Quantum Key Distribution for Wi-Fi Network Security

Xu Huang

School of Information Sciences and Engineering

University of Canberra

ACT 2601, Canberra, Australia

Xu.Huang@canberra.edu.au

Dharmendra Sharma

School of Information Sciences and Engineering

University of Canberra

ACT 2601, Canberra, Australia

Dharmendra.Sharma@canberra.edu.au

***Abstract*—There are a large variety of kinds of mobile wireless networks, Wi-Fi, based on the IEEE 802.11 standard, is a wireless local area network, mainly used in offices and campus at universities, meeting rooms, halls in hotels or in airports. For such limited coverage area, IEEE 802.11 standard may be observed as building-oriented environment, which potentially offers a chance to let quantum key distribution (QKD) play a role in the security of wireless communications. In fact, secured data transmission is one of the prime aspects of wireless networks as they are much more vulnerable to security attacks. In this paper, we explore the possibility of using Quantum Key Distribution (QKD) for authentication and data encryption for IEEE 802.11 standard. It will focus on some basic concept that how QKD merges the wireless communication, in particular the IEEE 802.11 standard. The software implementation of the first two phases of QKD, namely (a) raw key extraction and (b) error estimation, will be carefully investigated in this paper. A TCP/IP based Client-Server concept has been extended to the implement the communication between two users in C++ language in this paper.**

Keywords—Quantum Key Distribution (QKD), B92 protocol, BB84 protocol, 802.11, Wi-Fi, Socket Programming

I. Introduction

Wireless security is becoming increasingly important as wireless applications and systems are widely adopted. Numerous organizations have already installed or are busy in installing "wireless local area networks" (WLANs). These networks, based on the IEEE 802.11 standard, are very easy to deploy and inexpensive. Wi-Fi allows LANs to be deployed without cabling for client devices, typically reducing the costs of network deployment and expansion. As of 2007 wireless network adapters are built into most modern laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in ever more devices. Wi-Fi has become widespread in corporate infrastructures, which also helps with the deployment of RFID technology that can piggyback on Wi-Fi. Wi-Fi is a global set of standards, unlike mobile telephones, any standard Wi-Fi device will work anywhere in the world. Other important trends in wireless adoptions are including the introduction of wireless email with devices such as the Blackberry and The Palm VII, rampant digital cell phone use, including the use of short message service (SMWS), and the advent of Bluetooth devices. But the risks associated with the adoption of wireless networking are only now coming to light. A number of impressive attacks are possible and have been heavily publicized, especially in the IEEE 802.11b area. As far as base technology is concerned, wireless security appears to be following the usual "penetrate and path" route. Early wireless security focused almost exclusively on cryptography and secure transmission-with unfortunate results thus far. Wired Equivalency Privacy (WEP) security, the cryptography built in to 802.11b, for example, is completely broken and offers very little real security. In fact, one might argue that using WEP is worse than using no cryptography at all, because it can lull users into a completely unfounded sense of security. For every time one introduces new technologies one can rest assured that exploits for it are soon to follow. So with this in mind it was no great surprise that 64 bit WEP was quickly found to be lacking in terms of its implementation. So the vendors upped the ante and came out with 128 bit WEP, and this in turn was also found to be lacking. Wi-Fi hacking has been around for some time now, and oddly enough has really received little press. Since 2001, 64 bit WEP has been breakable [1]. That was also around the time that well known tools such as Airsnort gave the ability to break into wireless network to the masses. In fact we looked at some of the tools that exist today which will allow user to discover wireless access points (WAP). It is obviously to face the fact that wireless network have become very popular over the past few years for not only business, but also the home market. In all likelihood user's neighbors are probably running a wireless router for their home computer network even though it is not using a wireless card. The wireless communication revolution has been bringing fundamental changes to data networking, telecommunication, and has been making integrated networks a reality. By freeing the user from the cord, personal communications networks, wireless LAN's [13], wireless MAN's, mobile radio networks and cellular systems, harbor the promise of fully distributed mobile computing and communications, any time, anywhere.

There are number of such wireless services widely in use at the moment. Wi-Fi (IEEE 802.11) [2] [5], WiMAX (IEEE 802.16) [8] and Mobile device networks such as GSM, 3G are now cater users across the globe.

Without physical boundaries, a wireless network faces many more security threats than a wired network does. For an example, WEP (Wired Equivalent Privacy) the authentication and data confidentiality definition of IEEE 802.11 standard was found to be vulnerable to security attacks, hence IEEE later came up with its 802.11i [3] to rectify the flaws of WEP. Likewise security flaws of IEEE 802.16 standard too have been exposed [4], [5]. This indicates how important the authentication and data encryption of these wireless networks. Given the tremendous growth in WLAN usage, and the weakness of current security protocols, new and better security mechanisms are required to protect wireless transmissions. One of these is the IEEE 802.1x standard [11]. 802.1x was intended to provide strong authentication, access control, and key management and allow WLANs to scale by allowing centralized authentication of wireless users or stations. It is well known that 802.1x is based upon an existing authentication protocol known as the extensible authentication protocol (EAP) which in itself is an extension of PPP (point-to-point protocol). It is also noted that 802.1x maps EAP to the physical medium, regardless of whether it is Ethernet, Token Ring or wireless LAN. In fact, it is necessary to note that the 802.1x standard provides for authentication only. The standard does not specify the specific types of authentication or any type of encryption. In fact, it is reported that 802.1x is susceptible to session hijacking as well as man-in-the-middle attacks [17], [18].

One area that hasn't got much attention, which has shown a great future, on wireless security is the use of quantum cryptography for encryption of data. The uncertainty principle in quantum mechanics created a new paradigm for Quantum Key Distribution (QKD) [7], [12], [16]. The uncertainty principle in quantum mechanics created a new paradigm for cryptography: Quantum cryptography, or more specifically QKD. Unlike the classical cryptography which relies on mathematical complexity, quantum cryptography is based on the laws of quantum theory in physics. The laws of quantum physics showed that nobody can measure a state of arbitrary photon carrying information without introducing disturbances to the transmission. Since all these eavesdropping can be detected, quantum cryptography is considered as providing unconditional security. In fact this is called "No-Cloning" Theorem [19] and implies that a possible eavesdropper cannot intercept, measure and re-emit a photon without introducing a significant and therefore detectable error in the re-emitted signal.

II. Wireless 802.11 and Quantum Cryptography

As we described above that 802.11 security defines WEP [14] for the authentication and data confidentiality of user data over the wireless link. However, WEP was not well designed and presents serious vulnerabilities as a new standard for the 802.11 security. In this context, 802.11i is defined to rectify the flaws of WEP. 80211i received much attention from specialists in cryptography and network security.

Regarding the 802.11i authentication and key management, we knew that 802.11i defines two authentication and key management methods, namely 802.1X authentication and preshared key. The former is for large network having an important number of access points and the later is suitable for small network.

Therefore, the former has three elements participating to the authentication and key management are the supplicant (or mobile terminal), authenticator (or access point), and the authentication server. Once having the pairwise master key (PMK), the access point starts the four –way handshake for the mutual authentication and the derivation of the pairwise transient key (PTK) with the mobile terminal.

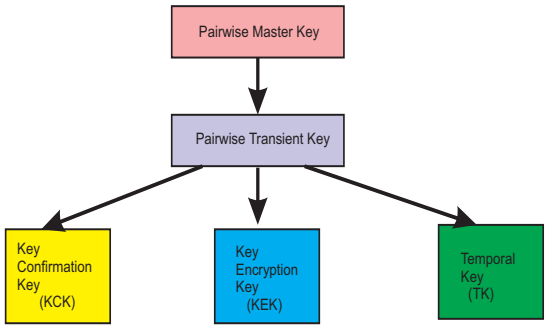

Figure 1. Pairwise key hierarchy

In contrast to the 802.1x, the preshared key is involved in the authentication and key management using preshared key without "authentication server" and no extensible authentication protocol (EAP)-based authentication.

Following [15], we are using Figure 1 shows the pairwise key hierarchy containing the keys related to the encryption of unicast traffic.

It is noted that 802.11i has many keys at different levels, which becoming a key hierarch as shown Figure 1. At the top level there is the master key titled pairwise master key (PMK) that is used to derive the other keys.

The pairwise transient key (PTK) is created between the access point and the mobile terminal during the 4-way handshake. The PTK is split into three final temporal keys, namely key confirmation key (KCK), key encryption key (KEK), and temporal key (TK).

Quantum Key Distribution systems transmit the secrete key, which are derived from random numbers, one photon (one bit) at a time in a polarized state. If intercepted by an eavesdropper or due to other atmospheric interferences etc, this state will change, and an error will be detected at the receiving side [6].

Quantum cryptography aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. For the moment, the use of quantum physics at cryptographic ends is limited mainly to the distribution of secret keys.

There are several QKD protocols available. Most widely used is being the BB84 [8]. B92 (Charles Bennett), a slight

variation of BB84, is another well known QKD protocol [9]. B92 can be used two non-orthogonal states which represent the bit values 0 and 1 as shown below:

$$|u_0>, \quad |u_1>, \tag{1}$$

BB84 coding scheme, invented by Charles Bennett and Gilles Brassard, is the first quantum cryptography communication protocol. There are four different quantum states. The corresponding four quantum states can be expressed as below:

$$|0>, \quad |1>, \quad |\overline{0}> = \frac{1}{\sqrt{2}}(|0> + |1>), \quad |\overline{1}> = \frac{1}{\sqrt{2}}(|0> - |1>), \tag{2}$$

As an example, this coding system uses four non-orthogonal polarization states identified as *horizontal*, *vertical*, 45° and *135*°.

This protocol operates with transmitting party (say, Alice) sending polarized quantum bits (qubits) to the receiving party (call, Bob) via the quantum channel.

Once the quantum transmission finishes, Bob publicly communicates to Alice which measurements operators he used for each of the received bit. Alice then informs Bob which of his measurement operator choices were correct.

The B92 quantum coding scheme is similar to the BB84, but uses only two out of the four BB84 non-orthogonal states, as shown in equation (1). It encodes classical bits in two non-orthogonal BB84 states. In addition to this, Bob simply sends the positions of the bases to retain, keeping the protocol simpler and faster to operate.

In out current paper, we decided to implement B92 protocol as a case study, the whole processing can be easily extended to four states, where BB84 used, and therefore from now on in this paper we are focusing on two quantum states, namely B92 protocol unless otherwise.

The Quantum key transmission happens in two stages that can be shown in Figure 2.

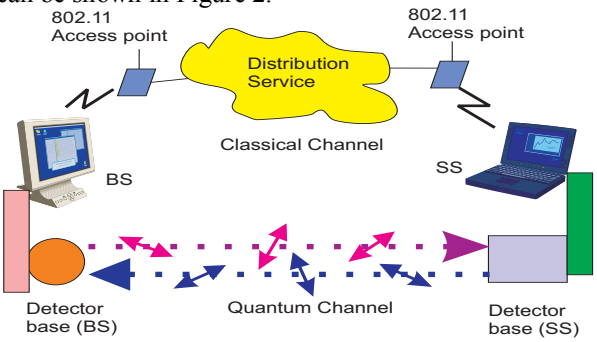

Figure 2. Simplified block diagram of a point-to-point QKD link in concept, where SS is denoted "subscriber station" and the BS standing for "base station"

Those two stages are as follows:

Stage 1: Quantum Channel (One way communication)

This transmission could happen in either through free space or optical fiber. At present this implementation is being done at the Monash University, Australia.

Stage 2: Classical Channel (Two way communication)

This phase deals with recovering identical secrete keys at both ends.

During the stage Alice & Bob communicate over a Classical channel that can be divided further in 4 main phases as shown below:

(a) Raw key extraction (Sifting), (b) Error Estimation, (c) Reconciliation, (d) Privacy Amplification.

It is noted that there are, in terms of physics concepts, two different channels one is classical channel another is quantum channel. For the implementation that we are going to present the wireless Wi-Fi is chosen as the classical channel (Figure 2). The quantum channel is the line of sight (LOS) optical path running by the polarization photon.

We can find, in Figure 2, that the classical channel forms by the standard Wi-Fi wireless and the quantum established by the optical photos. In Figure 2, in order to discuss our implementation more generally, SS is denoted "subscriber station" and the BS standing for "base station".

The Quantum channel is taking the task that using quantum cryptography to establish the key used for the encryption of user data in 802.11i, which is the TK. It is noted that TK is part of the PTK, as shown in Figure 1, which is established during the four-way handshake, we shall modify the four-way handshake to integrate the B92 protocol, as a case study, and make it as quantum handshake.

When the quantum handshake completion the wireless Wi-Fi will either refuse the subscriber station to communicate data via the classical channel or take the subscriber station to access the Wi-Fi and the system becomes "normal" Wi-Fi working states, which will run the communications in the defined classical channels.

Quantum Network

Quantum Key Distribution techniques are emerging as useful building blocks in highest secure networks. The quantum network marries a variety of QKD techniques to well established internet technology in order to build a secure key distribution system employed in conjunction with the public internet or, more likely, with private networks that employ the internet protocol suite [2]. At present there are large numbers of such private networks in widespread use around the world with customers' desire secure and private communications.

The merge of QKD technologies to these networks proves feasible and appealing in certain contexts.

Free space QKD uses the air as the medium for the transmission of photons between the quantum sender and receiver. The feasibility of QKD over the air is considered problematic because of a medium with varying properties and a high error rate. In particular for the limited distance and indoor environment the quantum channel would be realized at the reasonable level.

Therefore QKD technology fits well with the wireless security architecture delivering guarantied secure wireless

traffic via quantum cryptography at the reasonable level and will be mature in the near future based on further researches.

Figure 3 shows the protocol for the first two stages of QKD described in above.

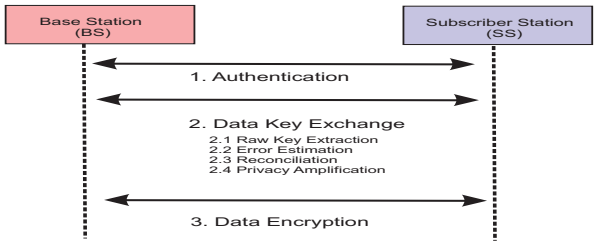

Figure 3. The protocol for first 2 stages of QKD

III. System Implementation

We have designed the framework as shown in Figure 4 which presented the integrate QKD (we have used B92 protocol as the case study) in 802.11i.

The KCK is generated from the PMK to serve the mutual authentication of the supplicant and the authenticator and protect the B92 protocol from the main-in-the-middle attack as described in [15]. Once the mutual authentication finished, the supplicant and the authenticator stats the B92 protocol for the establishment of the Q-PTK. The Q-PTK is splits into the KEK and TK .

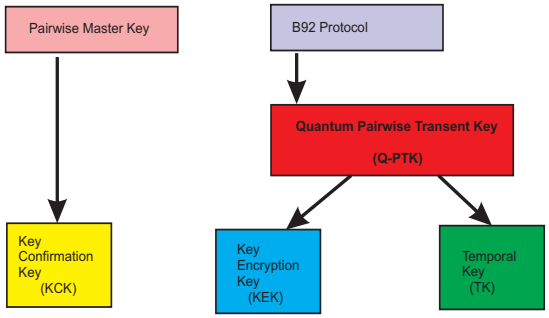

Figure 4. Quantum handshake framework for B92 protocol with Wi-Fi

It is noted that we can use quantum cryptography to establish the PK, therefore all KEK, KCK, and TK are established using quantum cryptography.

Security provides subscribers with privacy across the broadband wireless network. It achieves security by encrypting connection between BS (Base Station) and SS (Subscriber Station).

The protocol for first 2 stages of QKD

Index Files

The software implementation depends on the key bits recorded at BS and SS. These key bits are to be recorded in set of files, known as "Index Files". Since the original key transmitted by BS in the Quantum Channel could contain many bits (gigabits), there will be multiple index files generated at either ends.

Those index files will act as the input to this software development project.

Index files at BS

All the key bits that BS transmits in the Quantum Channel are to be recorded into index files at her end. These files hold the original key that BS transmitted to SS.

Examples of the bits recorded in those index files:-
1,0,1,1,0,0,0,1,1,0,0,1,0,1,1,1,0,0,0,1,1,0
where "," being the delimiter

Index files at BS

All the key bits that BS transmits in the Quantum Channel are to be recorded into index files at her end. These files hold the original key that BS transmitted to SS.

Examples of the bits recorded in those index files:-
1,0,1,1,0,0,0,1,1,0,0,1,0,1,1,1,0,0,0,1,1,0
where "," being the delimiter

Index files at SS

During the Quantum transmission, SS too records the key bits that he received from BS in Index files. These bits will not be identical to what BS has transmitted due to the random bases used by SS's photon detector, eavesdropper attacks, channel noise, dark counts of the photon detector etc..

Therefore the index files recorded at SS's end will comprise non-receptions. Non-receptions are the bit positions that SS should have received, but not receive a bit.

Examples of the bits recorded at SS's index files:-
1,1,,,0,0,,0,1,,1,0,0, ,0, ,1,,1,0,0, ,1,1,0
where "," being the delimiter

With the use of delimiter to separate each key bit, it is easy to identify the of non-reception bits.

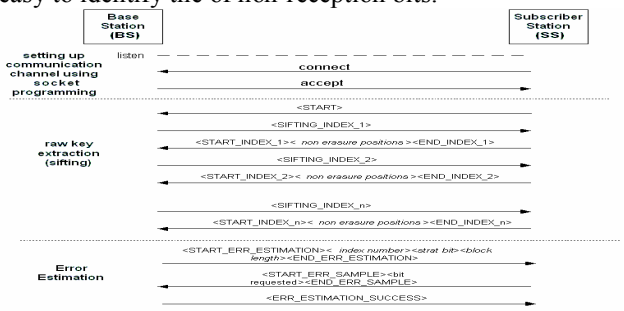

Figure 5. The protocol for first 2 stages of QKD

Program Structure and Protocol

Both BS and SS maintain a C++ class to hold individual parameter values of each index file. This class comprises of: Key bits, total number of bits, non-receipt bit positions etc.

At start up, BS and SS reads all the index files and populates the respective parameters in their data structures. Figure 5 shows the protocol used between BS and SS.

The software has been developed in C++ language using UNIX socket programming.

In order to establish the communication path, BS first *listen*s to a specified port. SS sends the *connect* message to the specified port in BS. Upon receiving the *connect* request, BS sends *accept* call to SS establishing the communication path between them.

Raw Key Extraction (Sifting)

During this process, which happens at start up, SS sends the non-erasure bit positions to Alice by running through the index file data loaded into the memory. BS in turn, processes her index files and keeps only those corresponding bits.

At the end of this process, both BS and SS will have index files of identical lengths after removing all non-receipt bits. This process is called *Raw Key Extraction* and the keys recovered after this phase is known as *BS Raw Key* and *SS Raw Key*.

Error Estimation

This process starts with BS requesting SS to send a block of bits of length "L" from a particular index file.

This request has the following format:

<STRAT_ERR_ESTIMATION> <INDEX FILE NUMBER> <START BIT> <LENGTH> <END_ERR_ESTIMATION>

All the above values can be read as configurable parameters to the program.

Upon receiving this message, SS sends the requested block of bits to BS.

BS calculates the Bit Error Rate (**e**) of the Quantum transmission.

$$\mathbf{e} = \frac{\text{Number of bits in error}}{\text{Total number of bits in the block}} \times 100\ \% \qquad (3)$$

BS then compares with the maximum error rate allowed ($\boldsymbol{e}_{max}$). This value is also known as Quantum Bit Error Rate (QBER).

If $\mathbf{e} <= \mathbf{e}_{max}$ they accept the quantum transmission and proceeds to the next phase called Reconciliation. Both BS and SS remove those bits which are publicly revealed from their index file(s).

If $\mathbf{e} > \mathbf{e}_{max}$ BS sends ABORT message to SS indicating the quantum transmission contains errors to a level where they cannot recover the key from the bits received. In this case, they seizes the session by terminating the program.

IV. Conclusion

In this paper we present the implementation of first two stages of KQD for Wi-Fi. At present, the first two stages of B92 protocol has been implemented in C++ language on Linux platform. GNU has been used as the compiler. This set up has been successfully tested with multiple index files at the University of Canberra test lab.

Lot of performance improvements have been done to improve the quality of the software. Initially all index files were processed by writing to various intermediate temporary files. This caused a heavy overhead as the program consumes considerable amount of time during bit comparisons etc when doing file processing. To avoid this inefficiency, a STL list structure has been implemented to hold the index file data. Due to this modification, most of the computations and bit comparisons are done in-memory. This has resulted in improving the efficiency by about 60%.

Also some of the important values have been fed to the program as configurable parameters. With this set up, the program can be operated by setting different values to suit any requirements. One such parameter is the QBER, where this value is used to calculate the error rate of the quantum transmission. QBER of the quantum transmissions could be impacted by various issues (described earlier) causing it to vary per each transmission. Therefore by having the QBER as a configurable parameter, this software can be used to run even for simulation purposes by setting different values.

At present the software designed to cater B92 protocol only. Except for the first phase, both B92 and BB84 operate in almost identical fashion [10]. Some Wi-Fi security flaws have been identified so far [4], [5]. Those flaws too will have to be taken into account to for the full protocol suite.

Since photon transmission of QKD only happens as a line-of-sight communication, special emphasis has to be paid to the NLOS feature of Wi-Fi. Also Point to multipoint feature of Wi-Fi needs to be implemented in KQD.

References

[1] Don Park, "The Lack of WiFi Security (part 1), Dec 07, 2006 http://www.windowsecurity.com/articles/WiFi-security-lack-Part1.html?prontversion.

[2] http://www.iop.org/EJ/article/1367-2630/4/1/346/nj2146.html Building the Quantum Network, Chip Elliott, BBN Technologies, New Journal of Physics 4 (2002) 46.1-46.12

[3] IEEE Standrad 802.11i, Part 11: Wireless LAM Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004

[4] Security Issues in Privacy Key Management Protocols of IEEE 802.16, Sen Xu, Manton Matthews, Chin-Tser Huang

[5] Security Issues of IEEE 802.16 (WiMAX), Jamshed Hasan

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

[7] Charles H. Bennett "Quantum Cryptography: Uncertainty in the Service of Privacy" Science 257, 752-3 (1992)).

[8] C.H. Bennett and G. Brassard "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179.).

[9] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. 68, 3121-3124 (1992).

[10] Samuel J. Lomonaco, A Quick Glance at Quantum Cryptography (1998)

[11] J. Philip Craiger, "802.11, 802.1x, and wireless security," GIAC security essentials certification Practical Asssignment, version 1.4, ©SANS Institute 2002.

[12] Moritz Lenz, "High Bit Rate Quantum Key Distribution Systems 5th Year Project Report 2006/2007", Heriot Watt University, Feb. 16, 2007. http://moritz.faui2k3.org/

[13] IEEE Standard for Local Metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems

[14] J. Edeny and W. A. Arbaugh, Real 802.11 Security-Wi-Fi protected access and 802.11i, Addision-Wesle, 2004.

[15] 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, Sepetember/October 2006, pp.9-20

[16] W.T. Buttler, R. J. Hughes, P.G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C.G. Peterson, and C.M. Simmons, "Free-space quantum key distribution," ar Xiv: quant-ph/9801006 v1, Jan. 1998.

[17] Connolly, P.J. "The trouble with 802.1x," InfoWorld. 8March 2002, URL: http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x.xml

[18] Schwartz, E. "Researchers crack new wireless security spec." InfoWorld. 14 February 2002, URL: http://www.infoworld.com/articies/hn/xml/02/02/14/020214hnwifispec.xml

[19] W. Wootters and W. Zurek, "A single quantum cannot be cloned". Nature, vol. 299, pp 802-803, 1982