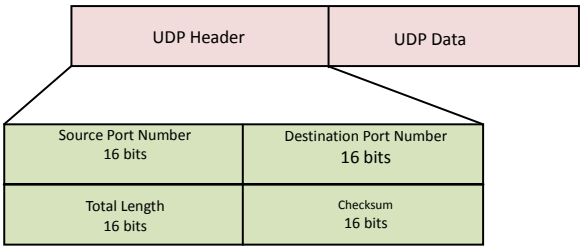


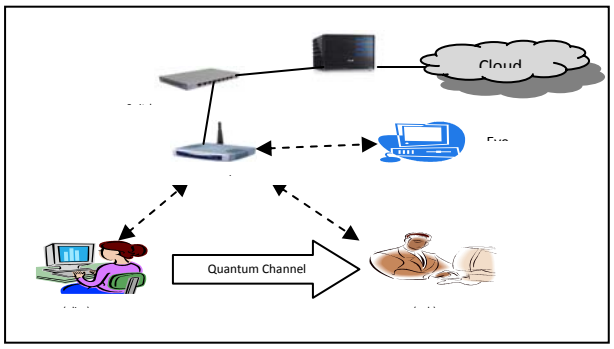
Figure 2: *UDP segment structure*

2.2 BB84

BB84 is one of the QKD protocols which is implemented in this study, is the first protocol that invented by Charles H. Bennett and Gilles Brassard in 1984, was originally described using photon polarization states to transmit the Information. In 1994, this protocol has been experimented and proved by Dominic Mayers, Eli Biham and Michael Ben-Or [3,4] where it is secure against eavesdropping.

BB84 protocol coding scheme uses four non-orthogonal polarization states (0º, 90º, 45º and - 45º). In this protocol Alice (sender) and Bob (receiver) have to communicate in two types of channel, Quantum Channel (eg. fiber optic or free space) and Public Channel (eg. Internet).

The quantum key distribution happens in two stages as illustrated in Fig. 3:



1) Via Quantum Channel (one way communication)

Step 1: Alice randomly chooses polarize photon (measure as bit) to generate photons and send them to Bob using Quantum Channel.

Step 2: Bob receives those photons with randomly chosen polarizes either to use diagonal or rectilinear basis.

2) Via Public Channel (two way communication)

Step 1: Alice will use public channel to tell Bob the polarization she choose for every bit she sent without disclosing the bit value she sent.

Step 2: Bob will compare the list of polarization he got from Alice with the one he generated when receiving.

Step 3: The union of these list can be used as their raw key, which is considered not fully secret, bits maybe tampered by Eve during the transmission.

Step 4: This communication is still continue in public channel and can be divided further in 4 main phases as below in order to obtain the correct key:

- Sifting Raw Key
- Error Estimation
- Error Correction
- Privacy Amplification

3. THE IMPLEMENTATION OF BB84

A. Software Structure

For the implementation of BB84, the software has been developed using JAVA language which run on UNIX environment. This software make available for Alice and Bob communicate with or without Eve attacks.

Based on physical implementation of BB84 [9], this software is working in two channel, which are quantum channel and public channel. Alice as a sender, Bob as a receiver and Eve as eavesdropper will play their own roles in this implementation. The software consists of five objects, Alice, Bob, Eve, Quantum Channel and public Channel. Alice, Bob and Eve will run in separated machine. In Quantum Channel, if there is an eavesdropper tap the communication, the bit will be changed. While in public channel, it is use for Alice and Bob communicate for error detection of bit and make the correction for the error bits. During this phase, Eve can only observe but cannot make any modification on bits.

B. Hardware structure

The implementation in hardware structure of BB84 in wireless environment can be illustrated as in the Fig. 3. All devices are setup in the same room. Switch is use to connect to the access points and all the workstations are connected to access point. Each workstation represents Alice, Bob and Eve respectively. Static IP are used to ensure all the workstation can communicate via the access point. Therefore, Eve will recognize Alice and Bob by their IP addresses. Developed software is installed on each of workstations to run the protocol.

Figure 3: *Hardware implementation*

C. The protocol

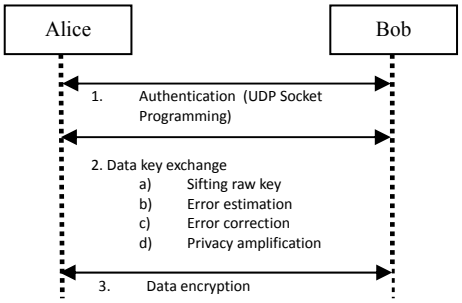


Figure 4: *The protocol of two stages in QKD*

The design framework of the protocol as shown in Fig. 4 shows the two stages of the implementation. In this process, each of the objects which are Alice, Bob and Eve play their own task. The Quantum channel and public channel object are executed on Alice's site, while Eve and Bob object are execute on different workstation respectively. This process works as follows:

1. First, Alice will establish connection between her and Bob because of UDP is connectionless protocol where she needs to initiate to connection. Means, she knows with who she communicates.
2. Then, Alice generated a length *k* of random number represented as bit, 0 and 1. These bits are sending to Bob through the quantum channel object. During the transmission, there is a possibility for Eve to read the sending bits.
3. If eavesdropping is exist, Eve is the first person who will read the bits in quantum channel object before it received at the Bob's site. Eve can modify the bits with two kinds of attack, which are intercept/resend or beam splitting.
4. Next, Bob read the updated version from quantum channel object and assume that he does not know about the Eve presence.
5. Then, Bob measure the bits that he read from the quantum channel object with his selected bases.
6. After that, Bob announce the bases he made to Alice via public channel which located at Alice's site.
7. Then, the sifting raw key will be established. Alice read the Bob measurement at the public channel and gives the confirmation to Bob about the position Bob has measures in the right bases; *m* bits by announce it at public channel.
8. Next step, Alice and Bob estimate the error to detect the presence of Eve. Both of them calculate and compare their bit error rate *e*. If they found their error rate is higher that maximum bits error rate, ($e > e_{max}$) , the communication will abort and start the communication from the beginning. (e_{max} has predetermined value)
9. Now, Alice and Bob will have a shared key which called as raw key. This key is not really shared because of the key version at Alice and Bob is still not the same. They eliminate the *m* bits from the raw key.
10. In order to obtain the final key, Alice and Bob have to pass through the error correction process on their own raw key to find the erroneous bits in some part of the keys that cannot be compared.
11. Then, privacy amplification is done to minimize the number of bits that Eve known as final key.
12. Lastly, Alice and Bob will get the same string of bits which known as shared secret key.

D. Measurement

This research will measure the key length of the raw key and error rate estimation based on attack from Eve on UDP wireless environment. There are three measurements that have been done as follows:

a) ***No Attack***: There is any attack from Eve during this process. Eve done nothing and give chance for Bob to receive all the bits send by Alice. Alice ill send all her generated bits to Bob through quantum channel to be read by Bob.
b) ***Intercept/resend:*** Intercept or resend attack give the opportunity foe Eve to read all the bits that has been written by Alice. From that, Eve can send a new modified string to Bob and pretend it was sent by Alice. Practically, Alice and Bob can measure 25% of error rate during the sifted key phase and Eve can get 50% of information from Alice site. Due to the random bits generated by Eve, the result of the key is still relying on comparison bit between Alice and Bob.
c) ***Beam Splitting:*** For this kind of attack, Eve will change the bits send by Alice that beam in quantum channel either 0 or 1 randomly and we assume that beam in quantum channel split successfully. Bits send by Alice will randomly split in quantum channel but it is rely on the strong level of mirror strength have been set by Eve to split the beam which is bits actually.

4. RESULT AND DISCUSSION

From the implementation, the result on key length and error shows the different value based on three measurements that have been experimented.

Fig. 5 shows the result of final bits length which is still not as the same as Alice send to Bob. Means, Eve is not only the agent that can affect the length of final bits but it cause from the quantum channel itself which contains of error because of imperfect channel due to the noise presence during the transmission.

The final bits length of intercept/resend attack seems similar as the result for no attack. Where Eve has generated a new string of random key and sends it to Bob as if the key string has been send by Alice. The probability of Alice and Bob to detect the presence of Eve is just 25% and the probability of similarity of key string generated by Eve with Alice is 50%. Both of Alice and Bob still can detect that error rate (e) but still lower than the maximum error rate ($e < e_{max}$) as illustrated in Fig. 6. Thus, they continued to error correcting process.

While in beam splitting attack, the result shows the final bits is much lower compared to the other two types of attack given. It cause of in this attack a random number of Alice's bits are split by Eve. As illustrated in Fig. 6, more error can be detected by Alice and Bob during error correction phase. Although the error rate (e) is still lower than the maximum error rate ($e < e_{max}$), Alice and Bob can detect as much as 50% of error in their sifted key. The length of corrected key is higher than other two attacks because of most of the bits have to eliminate in error correction process to minimize the information for Eve.

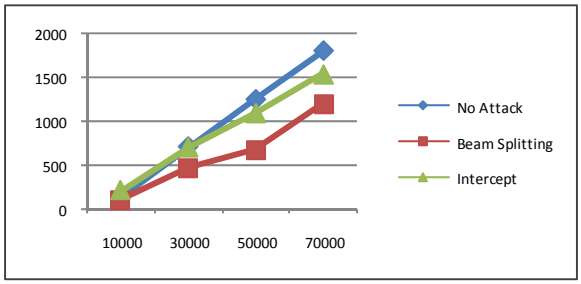


Figure 5: *Comparison of key length (Initial bits length vs. Final bits length)*

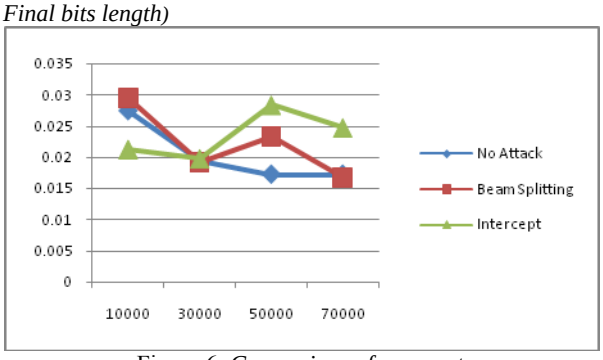


Figure 6: *Comparison of error rate*

5. CONCLUSION

From this paper, we can conclude that the QKD could be implemented on wireless by represent the photon as bit, 0 and 1. In wireless environment, the size of final key length which is known as final bit is depends on types of attack and noise. For future works, it could be expand in implementing in general wireless and differentiate the effect on UDP and TCP communication protocol.

REFERENCES:

[1] Ergűn Gűműş, G.Zeynep Aydin and M.Ali Aydin, "Quantum Cryptography and Comparison of Quantum Key Distribution Protocol", Journal of Electrical & electronics Engineering, vol.8, no.1, 2008, pp. 503-510.

[2] Vladimir L. Kurochkin and Igor G. Neizvestny, "Quantum Cryptography", 10th International Conference And Seminar Edm'2009, Section Iii, July 1-6, Erlagol.

[3] D. Mayers, "Unconditional Security in Quantum Cryptography", Journal of the ACM, Vol. 48, 1998, pp. 351.

[4] H.K. Lo, and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances",Science, Vol. 283, 1999.

[5] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie, "802.11i Encryption Key Distribution Using Quantum Cryptography", Journal Of Networks, vol. 1, no. 5, September/October 2006.

[6] IEEE 802.11 Wireless LAN Standards, IEEE 802.11 working group, Task Group I, URL: http://grouper.ieee.org/groups/802/11, March 2006.

[7] Nicolas Sklavos, Xinmiao Zhang, "Wireless security and cryptography: specifications and implementations",2007.

[8] B. Schneier, Applied Cryptography, John Wiley & Son, 1996.

[9] Xu Huang and Dharmendra Sharma, "Quantum Key Distribution for Wi-Fi Network Security", IEEE, 2008.

[10] C.H. Bennett et al., "Experimental Quantum Cryptography," *J.Cryptology*, vol. 5, no. 1, 1992, pp. 3–28.

[11] J. Postel," User Datagram Protocol", RFC 768, 28 August 1980.