2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery

Fuzzy Dynamic Switching in Quantum Key Distribution for Wi-Fi Networks

Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma
Faculty of Information Sciences and Engineering
University of Canberra, ACT 2601
Australia

{Xu.Huang, Shirantha.Wijesekera, Dharmendra.Sharma}@canberra.edu.au

Abstract

It is the fact that wireless networks have become one of the most widely used communication systems in the world due to the wireless network's natures. However, at the same time providing secure communication for wireless networks has become one of the prime concerns. There are many ways to improve security issues, one of them, titled quantum cryptography, namely quantum key distribution (QKD), offers the promise of unconditional security. It is well known that traditional QKD can work well in the traditional networks because of the full optical system will meet the requirement of photon communication, which becomes serious problem in wireless communication system, as in free space photon transmission is the difficulty in providing line-of-sight (LOS) between the transmitter and the receiver for long distances. In this paper, we are going to focus on two dimensional (2D) fuzzy dynamic switching between the transmitter and the receiver for reasonable long distances. The research results show fuzzy dynamic switching has potential capability to carry on this project and the future papers will follow for 3D cases.

1. Introduction

As the wireless communication has gone through rapid advancements during the last few decades, an increasing number of government agencies, businesses and home users are either using, or considering using, wireless technologies in their environments [1, 4, 24]. Therefore it is the fact that in the near future wireless technology will dominate the communication industry. While wireless networks and its applications are becoming popular every day, security issues associated with have become a great concern. In this paper we are going to make a novel protocol with a method to create an implementation of quantum cryptography for key distribution in Wi-Fi networks.

As wireless communications use the airwaves, they are intrinsically more vulnerable to interceptions and attacks than their wired counterparts. As the service become more popular, there are a great number of security risks associated with the current wireless protocols and encryption methods [6, 8]. Some of the common types of attacks against wireless networks are; Denial of Service (DoS) attacks, Identity theft (MAC spoofing), Man-in-the-middle attacks, ARP poisoning, etc. DoS attacks are typically associated with 802.11 wireless communications [24].

Based on the laws of physics, quantum cryptography allows exchange of cryptographic key between two remote parties with unconditional security. Quantum cryptography is used to produce and distribute a key, known as Quantum Key Distribution (QKD). Several QKD protocols such as BB84, B92 [20] and six-state [18] exist in optical communications, in particular with optical fiber systems, as of now. Out of those, BB84 is more popular and widely used in practical networks [25]. As the nature of BB84 and B92 [18, 20, 21] we have chosen a variation of BB84 called SARG04 (Scarani, Acin, Ribordy, and Gisin) [21] to employ in our current work. SARG04 is robust against photon-number splitting (PNS) attack [21]. Explaining how SARG04 protocol works is not in scope of this paper. QKD has gone through significant advancements in optical networks [17, 19]. However, QKD with respect to free-space is showing rather slow progress. One of the main reasons for this slow progress in free space photon transmission is the difficulty in providing Line-Of-Sight (LOS) between the transmitter and the receiver for long distances. However, there are some papers discussed this issue, we may use different models for different situations of the multi-path communication channels, such as almost-LOS (ALOS), quasi-LOS (QLOS), non-LOS (NLOS) with responding statistic distributions, which will not be discussed in our current paper.

In our work, we target the IEEE 802.11 wireless network to integrate with quantum cryptography with fuzzy logic control. This is because the coverage area of 802.11 network small, the line-of-sight issue between the participating entities can be minimized. Therefore, currently we assume the LOS problem is not major concern in this paper.

In this paper we are focusing on how to deal with LOS problem with Fuzzy logic method. Next we shall discuss IEEE 802.11i standard then we highlight our QKD system, by which LOS problem will occur. In the section IV we show our fuzzy

978-0-7695-3735-1/09 $25.00 © 2009 IEEE
DOI 10.1109/FSKD.2009.546

system for switching. The conclusion will present in section V.

2 IEEE 802.11i Standard

Before we introduce our new protocol, we need to have a closer look at IEEE 802.11i standard as some of which shall be introduced into our current work. The security of 802.11 is defined by Wired Equivalent Privacy (WEP). However WEP was identified by cryptanalysts to have severe security weaknesses. As a result of this, an amendment to the IEEE 802.11 standard called IEEE 802.11i [3] was approved in 2004.

IEEE 802.11i is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. It defines two classes of security algorithms: Robust Security Network Association (RSNA) and Transition Security Network (TSN). IEEE 802.11i describes two new confidentiality algorithms to address those two cipher suites, namely Temporal Key Integrity Protocol (TKIP) and Counter-mode/CBC-MAC Protocol (CCMP) respectively [12]. 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) [13] to allow a wide variety of authentication mechanisms, which we are going to keep it in our current work. The EAP integration with QKD will be discussed in the next section.

RSNA defines two types of key hierarchies to divide initial key material into useful keys. The two key hierarchies are: Pairwise key hierarchy, which is used to protect unicast traffic and, Group key hierarchy which is used to protect multicast and broadcast traffic. We can show the simplified block diagram of a point-to point QKD link in concept in Figure 1.

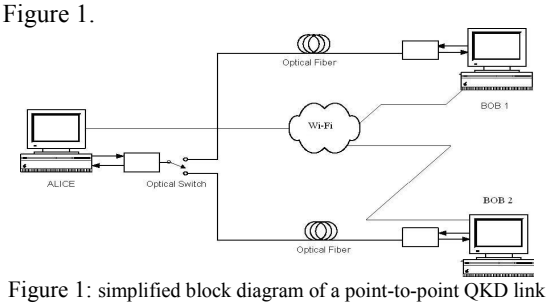


Figure 1: simplified block diagram of a point-to-point QKD link in concept[23].

3. QKD for Wireless Networks

Quantum cryptography or QKD is one area that did not get enough attention in wireless networks so far with respect to providing secrete key distribution. Even though there are lots of things need to be investigated before this technology applies to the real world. Our current work is part of the contributions toward to the final successful target. In this section we are going to build a bridge between QKD and wireless networks.

In 802.11i networks there are two places where the mutual authentication can be employed. Firstly, by selecting a correct EAP type such as EAP-TLS, EAP-TTLS that offer mutual authentication during IEEE 802.1X authentication process. Secondly, the IEEE 802.11i 4-way handshake makes the mutual authentication happens in second and third messages. In the second message of 4-way handshake, authenticator receives the reply and message integrity code (MIC) from the supplicant. Authenticator checks the received and calculated MIC values to authenticate the Supplicant. In the third message, Authenticator sends the calculated MIC to the Supplicant. Supplicant then checks the MIC to authenticate the Authenticator, achieving mutual authentication.

In our work, we paid special attention on the stage where the mutual authentication takes place in 802.11i networks. Therefore, we shall take the advantage of EAP types such as EAP-TLS, EAP-TTLS which offer mutual authentication, to merge 802.11i networks with QKD. In order to make QKD well match wireless communications, i.e. our aim is to introduce quantum key transmission soon after the 802.1X authentication is completed. The proposed protocol is shown in figure 2.

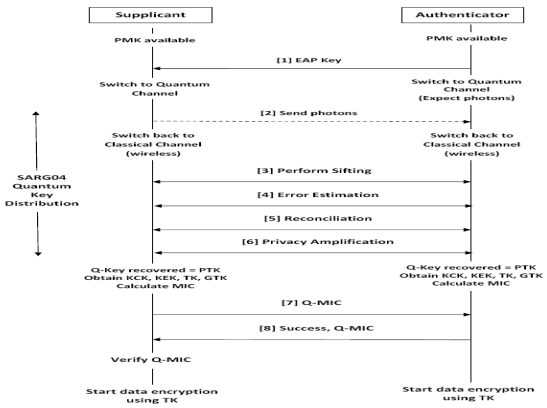


Figure 2: The Proposed Protocol [22]

As described in flow 13 of figure 1, the last message of 802.1X protocol is the EAPOL message giving the EAP Key from Authenticator to the Supplicant. Since the two parties are mutually authenticated at this stage, we know that 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 soon as the Supplicant receives the EAP Key message, the communication switches to quantum channel.

Once the photon transmission finishes, the communication switches back to classical wireless channel. Afterwards they complete the SARG04 quantum key exchange as shown in flows 3 to 6 of

Figure 2. Some of the transferred bits will get discarded during the final key recovery process of SARG04 protocol. Our next aim is to set the length of Q-Key equal to the length of PTK. For example, CCMP, PTK is 256 bits, while TKIP occupies 384 bits for PMK. So that we have to make sure the derived Q-Key will contain bits greater than or equal to the number of bits of PTK. We get this stripped Q-Key as the PTK.

Then from PTK, we can derive KEK, KCK and TK, while from KCK, MIC can be calculated. We shall use this MIC in our subsequent protocol messages to implement mutual authentication. In order to simplify the operation in wireless networks 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) and make the following protocol:

Q-MIC = (*MIC*) XOR (*first bits of PMK equivalent*

to the length of MIC)

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 use the GTK for multicast applications if needed.

Recent research work explores some of the flaws of 4-way handshake [5, 6, 8, 16]. It was shown that the message 1 of 4-way handshake is subject to DoS attacks. For example, intruders can flood message 1 to the supplicant after the 4-way handshake has completed, causing the system to fail. Since key distribution of our protocol is done by the SARG04 protocol.

In order to under our protocol let's assume an eavesdropper send a fake photon transmission towards Authenticator soon after the EAP Key message (flow 2 of Figure 2). Then once the Q-Key is derived by SARG04 process, supplicant sends Q-MIC to Authenticator in flow 7. Authenticator can check this Q-MIC value as it has all the ingredients to generate its own Q-MIC.

4. Fuzzy Switching System in QKD

It is clear, from above description, that the photon communication becomes a vital issue in QKD. For the 802.11 networks, even it has a reasonable good area covering the communications but for QKD it would be a problem to "just" transmitter right hitting receiver, which is called "LOS" problem. We propose a 2D fuzzy switching system as shown in this section to tentatively run our system, which shows that the dynamic switching has good potential for our system. The future 3D system will follow in our next paper.

The fuzzy decision problem introduced by Bellman and Zadeh [26] has as a goal the maximization of the minimum value of the membership functions of the objectives to be optimized. Accordingly, the fuzzy optimization model can be represented as a multiobjective programming problem as follows:

$$Max \min\{\mu_s(D)\} \& \min\{\mu_l(U_l)\} \ \forall s \in S \ \& \ \forall l \in L$$

$$\text{such that } A_l \le C_l \qquad \forall l \in L,$$

$$\sum_{r \in R_p} x_{rs} = 1 \qquad \forall p \in P \ \& \ \forall s \in S,$$

$$x_{rs} = 0 \text{ or } 1 \qquad \forall r \in R \ \& \ \forall s \in S$$

In above equation, the objective is to maximize the minimum membership function of all delay, denoted by *D*, and difference between the recommend value and the measured value, denoted by *U*.

The control system is shown in Figure 3. The first estimated angle is input and then the set motor controller will run follow the feedback values from the photon receiver & comparing. The outputs are three: anti-clock (or called "negative"); no change (or called "zero"); and clockwise (or called "positive"). There are two ranges are defined, namely "negative" = -100 to 0.0) and "positive" = 0.0 to +100.

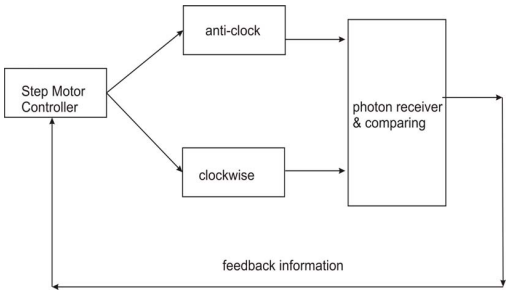


Figure 3: Control system

There are two inputs for this control system, namely (1) the "difference" of the angles between the existed value and the measured value, which is for the step motor to just the transmitter and receiver direction. When those two values are perfectly matching, the LOS is recognized and this "difference" ideal value would be zero. (2) the "differential" of the angles that describe how "quickly" to get the angles changed and in which direction changing (anti-clock or clockwise directions). Those two inputs are shown in Figure 4 with some values we have used in our testing.

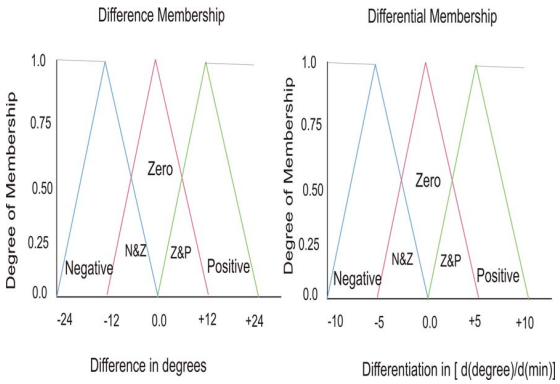


Figure 4: Degree of Memberships for the two input in our fuzz control system.

For the rule structure and matrix, we have:

1. If the existed angle value – measured value = negative and d(existed angle value –measured value)/dt = negative THEN output = anti-clock turn
2. If the existed angle value – measured value = zero and d(existed angle value –measured value)/dt = negative THEN output = clockwise turn
3. If the existed angle value – measured value = positive and d(existed angle value –measured value)/dt = negative THEN output = anti-clock turn
4. If the existed angle value – measured value = negative and d(existed angle value –measured value)/dt = zero THEN output = anti-clock turn
5. If the existed angle value – measured value = zero and d(existed angle value –measured value)/dt = zero THEN output = no change (zero)
6. If the existed angle value – measured value = positive and d(existed angle value –measured value)/dt = zero THEN output = clockwise turn
7. If the existed angle value – measured value = negative and d(existed angle value –measured value)/dt = positive THEN output = anti-clock turn
8. If the existed angle value – measured value = zero and d(existed angle value –measured value)/dt = positive THEN output = anti-clock turn
9. If the existed angle value – measured value = positive and d(existed angle value –measured value)/dt = positive THEN output = clockwise turn

Therefore, we have the matrix from the nine rules to as shown in below:

Differential \ Difference	N	Z	P
N	AC	CW	CW
Z	AC	NC	CW
P	AC	AC	CW

where AC= anti-clock direction; CW=clockwise direction and NC= no change (or zero).

As an example, we have two inputs say "difference" = -6 and "differential" = +2.5, as shown in Figure 5.

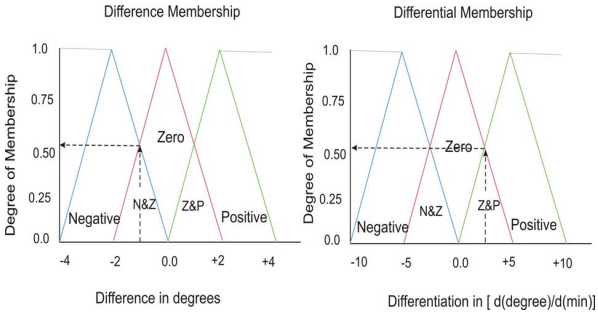
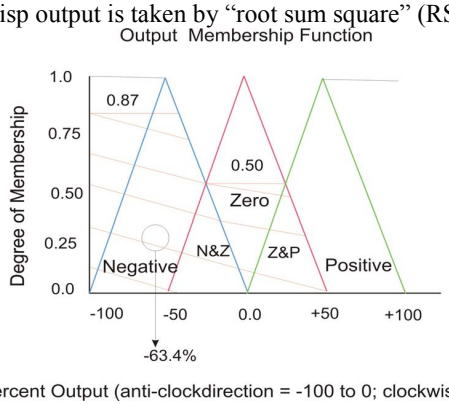


Figure 5: An example for the fuzzy calculation. Two inputs say "difference" = -6 and "differential" = +2.5.

The calculation result is -63.4% anti-clock direction as shown in Figure 6 and defuzzification process for crisp output is taken by "root sum square" (RSS).



Some final testing results are shown in below:

1. Two inputs: "difference" = -3 and "differential" = +1.25 then output = -55.1% anti-clock direction;
2. Two inputs: "difference" = 0 and "differential" = +2.5 then output = -50.1% anti-clock direction;
3. Two inputs: "difference" = +3 and "differential" = +2.5 then output = -10.8% anti-clock direction;
4. Two inputs: "difference" = +1 and "differential" = +2.5 then output = +12.1% clockwise direction;

The dynamic control system works and the result is fairly reasonable, which gives the enough photon to be communicated by the wireless channel.

5. Conclusions

Risks are inherent in wireless technology. Most significant source of risks in wireless networks is that the technology's underlying communication medium, the airwave, is open to intruders. Due to

this reason a lot of efforts have been put to address security issues in wireless networks.

The advantage of quantum cryptography over traditional key exchange methods is that the exchange of information can be shown to be secure in a very strong sense, without making assumptions about the intractability of certain mathematical problems. But the LOS problem becomes one of major barriers in this application. In our work, we take advantage of fuzzy logical control in our designed QKD system to merge with IEEE 802.11i wireless network. We have noted the there is huge potential capability to carry on this project and the future papers will follow for 3D cases due to the conference paper size.

6. References

[1] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, "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.

[2] ANSI/IEEE 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[3] IEEE Std 802.11i, IEEE Standard for Information Technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control O(MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[4] IEEE Std 802.1X, 2004, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control

[5] Changhua He, John C Mitchell, Analysis of the 802.11i 4-way Handshake

[6] Floriano De Rango, Dionogi Lentini, Salvatore Marano, Statis and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i, June 2006.

[7] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, "Quantum Cryptography for Wireless Network Communications," IEEE International Symposium on Wireless and Pervasive Computing, 11-13th February 2009, Melbourne, Australia, ISBN: 978-1-4244-2966-0, Security pp.1-pp5.

[8] Changhua He, John C. Mitchell, Security Analysis and Improvements for IEEE 802.11i.

[9] Thi Mai Trang Nguyen, Mohamad Ali Sfaxi, Solange Ghernaouti-Helie, 802.11i Encryption Key Distribution Using Quantum Cryptography, 2006.

[10] Yang Xiao, Jie Li, Yi Pan, 2005. Security and Routing in Wireless Networks,

[11] Bob O'Hara, Al Petrick, IEEE 802.11 Handbook, A Designer's Companion,2005.

[12] D. Whiting, R. Housley, N. Ferguson, Request for Comments: 3610, Counter with CBC-MAC (CCM), September 2003

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, , RFC – 3748, Extensible Authentication Protocol (EAP), 2004

[14] Matthias Scholz, Quantum Key Distribution via BB84, An Advanced Lab Experiment, August 2005

[15] Kenneth G. Paterson, Fred Piper, Rudiger Schack, Why Quantum Cryptography? , June, 2004.

[16] ChangHua He, John C. Mitchell, 1 Message Attack on the 4-Way Handshake, May 2004.

[17] http://www.computerworld.com/securitytopics/security/story/0,10801,96111,00.html , Quantum cryptography gets practical

[18] Dagmar Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Physical Review Letters, 81.3018, October 1998.

[19] M.S. Goodman, P. Toliver, R.J. Runser, T.E. Chapuran, J. Jackel, R.J. Hughes, C.G. Peterson, K. McCabe, J.E. Nordholt, K. Tyagi, P. Hiskett, S. McNown, N. Nweke, J.T Blake, L. Mercer, H. Dardy, Quantun Cryptography for Optical Networks: A Systems Perspective.

[20] C.H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[21] Valerio Scarani, Antonio Acin, Grégoire Ribordy and Nicolas Gisin, Quantum cryptography protocols robust against photon number splitting attcks

[22] Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, "Novel Protocol for Quantum Cryptography of Secure in Wireless Communications," the IEEE 11th International Conference on Advanced Communication Technology, February 15-18, 2009, Phoenix Park, Korea. ISBN: 978-89-5519-139-4, pp 913-918.

[23] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, "Implementation of QKD in 802.11 Networks," accepted by NSWCTC2009, Wuhan, P.R.China, 24-25, April 2009. Accepted.

[24] Tom Karygiannis, Les Owens, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, NIST, Special Publication 800-48, November 2002.

[25] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, Harald Weinfurter, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. 98, 010504, January 2007.

[26] H R. Bellman and L.A. Zadeh, Decision-making in a fuzzy environment, Management Science 17 (1970) 141-164.