13

Agent-Oriented Novel Quantum Key Distribution Protocol for the Security in Wireless Network

Xu Huang, Shirantha Wijesekera and Dharmendra Sharma
University of Canberra
Australia

1. 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 [Park, Don 2006]. 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

Source: Multiagent Systems, Book edited by: Salman Ahmed and Mohd Noh Karsiti,
ISBN 978-3-902613-51-6, pp. 426, February 2009, I-Tech, Vienna, Austria

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 [IEEE Standard for Local Metropolitan area networks], 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) [Chip Elliott, 2002] [Hasan Jamshed 2006], WiMAX (IEEE 802.16) [Bennett, C.H. 1984] 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 [IEEE Standrad 802.11i] to rectify the flaws of WEP. Likewise security flaws of IEEE 802.16 standard too have been exposed [Sen Xu, et.al. 2006], [Hasan Jamshed 2006]. 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 [Craiger, J. Philip 2002]. 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 [Connolly, P.J., 2002], [Schwartz, E. 2002].

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) [Bennett & Charles H., 1992], [Lenz & Moritz, 2007], [Buttler et al., 1998]. 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 [Wootters, W. and Zurek, W., 1982] 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. In this chapter we shall introduce some updated research results of our current projects [Huanget al., Feb 2008] and [Huang et al., May 2008]. The next section describes wireless 802.11 and quantum cryptography. In section 3, we shall discuss the system implementation for QKD in a wireless communication. In section 4 we present our new developed protocol for wireless networks and in section 5 we present our conclusion.

2. Wireless 802.11 and quantum cryptography

As we described above that 802.11 security defines WEP [Edeny, J. & Arbaugh, W.A., 2004] 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.

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 [Thi Mai Trang Nguyen et al., 2006], 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.

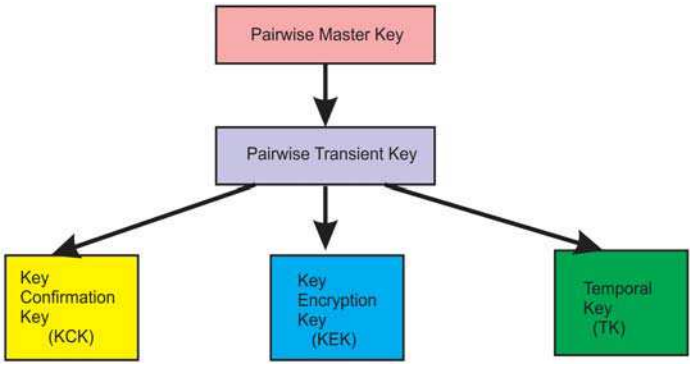

Fig. 1. Pairwise key hierarchy

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 [Bennett et al., 1992].
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 [Bennett, C.H. & Brassard, G, 1984]. B92 (Bennett, Charles 1992), a slight variation of BB84, is another well known QKD protocol [Bennett, C.H., 1992]. B92 can be used two non-orthogonal states which represent the bit values 0 and 1 as shown below:

$$\begin{aligned} &| u_0 >, \\ &| u_1 >, \end{aligned} \tag{1}$$

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:

$$\begin{aligned} &| 0 >, \\ &| 1 >, \\ &| \overline{0} >= \frac{1}{\sqrt{2}}(| 0 > + | 1 >), \\ &| \overline{1} >= \frac{1}{\sqrt{2}}(| 0 > - | 1 >), \end{aligned} \tag{2}$$

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. It is noted that in Figure 2 the Wi-Fi connections are classical channels and the "optical Fiber" channels are quantum channels.
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.

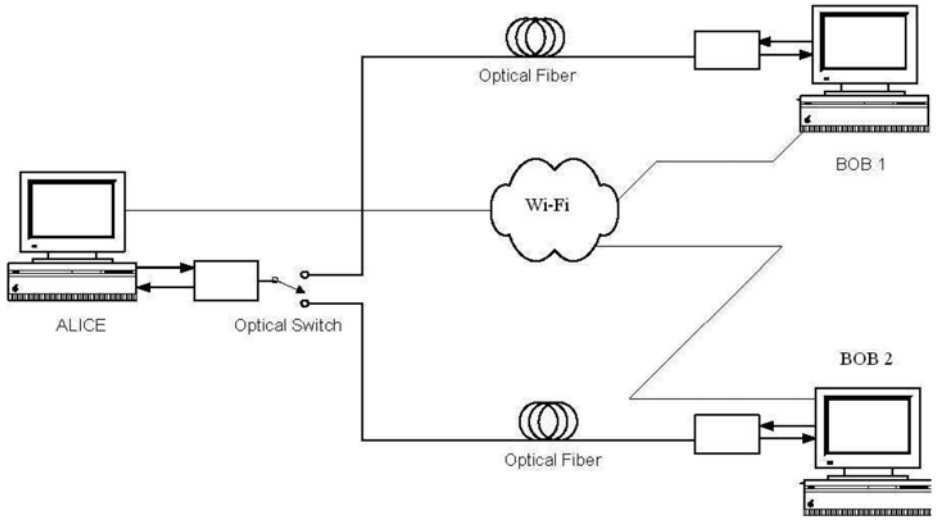

Fig. 2. Simplified block diagram of a point-to-point QKD link in concept, where SS is denoted "subscriber station" and the BS standing for "base station"

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.

The quantum channel between Alice and Bob1 is shown in Fig. 3, the channel between Alice and Bob2 is similar. At Alice, laser pulses are generated by vertical cavity surface emitting lasers (VCSELs) and attenuated into single photon level. The polarization states of photons

are set by polarizers according to corresponding protocol (B92 or BB84). Then photons are combined and sent into a fiber through a non-polarizing beam splitter (NPBS). The polarizers Pol. 0A, 0B, 1A, and 1B are oriented to 0°, 90°, +45°, and -45° respectively. Only two channels, 0A and 1A, are used for B92, while all four channels are used for BB84. At Bob, polarization controllers recover the polarization state of photons to their original state at Alice. The 3-dB coupler randomly chooses the detection base and the polarization beam splitter (PBS) helps to determine the key value via the an agent-ortened. Finally the photons are detected by single photon detectors (APDs). Two APDs, 0A and 1A, are used for B92, while four APDs are all used for BB84.

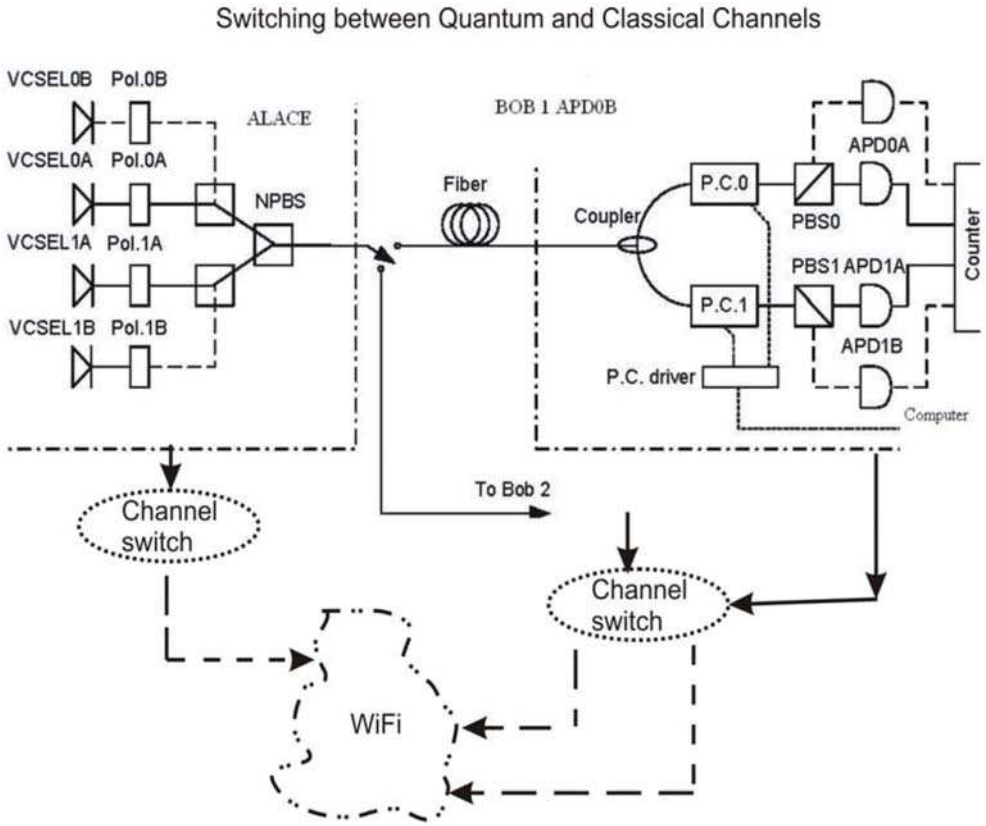

Fig. 3. Quantum channel implementing by optical fibers: schematic diagram of the QKD system with PRAC sub-systems. VCSEL: Vertical Cavity Surface Emitting Laser ; Pol.: Polarizer; NPBS: Non-Polarizing beam splitter; P.C.: Polarization Controller; PBS: Polarizing beam splitter; APD: Silicon avalanche photodiode.

2.1 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.

2.2 Agent society

Computer systems no longer stand along, but are networked into large distributed systems. The movement away from machine-oriented views of programming toward concepts and metaphors that more closely reflect the way we ourselves understand the world. Programmers conceptualize and implement software in terms of ever higher-lever more hunan-oriented.
An agent is a computer system that is capable of independent (autonomous) action on behalf of its user or owner (figuring out what needs to be done to satisfy design objectives, rather than constantly being told)..
Normally there are two key problems need to be noted for agnet society designs, namely (a) How to we build agents that are capable of indendent, autonomous action in order to successfully carry out the tasks that we delegate to them? (b) How do we build agents that are capable of interacting (cooperating, coordinating, negotiating) with other agents in order to successful cary out the tasks that we delegate to them, particularly when the other agents cannot be assumed to share the same interests/goals?
It is well known that an intelligent agent is a computer system capable of flexible autonomous action in some environment. Here "flexible" means (a) reactive (b) pro-active and (c) social.
A reactive system is one that maintains an ongoing interaction with its environment, and responds to changes that occur in it (in time for the response to be useful).
Pro-activeness is generating and attempting to achieve goals; not driven solely by events; taking the initiative.
Social ability in agents is thew ability to interact with other agents (and possibly humans) via some kind of agent-communication language, and perhaps coopewrate with others.
There are other properties of agency somethimes to be discussed depend on the indivical cases, such as mobility, which shows an agent to move around an electronic network; veracity, showing whether an agent will knowingly communicate false information; benevolence, showing whether agents have conflicting goals, and thus whether they are inherently helpful; rationality, showing whether an agent will act in order to achieve its goals, and will not deliberately act so as to prevent its goals being achieved.
In fact, for the channle switching shown in Figure 3 it can be expressed as in block diagram shown in Figure 4.
The design for the implemation of the switching will be run by the "operational agent society" shown in Figure 5.

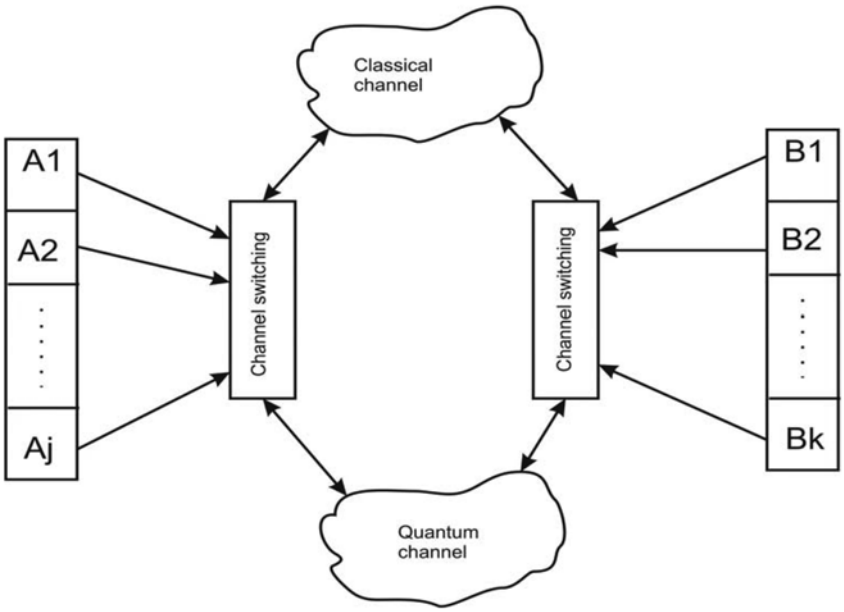

Fig. 4. A block diagram for QKD channels' switching

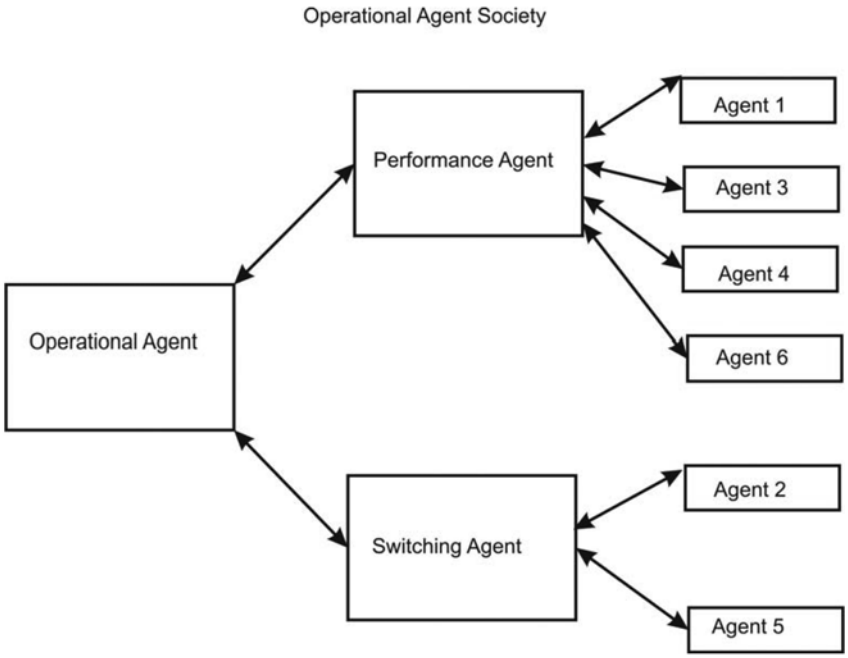

Fig. 5. A block diagram for "Operational Agent Society".

We design two types agents, switching agent and performance agent. The performance agent looks after the "perfomances" between transmiters and seitching, namely Alace 1 (A1), Alace 2 (A2), etc to channel switch or Bob 1 (B1), Bob 2 (B2) etc to channel switch. The switch agent takes of the channel switching. In Figure 4, we labeled the agent number from left to right between Ai ($i \leq j$) and channel switch (left hand side in Fig 4) as "Agent 1",looking after channel switch is "Agent 2," between channel switch and mediea as "Agent 3", between media and another channel switch (right hand side in Fig 4) is "Agent 4", the rigth hand side channel switch is taken care of by "Agent 5" and between channel switch and receiver Bq ($q \leq k$) is "Agent 6". All the labeled agents are shown in Figure 5 for the Operational Agent Society.
Therefore, agent 1 makes sure the tresmitor Ai ($i \leq j$) is connected to channel switch via the media. Agent 3 ensures the transimitions are connected by quantom channel when the communications are beginning. Agent 4 would play the similar role for the transmitions. Agent 6 will check the the receivers between the switch channel are correctly connected. Angent 2 and agent 5 check the channel situation, either in quantum state (at the beginning for the communications) or classical state (after identifications via quantum channels). The performance agent will cooperatively working with switching agent via operational agent.

3. System implementation

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 [Thi Mai Trang Nguyenet al., 2006].
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.
It is noted that we can use quantum cryptography to establish the PK, therefore all KEK, yKCK, 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

3.1 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.

3.2 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.

3.3 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.

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

BS then compares with the maximum error rate allowed (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.

4. Our new developed protocol for wireless networks

Recall IEEE 802.1X offers an effective framework for authenticating, managing keys and controlling user traffic to protect large networks. It employs the Extensible Authentication Protocol (EAP) [11] to allow a wide variety of authentication mechanisms. 802.1X authentication process happen between three main elements. The user or the client that wants to be authenticated is known as Supplicant or Station (STA). The actual server doing the authentication is called Authentication Server (eg: RADIUS, DIAMETER). The Authenticator or the Access Point (AP) allows only the supplicants who are authorized by the authentication server to gain access to the network.
Figure 2 shows the RSN Association, IEEE 802.1X authentication and key establishment process. This assumes the pre-shared key is not used. In Figure 2, flows 1 to 6 illustrate the IEEE 802.11 association and authentication process. Once the IEEE 802.11 association is completed, the IEEE 802.1X authentication starts. This is shown by flows 7 to 13 in Figure 2. During this process "Supplicant" sends "Request Association" to "Authenticator". Authenticator responds with "Association Response" to indicate the supplicant system has associated with the switch. Supplicant then sends EAP-Start message to the Authenticator. This begins a series of message exchanges to authenticate the Supplicant. Having seen the link is active, Authenticator sends "EAP-Request/Identity" packet to Supplicant. The Supplicant sends an "EAP-Response/Identity" packet to the Authenticator, which is then passed on to the Authentication Server. The Authentication Server sends back a challenge to the Authenticator, such as with a token password system. The Authenticator unpacks this from IP and repackages it into EAPOL (EAP over LAN) and sends it to the Supplicant. Different authentication methods will vary this message and the total number of messages. The Supplicant responds to the challenge via the Authenticator, which passes the response onto the Authentication Server. The Authentication Server responds with a success message, if the Supplicant provides proper identity, which is then passed onto the supplicant. Authenticator then allows the Supplicant to access the network with restrictions based on attributes that came back from the Authentication Server. For example, the Authenticator might switch the Supplicant to a particular virtual LAN or install a set of firewall rules. At the end of this stage, the Supplicant and Authentication Server have generated a shared Pairwise Master Key (PMK). The Authentication Server then transmits PMK to the

Authenticator through a secure channel (e.g.: TLS). This PMK is used to derive Pairwise Transient Key (PTK) through an exchange of IEEE 802.1X EAPOL-Key frames, often called as 4-Way Handshake in the IEEE 802.11 standard. Once the 4-Way Handshake is completed, the group key handshake is initiated. It is used to generate and refresh the group key, which is shared between Authenticators (APs) and group of Supplicants. This key is used to securely exchange broadcast and multicast messages in the air.

In our current work, we paid special attention on the stage where mutual authentication employs in 802.11i networks. We take the advantage of EAP types such as EAP-TLS, EAP-TTLS which offer mutual authentication, to merge 802.11i networks with QKD. Our aim is to introduce quantum key transmission soon after the 802.1X authentication is completed. The proposed protocol is shown in figure 7.

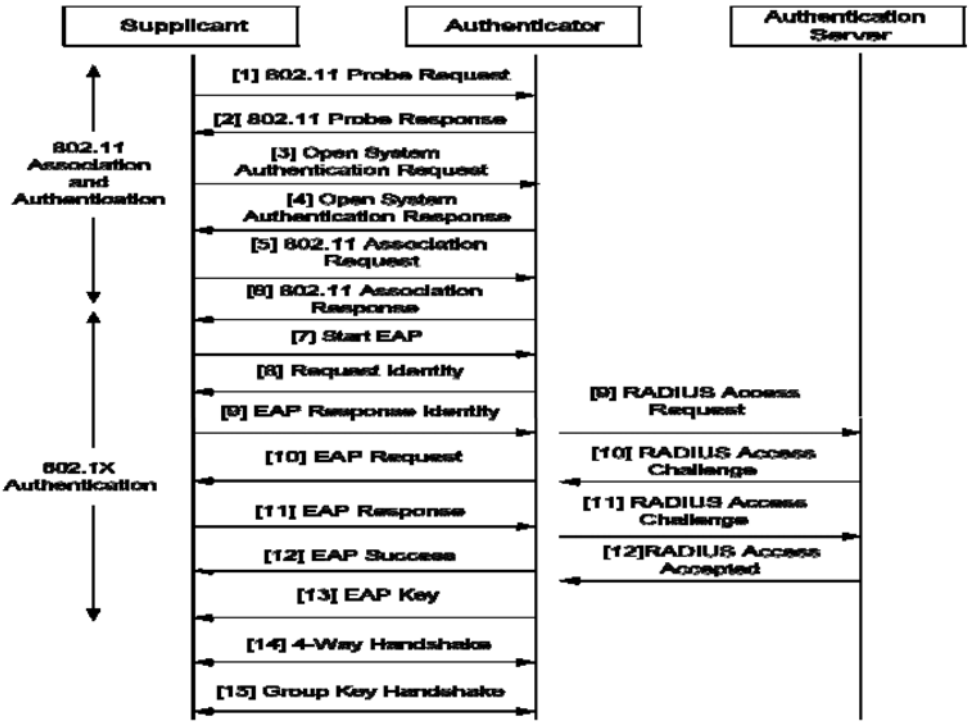

Fig. 7. RSN Association, IEEE 802.1X Authentication and Key Establishment process

At the end of the IEEE 802.1X authentication, both supplicant and authenticator hold PMK. As described in flow 13 of figure 7, the last message of 802.1X protocol is the EAPOL message giving the EAP Key from Authenticator to Supplicant. Since the two parties are mutually authenticated at this stage, we know this message is genuine. We use this message as the starting point of quantum transmission. By this way we can safely start the quantum key exchange as both the Supplicant and Authenticator are mutually authenticated.

As soon as the Supplicant receives the EAP Key message, the communication switches to quantum channel. Supplicant starts BB84 key distribution, by sending series of photons towards the Authenticator. Once the photon transmission finishes, the communication switches back to classical wireless channel. Afterwards they complete the BB84 quantum key exchange as described in previous section. At the end of this process, i.e. at flow 6, both Supplicant and Authenticator hold a common key, which we call as Quantum Key (Q-Key). We get this Q-Key as the PTK. For CCMP, PTK is 256 bits, while TKIP occupies 384 bits for PMK. Once PTK is available, we can retrieve the key hierarchy containing all other keys using the Pseudo Random Function (PRF) as previously described.

From PTK, we can derive KEK, KCK and TK. From KCK, MIC can be calculated. We use this MIC in our subsequent protocol messages to implement mutual authentication. The main reason of performing mutual authentication at this stage is that, BB84 is subjected to man-in-the-middle attacks [IEEE Standard for Local Metropolitan area networks]. Even though the Supplicant and Authenticator are mutually authenticated during the EAP authentication, an eavesdropper can fake a photon transmission towards Authenticator after seen the EAP Key message. At this stage, Supplicant performs XOR operation with the MIC and the first set of bits of equal length in PMK. We call this resulted MIC as Quantum MIC (Q-MIC).

$$Q\text{-}MIC = (MIC)\ XOR\ (first\ bits\ of\ PMK,\ same\ length\ as\ MIC) \tag{4}$$

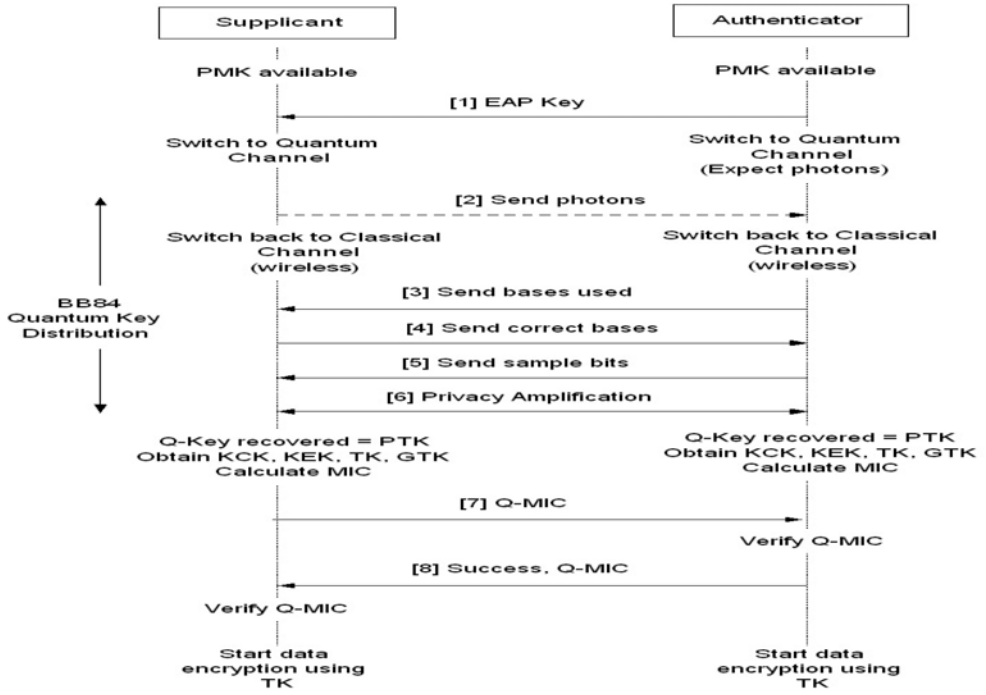

Fig. 8. Novel Proposed Protocol

The Supplicant sends the Q-MIC to Authenticator as shown in flow 7 of Figure 8. Upon receiving Q-MIC, Authenticator verifies the Q-MIC. Since the Authenticator is in possession of all the keys, it can calculate its own Q-MIC and compares with the one came from the Supplicant. If they match, the Supplicant is authenticated. The Authenticator then sends Success message along with Q-MIC to Supplicant as shown in flow 8 of Figure 8. Supplicant verifies the Q-MIC to authenticate the Authenticator, thus achieving the mutual authentication. From now on both parties use TK to encrypt the data and start secure communication and also the GTK for multicast applications.
With this protocol, we can eliminate the use of IEEE 802.11i 4-way handshake. It was shown that the message 1 of 4-way handshake is subject to DoS attacks. Intruders can flood message 1 to the supplicant after the 4-way handshake has completed, causing the system to fail.

5. Conclusion

In this paper we present the implementation of first two stages of an agent-oriented KQD for Wi-Fi. At present, the first two stages of B92 (or BB84) protocol has been implemented in C++ language on Linux platform. The KQD can handle multiuser as it benefits from an agent-oriented mechanism.
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%.
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.

6. References

Bennett, C. H. and Brassard, G., 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..

Bennett et, C.H. , Bessette, Francois, BBrassard, Gilles, Salvail, Louis, and Smolin, Jojn., Experimental Quantum Cryptography, *J. Cryptology,* vol. 5, no. 1, 1992, pp. 3–28.

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

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

Buttler, W.T., Hughes, R.J., Kwiat, P.G., Luther, G.G., Morgan, G.L., Nordholt, J.E., Peterson, C.G., and Simmons, C.M., Free-space quantum key distribution, at Xiv: quant-ph/9801006 Vo1. 1, Jan. 1998.

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

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

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

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

Hasan, Jamshed , Security Issues of IEEE 802.16 (WiMAX), 2006. http://scissec.scis.ecu.edu.au/conference_proceedings/2006/aism/Hasan%20-%20Security%20Issues%20of%20IEEE%20802.16%20(WiMAX).pdf

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

Lomonaco, Samuel J., A Quick Glance at Quantum Cryptography (1998), http://www.cs.umbc.edu/~lomonaco/lecturenotes/9811056.pdf

Huang, Xu, Wijesekera, Shirantha and Sharma, Dharmendra, Implementation of Quantum Key Distribution in

Wi- Fi (IEEE 802.11) Wireless Networks, *IEEE the 10th International Conference on Advanced Communication Technology*, Feb 17-20, 2008 Phoenix Park, Korea. Proceedings ISSN 1738-9445, ISBN 978-89-5519-135-6, Vol. II, p865.

Huang, Xu and Sharma, Dharmendra Quantum Key Distribution for Wi-Fi Network Security, I*EEE International Conference on Circuits & Systems for communications*, 26-28 May 2008, Shanghai, China. Accepted.

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

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

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

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

Sen Xu, Manton Matthews, Chin-Tser Huang, Security Issues in Privacy Key Management Protocols of IEEE 802.16, *ACM SE'06*, March 10-12, 2006, Melbourne, Florida, USA, pp113-118.

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

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

Multiagent Systems

Edited by Salman Ahmed and Mohd Noh Karsiti

ISBN 978-3-902613-51-6
Hard cover, 426 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

Multi agent systems involve a team of agents working together socially to accomplish a task. An agent can be social in many ways. One is when an agent helps others in solving complex problems. The field of multi agent systems investigates the process underlying distributed problem solving and designs some protocols and mechanisms involved in this process. This book presents an overview of some of the research issues in the field of multi agents. It is a presentation of a combination of different research issues which are pursued by researchers in the domain of multi agent systems as they are one of the best ways to understand and model human societies and behaviours. In fact, such systems are the systems of the future.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821