Quantum Cryptography with Key Distribution in Wireless Networks on Privacy Amplification

R.Lalu Naik [1], Dr.P.Chenna Reddy [2], U.Sathish Kumar[3], Dr.Y.V.Narayana[4]

[1]Department of Computer Science and Engineering, Tirumala Engineering college (AP.), India

[2]Department of Computer Science and Engineering, JNTUA, Pulivendula (AP.), India

[3] Department of Computer Science and Engineering, Tirumala Engineering college (AP.), India

[4] Principal, Tirumala Engineering college, Narasaraopet (AP.), India

E-mail: [1]rlalunaik@yahoo.com, [2] pcreddy1@rediffmail.com,[3] sathishummadi@gmail.com

Abstract- Wireless networks have become one of the most extensively used communication systems in the world. Providing secure communication for wireless networks has become one of the main concerns. Wireless local area networks (WLAN) are more and more popular; increasingly place of work buildings, airports, and other public places are being prepared with them. Quantum key distribution is a new method in key distribution system in quantum cryptography used to broadcast secret key between two legal parties. This method is an creation in quantum cryptography as part of quantum mechanics which solves the key distributions problem in cryptosystem by providing a secure communication channel between two parties with complete security guaranteed by the laws of physics. In this paper, we analyses the experimental results of using quantum cryptography for secure key distributino in IEEE 802.11 networks focusing on the privacy amplification phase of this protocol.

Key words: IEEE 802.11, Quantum Key Distribution, Wireless Security.

I. INTRODUCTION

Wireless LANs are becoming popular, and majority of office buildings, airports, and other public places are made ready with them. Wireless LANs can operate in one of two configurations; one is with a base station and antoher without a base station. Therefore wireless networks are suitable everywhere in homes, offices and enterprises with its skill to provide high-speed, high quality information exchange between portable devices. It is clear that in the near future wireless technology will lead the communication industry. While wireless networks and its applications are becoming popular every day, security issues connected with it have become a great concern. Due to the natural world of wireless communications, it is possible for an attackers Denial Of Service(DOS) attacks, MAC Spoofing, Man –In –The- Middle attacks, ARP(Address Resolution Protocol) poison, Network booster etc.

As wireless communications use the airwaves, they are essentially more vulnerable to interceptions and attacks than its wired communications. As the service become more popular, the risks to users of wireless technology have improved significantly. Thus, there are a huge number of security risks associated with the current wireless protocols and encryption methods [6, 8].

Quantum Key Distribution (QKD) is in the form of number of protocols such as BB84 [7], B92 [15] and six-state [18] exist as of now which are provably secure, by which private key bits can be shaped between two parties over a public channel. The key bits can then be used to execute a classical private key cryptosystem, to allow the parties to communicate securely. The only condition for the QKD protocol is that quantum bits can be communicated over the public channel with an error rate lower than a positive doorsill. The security of the resulting key is sure by the properties of quantum information, and thus is conditioned only on fundamental laws of physics.

The QKD procedure takes place in two channels: Quantum channel and classical channel. During the quantum channel, series of polarized photons representing the key bits are sent to the receiver with designed QBER(Quantum Bit Error Rate). The classical channel (the IEEE 802.11 wireless network in this case) is used to recover the final key by removing errors introduced during key transmission. The final key recovery of classical channel comprises of four stages: Shifting, Error Estimation, Reconciliation, and Privacy Amplification.

During the shifting phase, Supplicant (STA or client) informs the bases used to authenticator (Access Point or AP). AP keeps only the bits that are recorded against the correct bases. In the error estimation they compare random bits mapped from quantum channel to check the error rate of the transmission. If this is over a threshold value they revert back to quantum channel and start a new photon transmission, proceeds otherwise. In reconciliation phase, they remove all the errors present in the key by applying a chosen reconciliation protocol to obtain a identical key. In privacy amplification they apply a hash function to eliminate possible information that may have leaked to a third party.

Quantum cryptography is only used to generate and allocate a key, know as Quantum Key Distribution(QKD), but not broadcast any message data. Among the QKD protocols, BB84 is more popular and widely used in practical networks [5]. We have chosen a variation of BB84 called SARG04 (Scarani, Acin, Ribordy and Gisin) [16] to use in our job. SARG04 is robust beside photon-number splitting (PNS) attacks [16,17].

QKD has gone through important advancements in both optical and wireless networks. Lots of research work is going on and development in this area is presented in [17, 19]. In QKD, the transmitter (Alice) sends the key as a sequence of polarized photons via quantum channel towards the receiver (Bob).

II. IEEE 802.11 PROTOCOLS

The security of 802.11 is based on Wired Equivalent Privacy (WEP), with some modifications [3].

IEEE802.11 is considered 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 Transaction Security Network(TSN). IEEE802.11 describes two new confidentiality algorithms to address those two cipher suites, namely Temporal Key Integrity protocol (TKIP) and counter mode/CBC-MAC Protocol(CCMP) [12]. IEEE 802.11 offers an efficient framework for authenticating, managing keys and controlling user traffic to protect large networks. It employs the Extensible Authentication Protocol (EAP) [13] to permit a wide variety of authentication mechanisms:

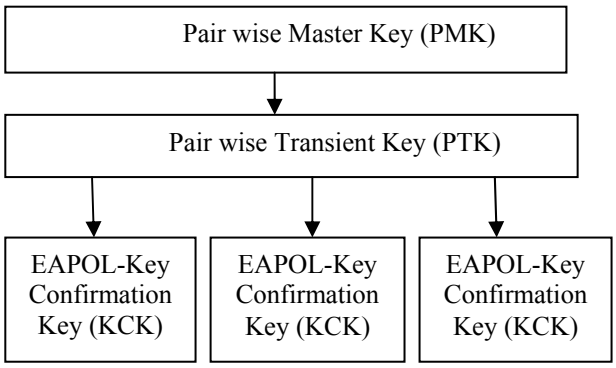

Figure1: Pair wise Key Hierarchy

Figure1 show the pair wise Key hierarchy [3].The PMK received from the Authentication server throughout 802.11 authentication is used to produce PTK by applying Pseudo Random Function (PRF).The PTK gets divided into three keys. The first key is the EAPOL-Key Confirmation Key (KCK). The KCK is used by the EAPO L-Key Exchanges to provided data origin authenticity. KCK is also used to compute message Integrity code (MIC). The second Key is the EAPOL-Key encryption key (KEK). The KEK is used by the EAPOL-Key connections to provide for privacy. KEK is used to encrypt the Group Temporal Key (GTK).The third key is the Temporal Key (TK), which is used by the data privacy protocols to encrypt unicast data transfer.

III. QUANTUM KEY DISTRIBUTION

Quantum Cryptography Quantum Key Distribution (QKD) is a new technique for key distribution to solve the flows in the conventional cryptography. This technique utilizes the standard of quantum mechanics to promise secure communication. It permits two legitimate parties share a random secret key which is known only to them to encrypt and decrypt the message [14].

The exclusive goods in quantum cryptography is the ability to detect the presence of eavesdropper or any third party. The results form a fundamental characteristic of quantum mechanics, where the process of measuring a quantum system in general disturbs the system. If a third party trying to eavesdrop on the key must in some way measure it, thus introducing visible anomaly.

By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. The communication is abort and no secret key can be shaped when the level of eavesdropping has reach or higher the sure threshold, or else if the level of eavesdropping is below a certain threshold, a key can be produced that is below a sure doorsill, a key can be produced that is guaranteed to be secure [5]. Quantum cryptography is used to create and allocate the key and not to use in transmitting any communication data. The produced key can be used with any selected symmetric classical cryptography to encrypt and decrypt the message, which can be transmitted more a standard communication channel which called as public channel.

While, in free room QKD uses the air as the medium in transmiting the photons or bits between sender and receiver. The probability of QKD over the air is measured problematic because of variable medium and high error rate. For the incomplete distance and indoor environment, the quantum channel would be realized at the reasonable level.

IV. PROPOSED PROTOCOL

With many special varieties of wireless networks such as GSM, GPRS, CDMA, CDMA/CD etc, the coverage offered by Wi-Fi networks is only in the range of 100 meters. Wi-Fi networks are extremely popular in places like russet shops, air ports, location halls etc. As our main hub is to offer secured key distribution in wireless networks using QKD, we found that IEEE 802.11 family (Wi-Fi) best suits to get married with QKD. The environmental circumstances impacting quantum missions in Wi-Fi networks can be minimized as the standard area is very small. The general communication of this new protocol takes two channels: wireless channel (Wi-Fi) and Quantum channel.

The SARG04 quantum key distribution process takes as shown the flows 3 – 6 of Figure 2. As the first tread, the transmission switches over to the quantum channel. Requester keeps track of all the photons that is received the length of with the bases it used to measure the photons. As soon as the

photon transmission finishes, the wireless channel resumes for the rest of the protocol implementation.

The keys obtained by both parties will contain errors due to eavesdropping etc. The subsequent 3 stages of QKD remove all these error in order to obtain the final secured key. The shifting process (flow 3 of Figure 2) removes all the bits which recorded against wrong bases used by the authenticator. The error correction process (flow 4 of Figure 2) determines the amount level in within the threshold level, the communication continues.

To complete this, the quantum transmission should guarantee to send sufficient number of photons in order to improve quantum key at least equal or greater than the PMK. For CCMP, PTK is 256bits, while TKIP occupies 384 bits for PMK. Therefore, at this stage, we slip any extra bits of quantum key so that it will have same length as PTK. We get this stripped quantum key as the PTK. Once PTK is available, we can repossess the key pecking order containing all other keys using the PRF.

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 execute 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 bit of PMK equivalent to the length of MIC)

Supplicant then sends Q-MIC to authenticator as shown in flow 7 of figure 3. Winning receiving Q-MIC, authenticator verifies the Q-MIC. Since the authenticator is in possession of all the key hierarchy, it can calculate its own –MIC and compares with the one came from the supplicant. If they match the supplicant is authenticated.

Recent research work explores some of the flaws of 4-wayhandshake [5, 6, 8, 16]. It was shown that the message 1 of 4-way handshake is subject to Denial of Service (DOS) attacks. Intruders can torrent message to the supplicant after the 4-way handshake has completed, causing the system to fail. Since 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 remove the requirement of LOS for quantum transmission. One such research work is done by Kedar and Arnon [9] to have Non Line Of Sight (NLOS) system for optical communication by using wireless sensor network.

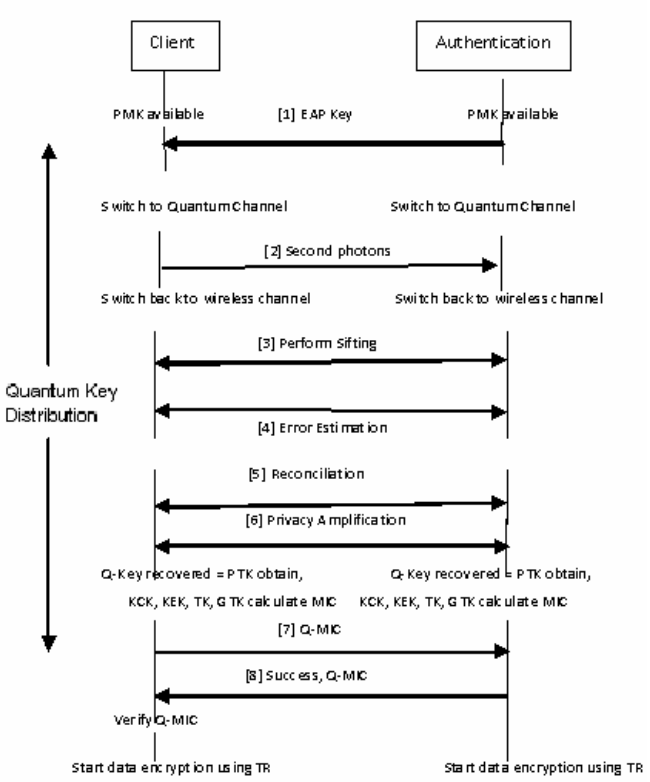

Figure 2 : The Proposed 4-Phase Handshake Protocol

V. PRIVACY AMPLIFICATION

The privacy amplification used can systematically increase the correlation between their key strings, while reducing eavesdropper Eve's mutual information about the result, to any desired level of security in quantum key distribution (QKD) protocol. Information reconciliation is nothing more than error-correction conducted over a public channel, which reconciles error between key length and time to obtain a shared bit string while sensational as little as possible to Eve.

Privacy amplification is the most significant time of 4-phase handshake protocol removes all the errors present in their individual keys to recover the final matching key. Unlike other phase handshake protocol, the number of communication flows complicated in the privacy amplification phase cannot be known in advance. This is because the number of cycles needed to complete this phase depends on the amount of errors present in the key and also the type of privacy amplification protocol being used.

The time taken to complete the privacy amplification process in this simulation model depends on several key factors:

-Length of the main key
-Length of the initial block size of the partition
-Number of cycles the parity check will run for

A number of scenarios have been attempted to approximate the time taken to complete the privacy amplification phase.

Throughout this model, keys with different levels of error rates and different key lengths have been feed into the simulink model. QBER levels between 5% - 9.1% have been achieved during those demonstrations. The time taken to complete privacy amplification under these input conditions for an initial block size of 16 bits is shown in Table I. The Key Length refers to the key obtained after error estimation, while block size refers to the size of the block that the main key was divided initially. This initial block size gets reduced each time the respective block is bisected.

Fig. 3 shows the line graph plot against these data. The results show that when the error rate is low, the final key can be recovered much quicker. The maximum key length tried in the simulations has the length of 900 bits, which is a good upper limit as it can produce a final key of 580 bits at 40% error rate. This is quite sufficient to obtain the final PTK of length 484 high error rates; more time is taken to complete the privacy amplification. This is mainly because under such conditions the initial key needs to go through a number of cycles of parity check. For larger key lengths and high error rates, bisected algorithm needs to go through a number of sub levels of bisections in order to locate the bits that are in error.

This always is more time overriding for the privacy amplification process. But it must be noted that modern QKD communications have achieved error rates well below 10% 15]. Even if such situations occur, they will be detected during the error evaluation phase. The error rates over 20% have been considered just to simulate the worst possible scenarios. The most distinguished observation is that all lines of Figure 3 show similar behaviour to various error levels and key lengths. The main conclusion is that regardless of the key length, for smaller error rates, the privacy amplification phase could be completed well within logical time frame.

Further analysis has been accepted out to find out how the initial block size could collision on the performance of the privacy amplification process. During this analysis, time to complete the privacy amplification has been calculated for various error levels for a fixed key length. Figure 4 shows how initial block sizes cooperate with the presentation of privacy amplification.

It could be seen that the smaller the bisect block size, the quicker the completion of the reconciliation process. With initial block sizes of 4, 8 and 16, reconciliation completes within 4ms time frame which is acceptable considering the amount of work involved in removing the errors. The main reason to this result is that when the initial block size is smaller, the errors can be located more quickly. Further, if a parity mismatch is found, then the respective block gets bisected and eventually another round of parity verification is added to the overall communication. With a smaller initial block size, the number of sub-blocks required is considerably low. Hence the reconciliation can be completed more quickly. Once the block size exceeds 16, it could be seen that the amount of time required for reconciliation increases significantly. The main reason for this observation is that number of cycles needed to process the full key length is considerably large. Larger block length will subsequently bisect into more and more sub-blocks hence parity check requires more time to complete.

TABLE I. TIME TAKEN FOR PRIVACY AMPLIFICATION WITH BLOCK SIZE=16

Key Length	**Time taken to complete Privacy Amplification with various error rates (ms)**			
	10%	**20%**	**30%**	**40%**
500	5.1	5.21	5.35	N/A
600	5.37	5.47	5.57	6.10
700	5.52	5.65	5.75	6.20
800	5.70	5.92	6.10	6.45
900	5.75	6.10	6.30	6.70

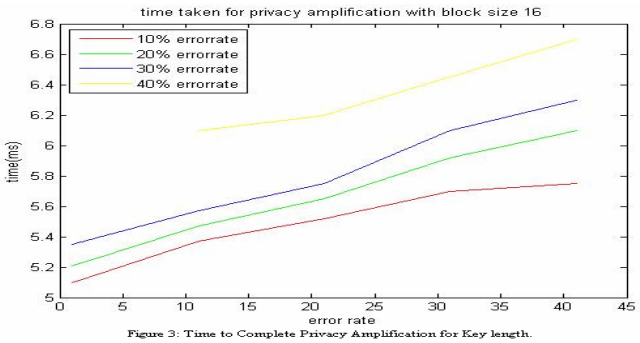

Figure 3: Time to Complete Privacy Amplification for Key length.

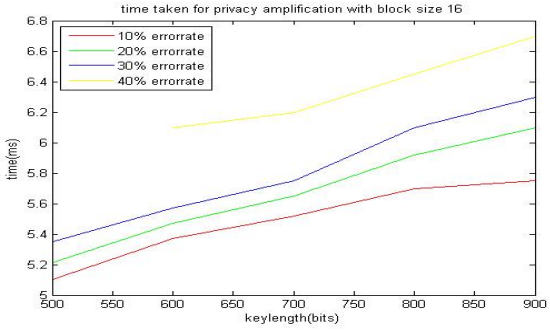

FIG. 4: TIME TO COMPLETE PRIVACY AMPLIFICATION FOR ERROR RATE

VI. CONCLUSION

The benefit of quantum cryptography over established key exchange methods is that the exchange of information can be shown to be secure in very physically powerful sense. We take improvement of the "unconditional safety measures" offered

by QKD to combine with IEEE 802.11 networks. For small wireless networks such as IEEE 802.11, Quantum cryptography can serve better to present secure data communications. The nature of modifications proposed in this research work focused on the process where the key is being distributed. The 4-way handshake protocol of the existing IEEE 802.11 has been replaced with the QKD based 4-phase handshake protocol. Only the key distribution portion is modified while rest of the overall IEEE 802.11 protocol remains unchanged. The aim is to see the behaviour of the modification key distribution process under various input conditions.

The implementation has tested against various input combinations which are based on the data obtained from the quantum channel. As per the simulation analysis, it could be seen that the proposed modifications do not have any major impacts in the overall key distribution process. Even under error rates of 30%, the results show the overall 4-phase handshake completes within reasonable time limits. Ideally, today's quantum transmissions achieve error rates well under 10%. Hence it can be concluded that the proposed solution is efficient enough to be incorporated in the IEEE 802.11 standard**.** We consider our work will contribute to develop secure communications for future wireless networks.

REFERENCES:

[1] ANSI/IEEE 802.11 , 1999 Edition (R2003),part 1.1: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY)Specifications.

[2] IEEE802.1X,2004, IEEE Standard for Local and metropolitan area networks,Port-Based Network Access Control.

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

[4] Floriano De Rango, Dionogi Lentini ,Salvatore Marano, statis and Dyanmic 4-way Handshake Solutions to Avoid Denial of Service Attack in Wi-FI Protected Access and IEEE802.11i,june 2006.

[5] 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,Decenber 1984,pp 175-179.

[6] Changhua He,John C.Mitchell, Security Analysis and Improvements for IEEE802.11i.

[7] Debbie Kedar,Shiliomi Arnon,Non-line-of-sight optical wireless sensor network operating in multiscattering channel,2006.

[8] Debbie kedar.Shilomi Arnon,Quantum Key Distribution by a Free space MIMO System,May2006.

[9] Bob O'Hara, A1 Petrick,IEEE 802.11 Handbook, A Designers's companion,2005.

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

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

[12] Matthias Scholz,Quantum Key Distribution via BB*4,An Advanced Lab Experiment,August2005.

[13] ChangHua He, John C. Mitchell, 1 message Attack on the 4-way Handshake, May 2004.

[14] Dagmar Bruβ,Optimal Eavesdropping in Quantum Cryptography with six States,Physical Review Letters,81.3018,Octobaer1998.

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

[16] Valerio Scarani,Antonio Acin,Gregoire Ribordy and Nicolas Gisin, Quantum Cryptography protocols Robust against Photon Number Splitting Attacks

[17] Tom Kargiannis,Les owens,Wireless Network Security,802.11,Bluetooth and Handheld Devices,NIST,Special Publication 800-48,November 2002.

[18]http://www.technologynewsdaily.com/node/8985,http://www.idquantique.com/,id Quantique,Quantum Cryptography.

[19] New Scientist , Quantum ATM rules out fraudulent web purchases,10 November 2007.

[1] **R.Lalu Naik** received the B.Tech degree in CSE (JNTU-Hyderabad) in 2002 and the M.Tech. Degree in CSE Engineering (JNTU-Anantapur) in 2004, pursuing the Ph.D Degree in dept. of CSE (JNTU-A),and working as an Assoc. Professor in CSE Dept. at Tirumala Engineering College, Narasaraopet.

[2]**Dr.P.Chenna Reddy** received Ph.D Degree in Computer Science and Engineering from JNTU-HYDERABAD, and working as an Assoc. Professor at JNTUA College of Engineering ,Pulivendula and research guide at JNTUA Anatapur and published number of technical Papers at various National/International Conference and Journals.

[3] **U.Sathish Kumar** received the B.Tech degree in Computer Science and Engineering(JNTU-Hyderabad) in 2006 and the M.Tech. Degree in Computer Science and Engineering(JNTUK-Kakinada) in 2010, and working as an Asst. Professor in Computer Science and Engineering Department at Tirumala Engineering College, Narasaraopet.

[4] Dr Y.V.Narayana did his B.Tech in Electronics and Communication Engineering from JNTU, Anantpur (India) in 1991. In 1998 he obtained M.Tech (E&I) from AU College of Engineering, Andhra university(Autonomous), and Visakapatnam. In 2008 he obtained his Ph.D. from AU. He is having total experience of 20 years in both teaching and industry. Presently he is working as Principal for Tirumala Engineering College, Narasaraoept. He published more than 40 papers in both National and International conferences/ Journals