QUANTUM CRYPTOGRAPHY BASED KEY DISTRIBUTION IN WI-FI NETWORKS

Protocol Modifications in IEEE 802.11

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

Keywords: Quantum Key Distribution (QKD), Wi-Fi, IEEE 802.11, Wireless Security.

Abstract: Demand for wireless communications around the world is growing. IEEE 802.11 wireless networks, also known as Wi-Fi, are one of the popular wireless networks with over millions of users across the globe. Hence, providing secure communication for wireless networks has become one of the prime concerns. We have proposed a Quantum Key Distribution (QKD) based novel protocol to exchange the encryption key in Wi-Fi networks. In this paper, we present the protocol modifications done in the existing IEEE 802.11 standard to implement the proposed QKD based key exchange.

1 INTRODUCTION

Wireless Local Area Networks (WLAN) brings great benefit to people due to their enhanced mobility, low cost and capabilities of rapid development etc. IEEE 802.11, is the wireless local area network standard (IEEE 802.11, 2003) developed by the IEEE LAN/MAN Standards Committee. It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. Wi-Fi (Wireless Fidelity) is a term for certain types of WLAN that use specifications of the 802.11 family.

The security of 802.11 is defined by Wired Equivalent Privacy (WEP). WEP was identified by cryptanalysts to have severe security weaknesses in the way it handles authentication and privacy. As a result, an amendment to the IEEE 802.11 standard called IEEE 802.11i (IEEE 802.11i, 2004) was approved in 2004.

Due to its popularity and the nature of the communication being wireless, Wi-Fi networks are vulnerable to security attacks than its wired counterparts. Therefore it is possible for an attacker to snoop on confidential communications or modify them to gain access to the wireless networks more easily.

In our previous research work (Xu Huang, et al, 2009), (Shirantha W. et al, 2009), (Xu Huang, et al, 2008), we have described a novel protocol based on Quantum Cryptography for the exchange of key that used to encrypt data in IEEE 802.11i networks. The key exchange of IEEE 802.11i is done by the process called 4-way handshake. In this new protocol, we have replaced this 4-way handshake with QKD to exchange the key and obtain the key hierarchy that used for subsequent secure data communication.

In order to accomplish this, we have proposed some modifications to the existing IEEE 802.11i protocol. In doing so, a special attention has been paid to minimise the impact on the existing protocol. Thus, in our changes, we reuse some of the existing fields of frames to represent new values for QKD. This paper describes the implementation of QKD based key exchange process by using the same frame formats of existing IEEE 802.11i protocol.

This paper comprises of 6 sections. This section gives an overview of the project. Sections 2 discuss the advantages of using QKD in Wi-Fi networks. Proposed QKD based protocol is described in section 3. Section 4 describes the required protocol changes and new fields, their parameters etc. Experimental results are given in section 5, while we conclude the paper in section 6. Acknowledgements and references follows.

Wijesekera S., Huang X. and Sharma D. (2010).
QUANTUM CRYPTOGRAPHY BASED KEY DISTRIBUTION IN WI-FI NETWORKS - Protocol Modifications in IEEE 802.11.
In *Proceedings of the 5th International Conference on Software and Data Technologies*, pages 146-151
DOI: 10.5220/0003008901460151

2 USE OF QKD IN IEEE 802.11 NETWORKS

As mentioned earlier, wireless networks are vulnerable to various types of security attacks. Some of the common types of attacks against wireless networks are; Denial of Service (DoS) attack, Identity theft (MAC spoofing), Man-in-the-middle attack, ARP poisoning, Network injection, Caffe Latte attack etc.

Based on the laws of physics, quantum cryptography allows exchange of cryptographic key between two remote parties with unconditional security. The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. The process of using quantum cryptography to distribute the key is known as Quantum Key Distribution (QKD). Several QKD protocols such as BB84 (Bennett, C. H., et al, 1984), B92 (C.H. Bennett, 1992), SARG04 (Valerio Scarani, et al., 2004) and six-state (Dagmar B., 1998) etc exists as of now. There is lots of research work in progress in QKD area and even commercial fibre optic QKD networks exits as of now (HP - Quantum Cryptography, 2009), (Computer World, 2004), (SECOQC, 2008).

Since QKD offer unconditional secure key distribution, it is worthwhile investigating the possibility of using QKD in wireless networks. In IEEE 802.11i networks, 4-way handshake process is used to exchange the secrete key and obtain the key hierarchy to establish secure communication. It was found that 4-way handshake process is subject to security attacks (Floriano De Rango, et al, 2006), (Changhua He, et al, 2005). The exact place to get QKD involved in the key exchange of Wi-Fi networks is the 4-way handshake process.

In QKD, the transmitter (Alice) sends the key as a series of polarized photons via quantum channel towards the receiver (Bob). Bob measures these photons using randomly selected bases to generate his version of the key. Once the photon transmission is over, the rest of the communication takes place in public channel (eg: internet, wireless). This process has been split into 4 main stages: *Sifting, error estimation, reconciliation* and *privacy amplification*. These 4 stages help Alice and Bob to recover identical "unconditionally" secure key to be used for the subsequent data encryption. This process is shown in Figure 1. Full explanation of the key recovery process of QKD is not in scope of this paper.

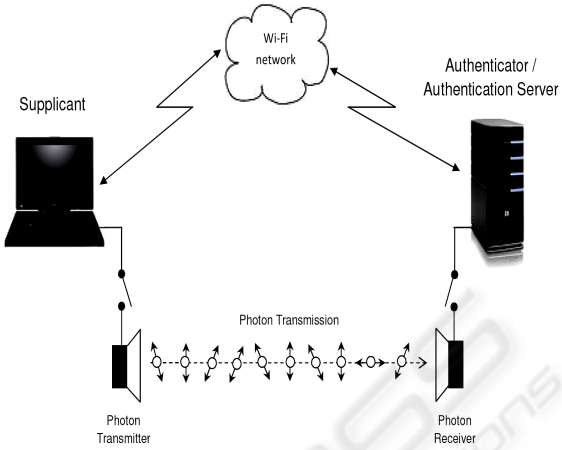

Figure 1: Quantum Key Distribution in Wi-Fi.

3 THE PROPOSED PROTOCOL

In this approach, our aim is to introduce quantum key transmission soon after the 802.1X authentication is completed. The proposed protocol is shown in figure 2.

At the end of the IEEE 802.1X authentication in IEEE 802.11i, both supplicant and authenticator hold a key known as Pairwise Master Key (PMK). Our aim is to obtain the IEEE 802.11i key hierarchy as shown in Figure 3. In the existing IEEE 802.11i, a Pseudo Random Function (PRF) is applied by the 4-way hand shake process to obtain Pairwise Transient Key (PTK). The PTK is then divided into three keys. The first key is the EAPOL-key confirmation key (KCK). The KCK is used by the EAPOL-key exchanges to provide data origin authenticity. KCK is also used to calculate Message Integrity Code (MIC). The second key is the EAPOL-key encryption key (KEK), which is used to provide data confidentiality. KEK is also used to encrypt the Group Temporal Key (GTK). The third key is the Temporal Key (TK), which is used by the data-confidentiality protocols to encrypt unicast data traffic.

The last message of IEEE 802.11X authentication is the EAPOL message giving the EAP Key from Authenticator to 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.

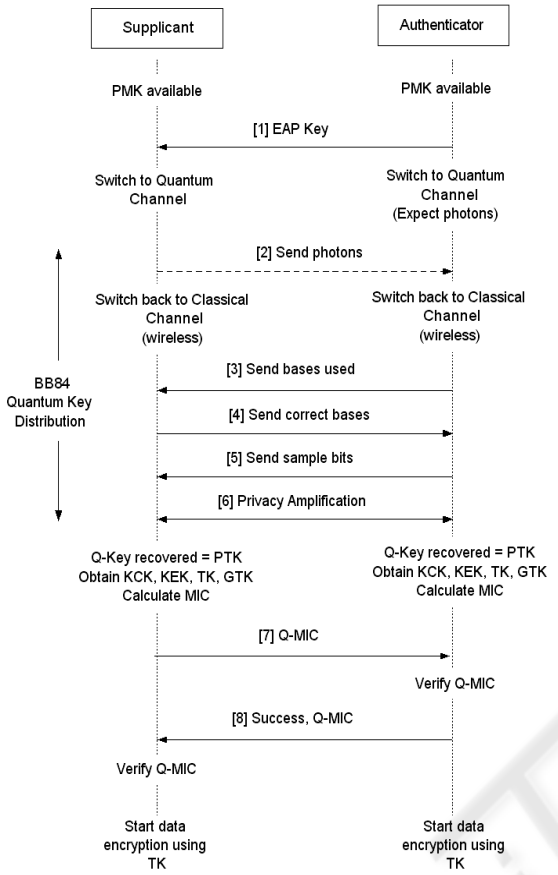

Figure 2: The QKD Based Wi-Fi Proposed Protocol.

Supplicant starts QKD 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 rest of the QKD process as shown in flows 3 to 6 in Figure 2. At the end of the QKD process, both Supplicant and Authenticator hold a unique common key (Bennett, C. H., et al, 1984), which we call as Quantum Key (Q-Key).

In QKD, the length of the final key cannot be known before the quantum transmission. Therefore the final key derived will be of varying length. Our aim is to set the length of Q-Key equal to the length of PTK. The IEEE 802.11i standard uses two encryption protocols known as Counter-mode/CBC-MAC Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP). For CCMP, PTK is 256 bits, while TKIP occupies 384 bits for PTK. Therefore, we have to make sure the derived Q-Key will contain bits greater than or equal to the number of bits of PTK. Thus, at this stage we strip the extra bits of Q-Key so that it will have same length as PTK. We get this stripped Q-Key as the PTK. Once PTK is known, the IEEE 802.11i key hierarchy, as in figure 3, can be retrieved.

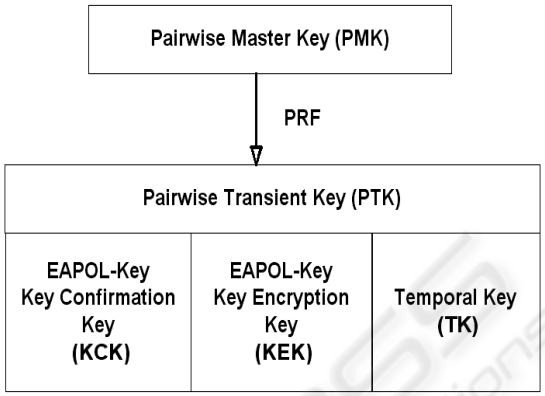

Figure 3: Key Hierarchy of IEEE 802.11i.

We use the derived MIC in our subsequent protocol messages to implement data integrity. At this stage, Supplicant performs XOR operation with the MIC and PMK. We call this resulted MIC as Quantum MIC (Q-MIC).

Q-MIC = (MIC) XOR (PMK)

The Supplicant then sends the Q-MIC to Authenticator as shown in flow 7 of Figure 2.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 the Supplicant as shown in flow 8 of Figure 2. 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.

4 MODIFICATIONS TO EXISTING PROTOCOL

IEEE 802.11 standard specifies changes in physical and MAC layers of OSI protocol stack. Hence our proposed modifications to implement QKD too are applied to the same two layers. Special attention has been made to minimise impact to the existing IEEE 802.11i protocol. Careful analysis of the existing IEEE 802.11i protocol shows that the communication flows of 4-way handshake process can be altered to implement the QKD based key

exchange. Some of the fields used by 4 way handshake in EAPOL frames are altered to occupy QKD information. The changes are made to the IEEE 802.11i standard without interrupting the existing frame formats.

IEEE 802.11 uses EAPOL-Key frames to exchange information between Supplicants and Authenticators. Hence the proposed modifications to implement QKD too are done through EAPOL-Key frames. Since we are not using 4-way handshake process, the fields used for the same have been modified to carry QKD specific information. In addition some of the unused fields too have been used. Figure 4 shows the modified EAPOL packet frame.

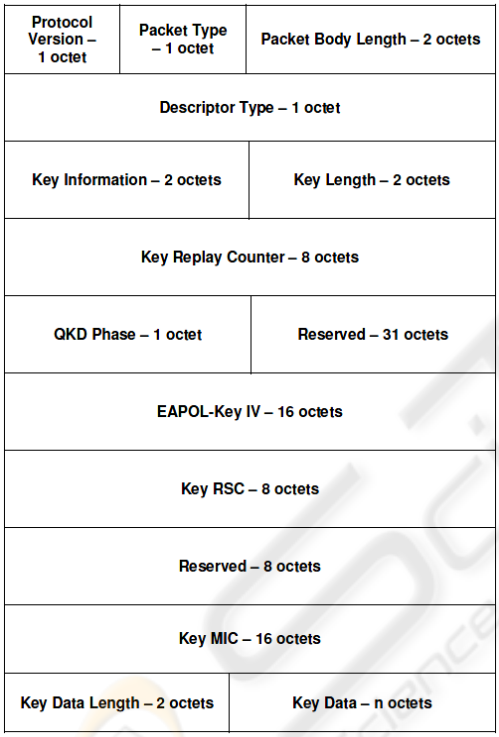

Figure 4: EAPOL-Key Frame with QKD changes.

The "Key Nonce" field used in IEEE 802.11 has been renamed as "QKD Phase". It is used to indicate 4 phases of QKD processes in progress at a given instance.

Below are the values that this "QKD Phase" field can have.

0000 0001: *Sifting*
0000 0011: *Error estimation*
0000 0101: *Reconciliation*
0000 0111: *Privacy Amplification*

Bulk of the processing happens during reconciliation phase. In this phase, the raw key is divided into several blocks to perform parity checks. The QKD Phase field is set to 0000 0101 and the Key Data field carries the parity check information.
The format of Data field:

<Block Number | Sub-Block Level | Parity Check Results>

Where:

Block Number. Number of the main block.
Sub-block Level: If the parity check of main block failed, it will be bisected and perform parity check on each sub-block. The "Sub-block Level" field specifies the level of bisection of each main block. If the main block is bisected once, Sub-block Level =2 and so on.

Sub-block Partition Number. Whenever a mismatch in parity of block/Sub-block is observed, that particular block/Sub-block is bisected. This Sub-block Partition Number field holds the partition number of each sub-block.

Parity Check Result. This field holds the result of parity check.

0: parity result (odd parity).
1: parity result (even parity).

Figure 5 shows the allocation of bytes within the Key Data field.

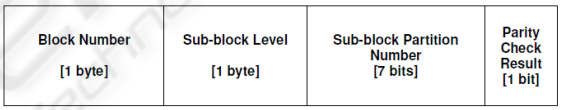

Figure 5: Key Data field values of EAPOL frame during reconciliation phase of QKD.

5 EXPERIMENTAL RESULTS

IEEE 802.11 standard defines Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless LANs (IEEE Std 802.11, 2007). Since the changes we made under the new QKD protocol are directly on the Physical and MAC layers, it is really difficult to rewrite those layers from scratch to reflect the changes within the research time frame. Therefore, the best possible way of implementing the new protocol is by simulation. The QKD processing has been coded using C++ language. For simulation, we have chosen Simulink as it provides S-Functions to incorporate C++ programs to provide simulations.

5.1 The Simulink Model

As mentioned, the QKD implementation in our

model has been done in C++. We use Simulink S--Functions to implement and simulate the results.

The main functionalities of each of the four phases of QKD have been identified in programming point of view as below:

Sifting: Construct a buffer containing the bit stream once the photon transmission is finished, Supplicant to inform the bases it used, Authenticator to reconstruct its buffer contents that matches the bases received from Supplicant.

Error Estimation: Supplicant to send a set of sample bits from its key, Authenticator to compare those bits and calculate the error rate, Authenticator to decide if the error rate is acceptable or not (based on the threshold level), Inform Supplicant about the decision, Proceed to next phase if the error rate is acceptable, reattempt photon transmission otherwise.

Reconciliation (Assuming "parity check" is used as the reconciliation method): Split the key into blocks, compare parity of each block, Split those blocks whose parity is mismatched, Perform parity check on those sub blocks until the error is found, Continue till all the errors are located and eliminated.

Privacy Amplification: Apply pre-defined hash function to the remaining key to eliminate possible leak of bits to outsiders.

For each phase, these functionalities have been implemented using C++ as several subsystems. During each phase, the communication is carried out between respective peer sessions of Authenticator and Supplicant.

During Sifting, Error Estimation and Privacy Amplification phases of QKD, the new protocol consumes fewer resources as it only needs few comparisons to be done. Bulk of the processing happens during Reconciliation phase. It needs few additional communication flows to obtain the final secured key. The number of additional steps depends on the type of reconciliation method such as CASCADE (Gilles B et al, 1994), WINNOW (Buttler W.T., 2003) etc, used.

In addition, we shall save several key refresh cycles that happens during existing IEEE 802.11 communication. In this new protocol, key refreshing is not required as the key obtained via QKD is proven to be unconditionally secure.

5.2 Analysis of QKD Solution for Key Exchange

In addition to the unconditional security achieved, the simulation analysis of QKD approach shows several other advantages. Main area of modifications applied to the existing protocol is the 4-way hand shake process. The first stage of QKD (sifting) only requires single EAPOL communication flow involving STA informing AP about the bases it used. Results show that there is no significant amount of processing needed as opposed to the nonce value calculations involved in the existing protocol.

The second stage of QKD process (error estimation) is implemented by two EAPOL communication flows. The first flow is to transmit bit sample while the second to inform the result. In this step too results shows that both STA and AP consume only small amount of processing power. At AP side it only performs simple bit comparison on a bit stream of small length.

The third stage (Reconciliation) is the stage where majority of processing takes place. The number of communication flows happen in this stage is depending on the reconciliation protocol used. We have implemented the parity check method. Parity check method involves more computations when compared to other existing reconciliation protocols such as Cascade or Winnow. Our choice of parity check method is to see the results in the worst case scenario.

The final stage of QKD (privacy amplification) involves just a single EAPOL frame, which does not requires much processing power at either end.

When compared to the existing protocol, it could be seen that only the reconciliation process is taking few additional EAOPL flows. However, the key exchanged in the existing protocol needs to be refreshed at regular intervals to maintain security of data encryption. But in the QKD based protocol, such key refresh cycles are not needed as the key exchanged provide unconditional security. Hence with this new protocol significant amount of processing time could be saved. Overall, this can compensate to the extra cycles of flows taken during the reconciliation process.

6 CONCLUSIONS

In this work, the changes to accommodate QKD have been done with extreme care so that it will have minimum impact to the existing IEEE 802.11 protocol. The main advantage of this protocol modification is that no major frame level changes are needed. QKD modifications use fields of the existing frames. Both Supplicant and Authenticator are able to identify if they can implement QKD for key exchange at the early stages (by listening to

Beacon). In case, any of the participants are not supporting QKD, they can still move on with the existing protocol.

Further, since the key obtained via this new protocol offer unconditional security, there is no need to refresh keys time to time during communication session. This improves the efficiency of the overall management and control communication significantly.

We regret that we are unable to provide readers with more description on quantum cryptography, QKD process, Wi-Fi network protocols etc due to the page limitations enforced by the conference guidelines.

ACKNOWLEDGEMENTS

We would like to take this opportunity to appreciate University of Canberra, Australia for the URG supports.

REFERENCES

IEEE 802.11 (2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

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

Shirantha Wijesekera, Xu Huang, and Dharmendra Sharma, 2009. "A Novel Protocol using Quantum Cryptography for Secure Communication in 802.11 Networks," *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks* (WoWMoM 2009), Kos, Greece.

Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, 2008. "Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks," *IEEE the 10th International Conference on Advanced Communication Technology,* Korea. Proceedings ISSN 1738-9445, ISBN 978-89-5519-135-6, Vol. II, p865.

IEEE Std 802.11i (2004), 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.

Bennett, C. H. and Brassard, G. (1984), "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.

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

Valerio Scarani, Antonio Acin, Grégoire Ribordy and Nicolas Gisin (2004), Quantum cryptography protocols robust against photon number splitting attcks.

Dagmar Bruß (1998), Optimal Eavesdropping in Quantum Cryptography with Six States, *Physical Review Letters*, 81.3018.

Computer World (2004), Quantum cryptography gets practical, http://www.computerworld.com/s/article/96111/Quantum_cryptography_gets_practical.

Hewlett-Packard - Quantum Cryptography (2009), http://www.hpl.hp.com/research/about/quantum_cryptography.html.

SECOQC (2008) , Development of a Global Network for Secure Communication based on Quantum Cryptography, http://www.secoqc.net/.

Floriano De Rango, Dionogi Lentini, Salvatore Marano (2006) , Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i .

Changhua He, John C. Mitchell (2005), Security Analysis and Improvements for IEEE 802.11i.

IEEE Std 802.11 (2007), IEEE Standard for Information Technology – Amendment 6: Medium Access Control (MAC) Security Enhancements.

Gilles Brassard, Louis Salvail, Secret-Key Reconciliation by Public Discussion, SBN 978-3-540-57600-6, 1994.

W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, Fast, Efficient error reconciliation for quantum cryptography,2003.