QUANTUM CRYPTOGRAPHY WITH KEY DISTRIBUTION IN WIRELESS NETWORK

[1]Premlata Sonawane, [2]Leena Ragha

[1]Scholar at Ramrao Adik Institute of Technology, Navi Mumbai, India,
[2]H.O.D. of Computer Engineering Department at Ramrao Adik Institute of Technology, Navi Mumbai, India
Email : [1]premlata.sonawane@gmail.com, [2]leena.ragha@gmail.com

Abstract: It is well known that wireless networks have become one of the most important part used communication systems, in particular for ubiquitous computing. However, providing secure communication for wireless networks has become one of the prime concerns. Quantum cryptography, namely quantum key distribution (QKD), offers the promise of unconditional security. 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. For small wireless networks such as IEEE 802.11, Quantum cryptography can serve better to present secure data communications. The 4-way handshake protocol of the existing IEEE 802.11 has been replaced with the QKD based 4-phase handshake protocol. For the integration of QKD and IEEE 802.11, only the key distribution portion can be modified while rest of the overall IEEE 802.11 protocol remains unchanged. The integration method takes the advantage of mutual authentication features offered by some EAP variants of 802.1X port-based network access control. Quantum message integrity code (Q-MIC) which provides mutual authentication between the two communication parties and its implementation.

Index Terms: 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. 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. 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[4] etc.

As wireless communications use the airwaves, they are essentially more vulnerable to interceptions and attacks than its wired communications. Our first tentative is towards WLAN 802.11 networks because of the four following reasons [17]. First, WLAN 802.11[1]-[2]-[3]-[8] is mainly used in office and campus environments. This building oriented environment facilitates the deployment of a quantum key distribution network with a high density of quantum apparatus if necessary. Second, the mobility speed of mobile users in WLAN 802.11 is relatively slower in comparison with cellular networks. Third, WLAN 802.11 terminals (e.g. laptop) usually have more computational capacity and more energy for the autonomy than cellular network's terminals. Fourth, from an application point of view, WLAN 802.11 is usually used to provide access to the Internet through an access point installed by an organization or by a wireless ISP.

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. The final key recovery of classical channel comprises of four stages: Shifting, Error Estimation, Reconciliation, and Privacy Amplification [17].

Quantum cryptography [4]-[5]-[6]-[7] 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. We have chosen a variation of BB84 called KMB09 [22] to use in our job. KMB09 is robust beside photon-number splitting (PNS) attacks [20]-[21] and it allows Alice and Bob to distinguish system errors from eavesdropping errors. As a result, Alice and Bob can tolerate lower eavesdropping

and higher system error rates without compromising their privacy.

II. CLASSICAL CRYPTOGRAPHY

The primary application of cryptography is to send secret messages. The central problem in cryptography is the key distribution problem, for which there are essentially two solutions: one based on mathematics, classical cryptography, and one based on Physics. While classical cryptography relies on the computational difficulty of factoring large integers, quantum cryptography relies on what we believe to be the universal laws of quantum mechanics.

These classical cryptosystems come in two flavors: symmetric systems, and asymmetric systems [6]. The security of public key cryptosystems is based on computational complexity. The idea is to use mathematical objects called one-way functions. So far, no one has proved the existence of any one-way function with a trapdoor; so, the existence of secure asymmetric cryptosystems is not proven.

III. LIMITATIONS

Classical cryptography faces the following two problems.

First, the security of many classical cryptosystems is based on the hardness of problems such as integer factoring or the discrete logarithm problem.

Second, the theory of quantum computation has yielded new methods to tackle these mathematical problems in a much more efficient way. Although there are still numerous challenges to overcome before a working quantum computer of sufficient power can be built, in theory many classical ciphers (such as RSA) might be broken by such a powerful machine.

So to overcome the limitation regarding mathematical computation and lack of eavesdropping detection of classical cryptography, the researcher found the efficient way of secure key distribution for communication between two parties by using quantum cryptography.

IV. LITERATURE REVIEW

- Charles H. Bennett & Gilles Brassard has found firstly that how photon transmission [4] occurs in quantum channel for making secure communication and they proposed the new protocol as Coin tossing as BB84 by exchange of quantum massage which is secure against traditional kind of cheating.
- Changhua He John C Mitchell analyze the IEEE 802.11i wireless networking standard may provide satisfactory mutual authentication and key management [8]. 802.11i IEEE standard designed to provide enhanced MAC security in wireless networks.
- A.Falahati , Hadi Meshgi has proposed the system which used quantum technique for the distribution of encryption keys in 802.11 wireless networks [9] and analyzed that if QBER ratio is increased then eves dropper is detected also they present modified 4-way handshake to integrate the BB84 protocol with 802.11
- Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, 2009 again modified the previous work of QKD in 802.11 IEEE wireless networks [12] by representing a new code called Quantum Message Integrity Code (Q-MIC) which provides mutual authentication between the two communication parties and its implementation.
- R.Lalu Naik , Dr.P.Chenna Reddy , U.Sathish Kumar & Dr.Y.V.Narayana they analyses the experimental results of using quantum cryptography for secure key distribution[17] by using SARG04 protocol with IEEE 802.11 networks focusing on the privacy amplification phase of this protocol.

IV. QUANTUM CRYPTOGRAPHY

Quantum Cryptography [4]-[5]-[6]-[7] is a relatively recent arrival in the Information Security world. The idea of quantum cryptography was first proposed in the 1970s, though it is only now that the field is applied to information security. The main advantage of quantum cryptography is that it gives us perfectly secure data transfer. The first successful quantum cryptographic device could translate a secret key over 30 centimeters using polarized light, calcite crystal(s), and other electro-optical devices. For Quantum Informatics the smallest unit of information is the qubit , which is a generalized form of the classical bit. In topics of quantum based communication the sender is called Alice, the receiver is called Bob and the eavesdropper is called Eve. The quantum channel or quantum link is the communications channel performing the transmission of the qubits. This can represent 0, 1, and any value in between at the same time. In a graphical sense, a vector pointing in a direction intermediate between those representing 0 and 1 represents the in-between position known as superposition.

A] Heisenberg's Uncertainty Principle

The Heisenberg states that certain pairs of physical properties [4]-[5]-[23] are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. For example, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequences measurements. This principle plays an important role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography.

B] Quantum Entanglement

Entanglement [4]-[5]-[23] is a kind of correlationlation that is stronger, in a certain sense, than any classical one. Quantum entanglanical phenomenon in which the quantum of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. As a result, measurements performed on one system seem to be instantaneously influencing other systems entangled with it.

V. QKD PROTOCOLS

In Quantum Cryptography the Quantum Key Distribution (QKD) [4]-[5]-[6]-[7]-[8] is a new technique for key distribution to solve the flows in the conventional cryptography. It is based on some protocols among of them we will discuss the basic QKD protocol bellow.

A] THE BB84 PROTOCOL

The first key distribution protocol was developed by Charles Bennett and Gills Brassard in 1984. It is recognized as BB84 [5]-[9].This is the first known quantum distribution scheme. The quantum system is based on the distribution of single particles or photons, and the value of a classical bit encodes by the polarization of a photon. BB84 allows two parties, conventionally "Alice" and Bob", to establish a secret common key sequence using polarized photons.

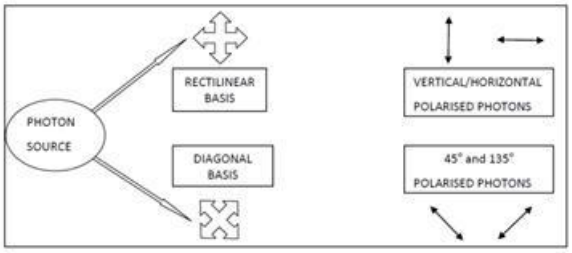

Fig.1 Rectlenier & Diagonal Polarization Bases [23]

Raw key exchange and key sifting [23] are done as follows:

- Photons are polarized using conjugate bases, either a rectilinear basis (vertical/horizontal polarizations) or a diagonal basis (45^o and 135^o polarizations) as shown in above Fig. 1
- These polarized photons can be used to send information if each polarization generated by a basis is allocated the value '0' or'1' , and these encodings are agreed between Alice and Bob before they attempt to exchange quantum states.
- Alice can produce photons with 4 different polarizations, and she chooses the basis for each photon at random and sends a stream of randomly polarized photons to Bob for measurement. This style of protocol is thus termed Prepare and Measure (P & M).
- Bob now has to detect and measure these polarizations. He passes them through filters – potentially changing their original polarizations - and records the results with a photon counter. As Bob does not know which basis Alice has used for each photon, he can only set his receiving bases randomly too. If he chooses correctly, the polarization is recorded accurately; if he chooses wrongly, then the result is a random polarization matching his (not Alice's) choice of basis, with all information about the initial photon polarization lost. This is the Raw Key Exchange stage.

The Key Sifting stage is done over a public classical channel, where Alice and Bob each broadcast their choice of basis for each photon. The bases are compared, and any photon which had been processed using non-matching bases is dropped from the raw key material.

In case of eavesdropper [23], Eve intercepts her bases, but she is in exactly the same position as Bob was previously. So, like Bob previously, she will have her bases correctly set only half the time, and the incorrect settings will result in random polarization readings and the destruction of the original polarization. As a consequence, when she then resends the photons she has intercepted, 50% of them will be wrong. Bob sets his bases randomly as usual, but in this case, when he sets a base the same as Alice, he only gets a correct result 50% of the time, as Eve has changed the polarizations of the photons he receives in 50% of cases. This will be highlighted at the Key Sifting stage, as the QBER will be too high. More stringent privacy amplification procedures can be brought to bear to remove the effects of any information that Eve has extracted.

There are some variant of BB84 protocol such as Two-state protocol B92 [15]-[23], Eckert's Protocol [5]-[18], COW Protocol [19], SARG04 Protocol [12]-[17]-[21], KMB09 Protocol [22].

VI. IEEE 802.11 WIRELESSES LAN

The protocols use by all the 802.11 wireless LANs [9]-[10]-[11]-[12]-[13] 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. IEEE802.11 is considered to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. 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) [12] to permit a wide variety of authentication mechanism.

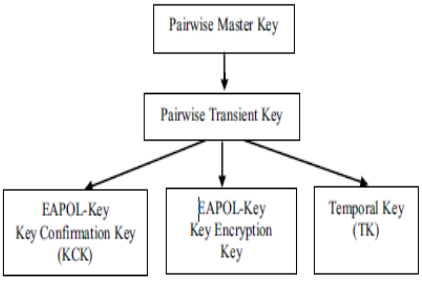

Fig.2. Pair wise Key Hierarchy [10]-[12]-[15]

Fig.2 shows the pair wise Key hierarchy for key management. 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 EAPOL-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.

VII. PROPOSED PROTOCOL

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 general communication of this new protocol takes two channels: wireless channel (Wi-Fi) and Quantum channel. However, in practical realizations, a QKD protocol is only secure, when the quantum bit error rate introduced by an eavesdropper unavoidably exceeds the system error rate. This condition guarantees that an eavesdropper cannot disguise his presence by simply replacing the original transmission line with a less faulty one. Unfortunately, this condition also limits the possible distance between the communicating parties, Alice and Bob, to a few hundred kilometers. To overcome this problem, we have chosen a KMB 09 QKD protocol [22], the proposed protocol employs an alternative encoding of information in two-dimensional photon states. Errors manifest themselves as quantum bit and as index transmission errors with a distinct correlation between them in case of intercept-resend eavesdropping. As a result, Alice and Bob can tolerate lower eavesdropping and higher system error rates without compromising their privacy. So here we show the 4 phase handshake protocol.

The KMB09 [22] quantum key distribution process takes as shown the flows 3 – 6 of Fig.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.

- Alice generates a random key sequence of classical bits and randomly assigns each bit value a random index i = 1, 2. . . N.
- Alice then uses this sequence and sends single photons prepared accordingly either in $|e_i>$ or $|f_i>$ to Bob.

As soon as the photon transmission finishes, the wireless channel resumes for the rest of the protocol implementation, then within key sifting (flow 3 of fig.3)

- Bob measures the state of every incoming photon, thereby randomly switching the measurement basis between e and f.
- Alice publicly announces the random sequence of indices i used to establish the cryptographic key.
- Bob interprets his measurement outcomes accordingly, using, value of N. He obtains a key bit whenever his index is different from the index announced by Alice.

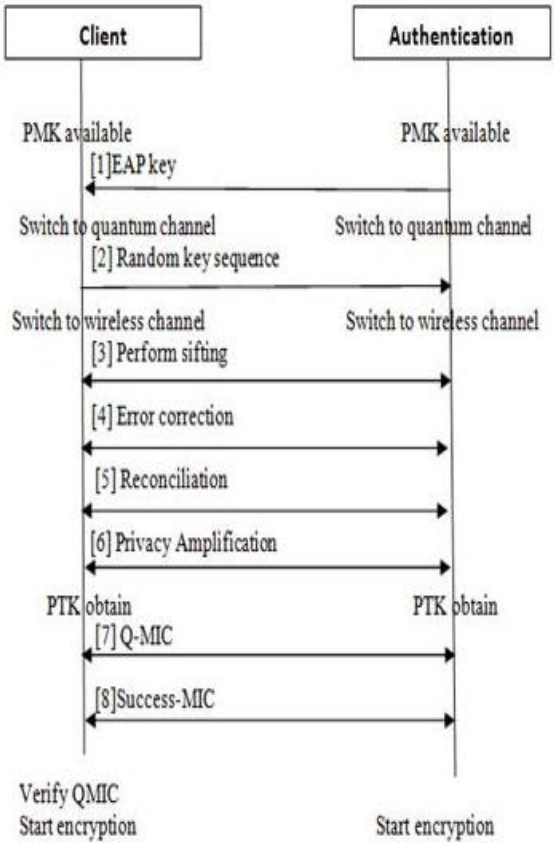

Fig.3. The proposed 4 phase handshake protocol

- Bob tells Alice which photon measurements have been successful and provide a bit of the Secret key.

In these subsequent stages of QKD removes all these error in order to obtain the final secured key.

- Finally in error correction, Alice and Bob determine whether an eavesdropper introduced an error into their communication. Whenever this error rate is sufficiently small, Alice and Bob can assume that no eavesdropping has occurred.

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. From the PTK we can derive KCK, KEK & TK, while from KCK, MIC can be calculated. Supplicant then sends Q-MIC to authenticator as shown in flow 7 of fig.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 Q-MIC and compares with the one came from the supplicant. If they match the supplicant is authenticated.

As a result, eavesdropping introduces quantum bit as well as index transmission errors. A quantum bit error occurs, when Alice and Bob both obtain different key bits. An index transmission error occurs when Alice and Bob use the same basis but their respective states nevertheless have different indices. Intercept-resend eavesdropping results, in general, in a significant change of both the Quantum Bit Error Rate (QBER) and the Index Transmission Error Rate (ITER).

It gives us the flexibility to maximize the error rate introduced by an eavesdropper in the case of an intercept–resend attack. The proposed solution is efficient enough to be incorporated in the IEEE 802.11 standard. And we consider this work will contribute to develop secure communication for future wireless networks.

VIII. 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. 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 behavior of the modification key distribution process under various input conditions.

The main purpose of the proposed QKD protocol is to make it much harder for an eavesdropper to conceal his presence. The eavesdropper now not only has to minimize different types of errors. The above mentioned strong correlations between the ITER and the QBER introduce a distinct signature of eavesdropping. This signature allows Alice and Bob to detect the origin of their errors and to tolerate lower eavesdropping and higher system error rates without compromising their privacy. As a result, Alice and Bob should be able to communicate securely over much longer distances.

REFERENCES

[1] Olli Vihervuori ,"Recent Developments in IEEE 802.11 Wireless Local Area Network Link-layer Security", TKK T-110.5190 Seminar on Internetworking,2009

[2] Kevin Hulin, Carsten Locke, Patrick Mealey, and Ashley Pham, "Analysis of Wireless Security Vulnerabilities, Attacks, and Methods of Protection", Erik Jonsson School of Engineering and Computer Science ,The University of Texas at Dallas, IJMUE, Vol. 3, 2008

[3] Changhua He John C Mitchell," Security Analysis and Improvements for IEEE 802.11i", 12th Annual network and distributed system security synomposium, 2005

[4] 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, PP.175-179. December 1984.

[5] GeraldScharitzer,"Basic quantum cryptography", Version 0.9, Oct 2003.

[6] Rajni Goel Moses Garuba, Anteneh Girma, "Research Directions in Quantum Cryptography", International Conference on Information Technology (ITNG'07)0-7695-2776-0/07,PP.1-6, 2007

[7] Vladimir L. Kurochkin, Igor G. Neizvestny, "Quantum Cryptography", 10th International Conference and Seminar, SECTION III, ERLAGOL, JULY 1-6, PP.166-170,2009

[8] Changhua He & John C Mitchell, "Analysis of the 802.11i 4-Way Handshake", WiSE'04 Philadelphia, Pennsylvania, USA ACM 1-58113-925, 2004

[9] A.Falahati , Hadi Meshgi, "Using Quantum Cryptography for securing Wireless LAN networks",International Conference on Signal Processing Systems, IEEE DOI 10.1l09/ICSPS.216 PP.698-701,2009

[10] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaouti-Hélie," Integration of Quantum Cryptography in 802.11 Networks", IEEE , Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) 0-7695-2567-9/06, 2006

[11] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie, "802.11i Encryption Key Distribution Using Quantum Cryptography", 2006 ACADEMY Publisher Journal of Networks, VOL. 1, NO. 5,PP.9-20, 2006

[12] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma," Novel Protocol and Its Implementation QKD in Wi-Fi Networks", Eight IEEE/ACIS International Conference on Computer and Information Science,IEEE 978-0-7695-3641-5/09DOI 10.1109/ICIS.2009.122 PP.812-817,2009

[13] G.Murali, R.Siva Ram Prasad V.Swetha Madhavi," Effective Key Authentication for Ieee 802.11 Networks using Quantum Cryptography", International Journal of Computer Applications , 0975 – 8887, Vol.46– No.7,PP.26-27, May 2012

[14] M. Indra Sena Reddy, K. Subba Reddy, M. Purushotham Reddy, P.J. Bhat, Rajeev ,"Key Distillation Process on Quantum Cryptography Protocols in Network Security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 6,PP.19-24,June 2012

[15] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma ,"Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks", ISBN 978-89-5519-136-3 ICACT, PP.17-20, Feb 2008

[16] R.Lalu Naik , Dr.P.Chenna Reddy , U.Sathish Kumar, Dr.Y.V.Narayana, "Provely Secure quantum Key Distribution protocol in 802.11Wireless Networks", International Journal of Computer Science and Information Technologies, , Vol. 2 (6),PP.2811-2815 , 2011

[17] R.Lalu Naik , Dr.P.Chenna Reddy , U.Sathish Kumar, Dr.Y.V.Narayana, "Quantum Cryptography with Key Distribution in Wireless Networks on Privacy Amplification", International Journal of Computer Networks and Wireless Communications, vol.1,PP.1-5,Dec 2011

[18] Artur K. Ekert,"Quantum Cryptography Based on Bell's Theorem", Physical Review Letters.,vol.67,No.6,PP.661-663 , Aug 1991.

[19] Damien Stucki, Claudio Barreiro, Sylvain Fasel, Jean-Daniel Gautier, Olivier Gay, Nicolas Gisin, Rob Thew, Yann Thoma, Patrick Trinkler, Fabien Vannel, Hugo Zbinden, "High speed coherent one-way quantum key distribution prototype", OPTICS EXPRESS 13326, ,No. 16 , vol. 17,PP.1-9, Aug. 2009

[20] Valerio Scarani Antonio Acin Gregoire Ribordy, Nicolas Gisin , "Quantum cryptography protocols robust against photon number splitting attacks".APS,Phys.Rev.Lett, Vol. 92,2004

[21] Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo," On the performance of two protocols: SARG04 and BB84", Center for Quantum Information and Quantum Control Canada,Feb 2008

[22] Muhammad Mubashir Khan, Jie Xu,and Almut Beige , "Improved Eavesdropping Detection in Quantum Key Distribution",arXiv.org, Quantum physics,PP.2-9, Dec 2011

[23] Sheila Cobourne, "Quantum Key Distribution Protocols and Applications", Surrey TW20 0EX, England, 2011

◈◈◈