Provably Secure Quantum Key Distribution Protocols in 802.11 Wireless Networks

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

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

Abstract:-The fact that wireless networks have become one of the most extensively used communication systems in the world. Though, providing secure communication for wireless networks has become one of the main concerns. Wireless local area networks are more and more popular, more and more 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 cryptography used to broadcast secret key between two lawful parties. This method is an creation in quantum cryptography as part of quantum mechanics which solves the key distributions problem in cryptosystem by provided that a secure communication channel between two parties with complete security guaranteed by the laws of physics. Communication not only occurred in wired medium but also in wireless medium. WLAN as a wireless medium are much noisier and less dependable in general than wired mediums. This type of noise will produce different numbers of key length and also special height of error rate estimation 802.11 wireless local area networks (WLAN) to show the influence of noise and eavesdropper might make the data transmission in a lot secure in wireless medium.

Key words: 802.11 WLAN, Quantum Key Distribution, Security.

I. Introduction

Wireless LANs are more and more popular, more and more office buildings, airports, and other public places are being ready with them. Wireless LANs can operate in one of two configurations; one is with a base station and anther 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 close to 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 fear. 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 a protocol which is 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 qubits 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 classical public–key cryptography uses asymmetric keys, with one that is private and another one that is public. Throughout the encryption process, the sending station uses a public key to encrypt the data earlier than transmission. The receiving station uses corresponding private key to decrypt the data ahead reception. Each station keeps their private key secreted in order to pass up compromising encryption information. In adding, to defensive information from hackers. Station can use public key cryptography to authenticate themselves to other stations or access points. The major flaw of this classical public key cryptography is based on the fact that the private key is always linked mathematically to the public key [14]. Due to this motivation, it is always possible to attack a public key system if the eavesdroppers prepared with sufficiently large computational resources. Therefore, the mathematical problem to derive the private key from public key must be as not easy possible. Hence those systems cannot provide any signal of eavesdropping or guarantee of key security.

Quantum cryptography is only used to generate and allocate a key, know as Quantum Key Distribution(QKD), but not broadcast any message data a number of QKD protocols such as BB84 [7], B92 [20] and six-state [18]exist as of now out of persons, BB84 is more popular and widely used in practical networks [25]. We have chosen a variation of BB84 called SARG04 (Scarani, Acin, Ribordy and Gisin) [21] to use in our job. SARG04 is robust beside photon-number splitting (PNS) ATTACKS [21, 22].

QKD has gone through important advancements in both optical and wireless networks. There are lots of research work in development in this area and even saleable QKD networks exited as of now [17, 19, 26, 27, 28]. 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 protocols use by all the 802.11 wireless LANs, with Ethernet have a certain arrangement of structure before we introduce our new protocol we require to have a closer look at IEEE802.11 standard as some of which we shall begin into our current work. The security of 802.11 is defined by Wired Equivalent Privacy (WEP), as a product of this an adjustment to the IEEE802.11 protocol [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].IEEE802.11 offer 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 mechanism:

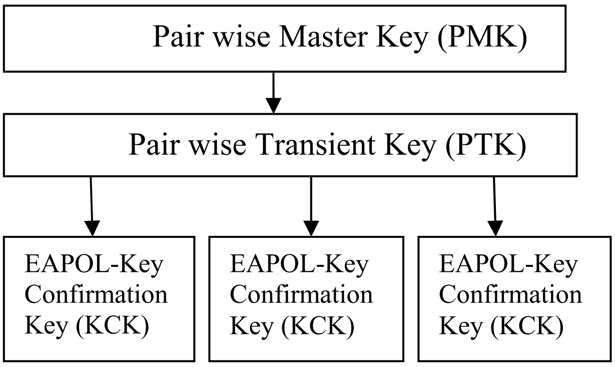
Pair wise Master Key (PMK)
Pair wise Transient Key (PTK)
EAPOL-Key Confirmation Key (KCK)
EAPOL-Key Confirmation Key (KCK)
EAPOL-Key Confirmation Key (KCK)

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 authenticaticity.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 permit two legitimate parties shared a random secret key which only identified 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 that difficult to gain information of the key. This results from 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 transmit 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.

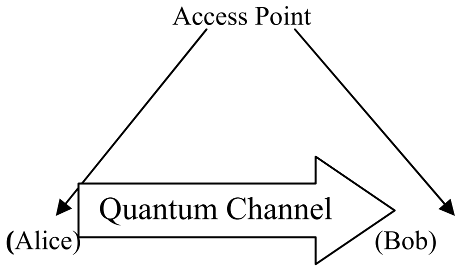

Figure 2 : Hardware implementation

IV. PROPOSED PROTOCOL

So 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 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 generally communication of this new protocol takes two channels: wireless channel (Wi-Fi) and Quantum channel.

Form the point forgotten the SARG04 quantum key distribution process takes as shown as flows 3 – 6 of figure 3. 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 various impressive situation, eavesdropping etc. The subsequent 3 stages of QKD remove all these error in order to obtain the final secured key. The sifting process (flow 3 of figure 3) removes all the bits which recorded against wrong bases used by the authenticator. The error correction process (flow 4 of figure 3) 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 be 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 DOS attacks. Intruders can torrent message I 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.

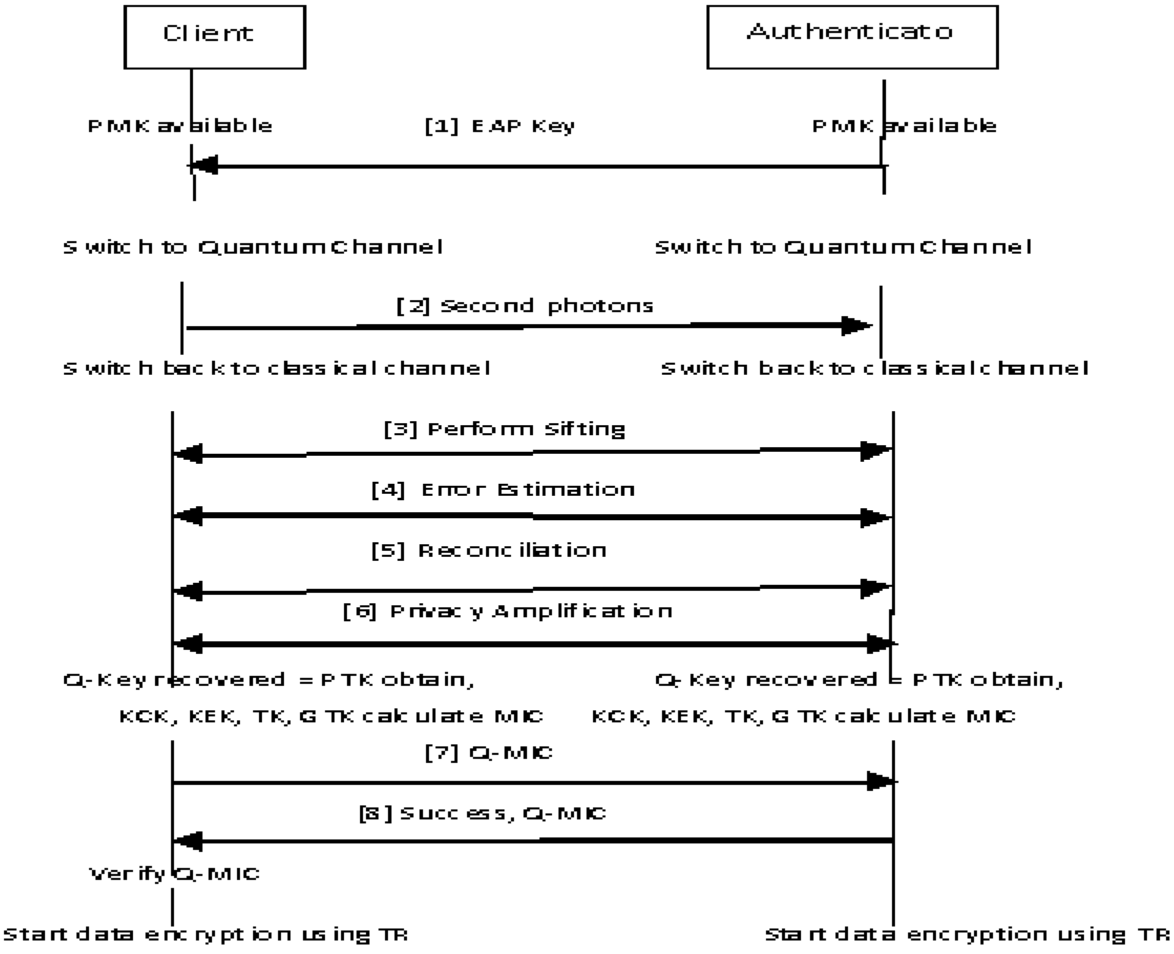
Client
Authenticato
PMK available
[1] EAP Key
PMK available
Switch to Quantum Channel
Switch to Quantum Channel
[2] Second photons
Switch back to classical channel
Switch back to classical channel
[3] Perform Sifting
[4] Error Estimation
[5] Reconciliation
[6] Privacy Amplification
Q-Key recovered = PTK obtain,
KCK, KEK, TK, GTK calculate MIC
Q-Key recovered = PTK obtain,
KCK, KEK, TK, GTK calculate MIC
[7] Q-MIC
[8] Success, Q-MIC
Verify Q-MIC
Start data encryption using TK
Start data encryption using TK

Figure 3: The Proposed Protocol

V. RESULT AND DISCUSSION

From the implementation, the result on key length and error shows the different value based on three measurements that have been experiment. From the fig 4 and fig 5 we can see the comparison of the graph between different network environments but the fraction obtained in wireless is lower than wired setting. It is because of the data transmission is not only being attack by Eavesdropper but also by the noise in wireless which much higher than in wired location.

Both of the figure shows that even there is no attack, Bob still cannot gain perfect bits length send by Alice. It caused by the quantum channel itself also hold other effect that cause to limitation channel which bring a little error on their bits during transmission. The same goes to intercept attack which gives the length of error bits as much as no attack type. During intercept attack Eve will generate a new string of random key and send it to Bob and assume it was generated by Alice. Hence, the possibility that key is generated by Eve similar to Alice is 50% while the probabilities for Alice and Bob can notice the survival of Eve is only 25%.

For the beam splitting attack, the number of error bits length is a large amount lower than the other two attacks because in this attack a random number sent by Alice are being whole by Eve. Thus, much more error can be detect by Alice and Bob in error modification process.

The implementation on wireless and wired was obtained different value of final bits due how many noise are occur during the transmission between Alice and Bob. While in wireless the noise are higher than weird medium and that is the motivation why the final bits in wireless medium are shorter.

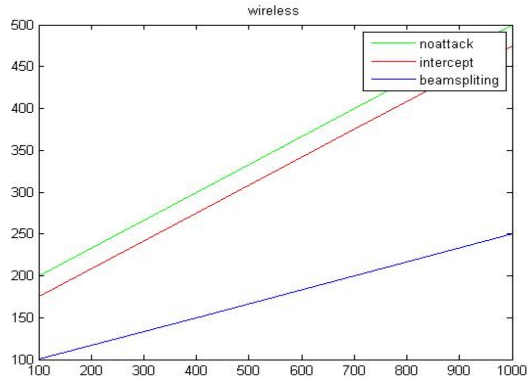

Figure 4: Key length vs. Error length on 802.11

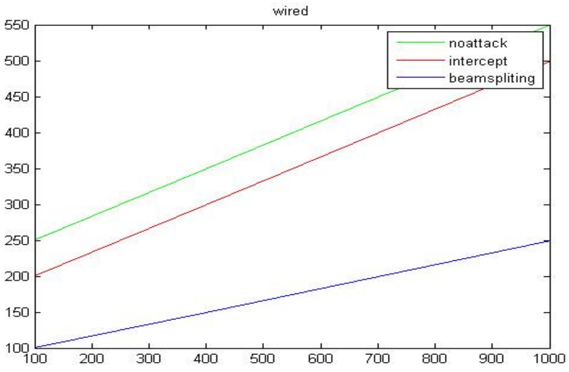

Figure 4: Key length vs. Error length on wired

VI. CONCLUSION

Wireless networks are subject matter to various security risks. Most significant source of risk in wireless networks is that the technology's fundamental communication medium, the airwave ,is open to intruders .Due to this reason ,lots of efforts have been put in to address security issues in wireless networks .To address the same issue ,we outline the usage of quantum cryptography for key distribution in 802.11 networks .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 ,without making assumptions about the intractability of certain mathematical problems .in our work, we take improvement of the "unreserved safety measures" offered by QKD to combine with IEEE 802.11 wireless network .For small wireless networks such as IEEE802.11, Quantum cryptography can serve better to present secure data communications. With the recent advancements on MIMO technology for quantum transmissions, shows us a better way towards eliminate the LOS restriction .Although present technology does not extend to supply quantum transmission in 802.11 equipment so far, we consider our work will contribute to develop secure communications for future wireless networks.

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 Phenonix Park, Korea.Proceedings ISSN 1738-9445,ISBN978-89-5519-135-6,vol.II,p865.

[2] ANSI/IEEE 802.11 , 1999 Edition (R2003),part 1.1: 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 (MAC) and Physical Layer (PHY) specifications, Amendment 6:Medium Access Control(MAC)Security Enhancements,2004.

[4] IEEE802.1X,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 Dyanmic 4-way Handshake Solutions to Avoid Denial of Service Attack in Wi-FI Protected Access and IEEE802.11i,june 2006.

[7] 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.

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

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

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

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

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

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

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

[15] Paul J.Edwards, The university of Canberra-Telstra Tower Quantum Crypto-Key Telecommunications Link, Advanced Telecommunications and Electronics Research Centre,http://www.ips.gov.au/IPSHosted/NCRS/wars/wars2002/proceedings/invited/print/Edwards.pdf.

[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 pratical.

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

[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.Hisket t,S.McNown,N.Nweke,J.T Blake,L.Mercer,H.Dardy ,QuantumCryptography for Optical Networks:A Systems Perspective.

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

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

[22] Valerio Scarani,Antonio Acin,Gregoire Ribordy and Nicolas Gisin, Quantum Cryptography protocols Robust against Photon Number Splitting Attacks for Weak laser Pulse Implementations,Phys.Rev.Lett.,Vol 92,057901,2004.

[23] Gilles Brassard,Norbert Lűtkeenhaus,Tal Mor,Barry C.Sanders, Limitations on Praticals Quantum Cryptogrphy,February2000.

[24] Tom Kargiannis,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 Fűrst,Rupert Ursin,Felix Tiefenbacher,Thomas Scheidl,Josep Perigues,Zoran Sodnik,Christian Kurtsiefer,John G.Rarity,Anton Zeilinger, Harald, Weinfurter , Experimental Demonstration of Free-space Decoy-State Quantum Key Distribution of Free-space Decoy-State Quantum Key Distibution over 144km, Phys.Rev.Lett .98,01054,January2007.

[26] http:// www.secoqc.net/,SECOQC,Development of a Global Network for Secure Communication based on Quantum Cryptography.

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

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