Effective Key Authentication for Ieee 802.11 Networks using Quantum Cryptography

G.Murali
Asst. Professor
Dept of CSE
J.N.T.U.A.C.E.P
Andhra Pradesh
INDIA

R.Siva Ram Prasad
Research Director
Dept of CSE
Acharya Nagarjuna University
Andhra Pradesh
INDIA

V.Swetha Madhavi
M.Tech
Dept of CSE
j .N.T.U.A.C.E.P
Andhra Pradesh
INDIA

ABSTRACT
Wireless networks are growing tremendously and their applications are also becoming prominent from day to day [5]. As wireless applications are becoming popular, the security issues [3] related to 802.11 are also has a great consideration. These are gaining popularity because of their mobility, low cost, convenience and easy establishment. Among many wireless networks, the 802.11 has a large amount of users than compared to the others globally. The key which is used for encrypting and decrypting purpose plays a crucial role between users.
As the wireless networks are open guide medium of wireless communications [3] , there is possibility for hackers to snoop on confidential communications. There is a chance to modify them to gain the access to the wireless networks more easily. In the key distribution of quantum is done according to Heisenberg uncertainty Principle. We will be focusing on Quantum Key Distribution which offers a high level security between two communication parties with the help of novel protocol. We will also focusing on the analysis of experimental results focusing on the different phases of protocol.

Keywords
Quantum cryptography, Heisenberg uncertainty Principle

1. INTRODUCTION
The usage of wireless networks is growing rapidly as it costs is very low. Compared to wired networks the wireless networks can be established any place with in short span of time. Communication industry is developing with the help of new technologies, devices etc. In wireless networks the communication is taken place in open air which has grater possibilities for security attacks. As the number of users are increasing , there is need to safeguard data against the attacks hence the key which is used for encryption plays a crucial role. In the case of 802.11[2] there are many approaches present for key distribution like 4-way handshake [7], which consumes a lot of memory. The Hash chain method will be lacking computation of the client. Cookie mechanism requires more memory and also includes the burden to the client by remembering keys. In order to overcome the disadvantages of various protocols in 802.11 we are using the quantum cryptography for key generation and distribution.Quantum key distribution is based on Heisenberg using Uncertainty principle. Uncertainty principle states that "Knowing or measuring the value of one quantum observable implies an intrinsic uncertainty about the values of some other observables i.e. obtaining some information about an unknown quantum system generally causes a disturbance to the quantum state of that system ". The quantum key distribution will be taken in two channels namely Quantum Channel and Classical Channel. Through Quantum channel, series of polarized photons representing the key bits are sent to the receiver with acceptable QBER (Quantum Bit Error Rate). The classical channel is helpful in retrieving the final key by removing errors introduced during transmission of key.

There are mainly four stages in classical channel for retrieving key. They are Sifting, Error Estimation, Reconciliation, and Privacy Amplification. During the Sifting phase the Supplicant (client/ STA) informs the bases used to authenticator (Access Point or AP). Access point records the bits which are incorrect against the bases. The error Estimation phase they compare the random bits that are mapped randomly from the quantum channel. In Reconciliation phase all the errors that are present in the key are removed. At the end of the reconciliation phase the STA and AP have identical keys. In the privacy amplification phase the Hash Function is applied in order to eliminate the possibility of third party attacks.

2. QUANTUM CRYPTOGRAPHY
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. That's why we very often use the more precise term of quantum key distribution (QKD) [8]. Quantum cryptography (or QKD) solves the secure random key distribution problem and enables the creation of a basic building block for cryptographic applications.

3. WLAN SECURITY FOR 802.11
Wireless Local Area Networks (WLAN) [3][11] are majorly used for home users, for small networks or for networks with low security requirements. With the deployment of wireless networks in business environments and in many institutions are trying to implement security mechanisms that are equivalent to those of wire-based LANs. There is also need for restricting access to legitimate users only. The WLAN physical access is different from access to a wired LAN. Existing wired network have access points like RJ45 connectors that are located inside buildings which are regarded as secured from unauthorized access with the help of such devices as keys and/or badges. A user gaining physical access to the building a plug to the client computer into a network jack is also must.

A wireless access point which is also known as (AP) can be accessed from outside the premises if the signal is detectable. Hence the wireless networks require a secure access to the AP in a different manner from wired LANs. There is importance for isolating the AP from the internal network until authentication is verified. The device which is attempting to connect to the AP must be authenticated. After tshe device is authenticated then the user who uses the device can be authenticated. At this point the user may want a secure channel for communication. The 802.11 standard provides the means to satisfy these security requirements like validation of the access device, user authentication and a secure channel.

4. RELATED WORK

4.1. Quantum key Distribution:

The polarization of photon is mainly used for Quantum cryptography [9] which describes polarized light photons in specific directions. The polarized photon is only detected by a photon filter .If they are not detected by photon filter then photon will be destroyed. This technique will be helpful in forming the basis for the in-built intrusion detection. Intrusion detection Determine the essential quality that users can find a hacker is eavesdropping or has intercepted the message. The users can also determine if the message has been received without any interception.

From PTK, we can derive KEK, KCK and TK, while from KCK, MIC can be calculated. We use this MIC in our subsequent protocol messages to implement mutual authentication. 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-MIC = (MIC) XOR (first bits of PMK equivalent to the length of MIC)

Supplicant then sends Q-MIC to Authenticator as shown in flow 7 of Figure 2.6. Upon receiving Q-MIC, Authenticator verifies the Q-MIC. Since the Authenticator is in possession of all the key hierarchy, it can calculate its own Q-MIC and compares with the one came from the Supplicant. If they match, the Supplicant is authenticated [6].

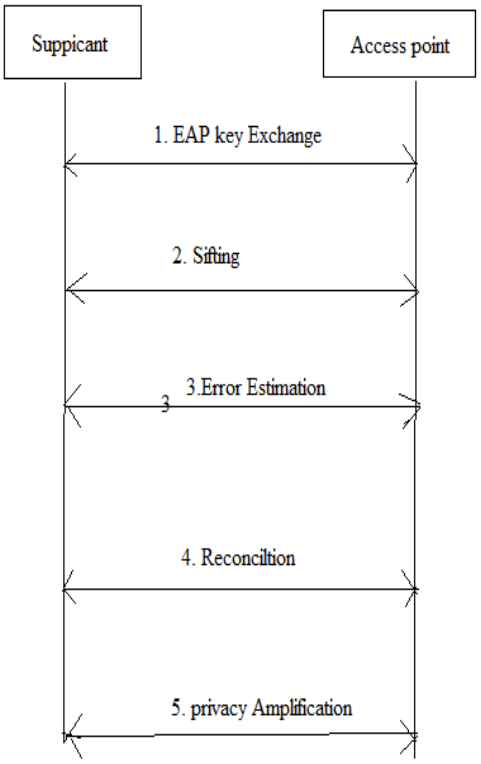

Figure 1: The Proposed Protocol [6]

Recent research work explores some of the flaws of 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. Since key distribution of our protocol is done by the QKD, use of nonce values in the message flows are not required. Present hardware devices for quantum transmission require Line of Sight (LOS) between the Supplicant and the Authenticator in order to transfer photons. However, there has been lot of new advancements happening in this area to
eliminate the requirement of LOS for quantum transmission. One such research work is done by Kedar and Arnon to have Non Line Of Sight (NLOS) system for optical communication by using wireless sensor network. (Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, 2010).

4.2. Novel Protocol Using Quantum Cryptography

Our implementation is twofold: Setting up the quantum channel, implementing the wireless communication. The implementation is currently happening in both streams (hardware and software) in parallel. University of Canberra has past research activities on QKD. During that project, a QKD system was successfully established between university of Canberra and Telstra tower. We choose this hardware setup as our quantum transmission between the Supplicant and Authenticator. We plan to have this hardware set up for a short distance to suit for Wi-Fi networks. We would like to emphasize that we do not pay much attention in converting the present bulky quantum hardware to fit in comparatively small Wi-Fi apparatus. There are lots of new developments taking place to include quantum devices in small gadgets [28]. Our aim in this research is to demonstrate a working QKD based key distribution process for Wi-Fi using the proposed protocol. For simplicity, we use both Authenticator and

Authentication Server as one entity. The high level view of this test set up is shown in Figure 2.7. (Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, 2010).

The Supplicant is running on Windows XP, while the Authenticator/Authentication Server machine is running on Windows Server 2000. We have chosen Microsoft "Native WiFi" product with its user Application Programming Interfaces (API) to be used for software developments. We start from the place where the 802.1X process deliver the PMK to the Authenticator and the Supplicant. At this stage both parties switch to hardware channel to start the photon transmission. Once the photon transmission finishes, they switch back to wireless channel. Both Supplicant and Authenticator store the states of the photons that they used during the communication. (Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, 2010).

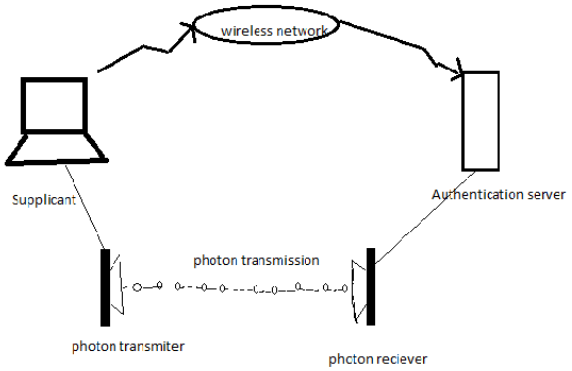

Fig 2: Test set up of QKD based key distribution for Wi-Fi

In the next message, Supplicant sends the bases it used to polarize the photons. Upon receiving the bases, the Authenticator extracts the bits based on the information it has. (We recall that describing the operation of SARG04 is not in scope of this paper). During this stage, the two parties estimate the error introduce during the transmission. This error could result due to atmospheric noise, dark counts in the photon detectors, eavesdropping etc. To estimate this error level, the Supplicant chooses a sample from its key and reveals to the Authenticator. This message frame consist of the start bit position and the length of the sample. The authenticator compares the bits it extracted and if it is below the threshold level, the Authenticator informs Supplicant with Success message to proceed with. Otherwise it sends out Fail message asking the Supplicant to reattempt the Photon transmission. The threshold value for error estimation has been set as a configurable parameter at the Authenticator [1].

Unlike in normal QKD systems, the key used is Wi-Fi is not very long. The maximum length of the key that will be transmitted via quantum link is 256 for CCMP and 384 for TKIP. Therefore the whole key of SARG04 can easily be accommodated into these message flows. Due to this reason, the key exchange does not require any indexing to maintain long keys spanning across multiple files. In our set up, all key manipulations, comparisons etc are done in memory enabling faster operation. 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.

5. CONCLUSION

As wireless Networks are sensitive and easily attacked by intruders we have to be more concern about their security issues. With the help of four way handshake, cookie mechanisms we can provide security for 802.11 networks up to some extent only. These are proven to be not secure under some circumstances. By using Quantum Cryptography we can provide security to much better extent. The four phases of quantum cryptography like sifting, error estimation, Reconciliation and privacy amplification are implanted. We can further extend by doing analysis on each phase.

6. REFERENCES

[1] . Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, "Secure Communication in 802.11 Networks with a Novel Protocol Using Quantum Cryptography", 2010.

[2] Karen Scarfone, Derrick Dicoi, Matthew Sexton and Cyrus Tibbs, "Guide to Securing Legacy IEEE 802.11 Wireless Networks", 2008.

[3] Robert J. Boncella, "WIRELESS SECURITY: AN OVERVIEW", 2002.

[4] Sandra Kay Miller, "Facing the Challenge of Wireless Security".

[5] Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, "Secure Communication in 802.11 Networks with a Novel Protocol Using Quantum Cryptography", 2010.

[6] 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.

[7] Changhua He, John C Mitchell, Analysis of the802.11i 4-way Handshake.

[8] BENNETT, c.H., BRASSARD, ***G.*** BREIDBART, **s.,** and WIESNER, s.: 'Quantum cryptography or unforgeable subway tokens' ***in*** CHAUM, D., RIVEST, R.L., and SHERMAN, A.T. (Eds.): 'Advances in cryptology: Proceedings of Crypto'BZ' (Alenium **Press,** New ***York*** 1983).

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

[10] P. J Edwards The University of Canberra –Telstra Tower Quantum Crypto –Key Telecommunications Link, Advanced Telecommunications and Quantum Electronics Research Centre University of Canberra, 2002.

[11] IEEE Std 802.11, IEEE Standard for Information Technology – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6, 2007.