Quantum Cryptography Implementation in Wireless Networks

Jarrar Ahmed[1], Ashish Kumar Garg[2], Man Singh[3], Sham Bansal[4], Mohammad Amir[5]

[1]Delhi University, Assistant Professor, Department of Mathematics, Dyal Singh College, Lodhi Road, New Delhi–110003, India

[2]Delhi University, Department of Mathematics, JDM College, Rajendra Nagar, New Delhi - 110005, India

[3]Delhi University, Department of Mathematics, SPM College, West Punjabi Bagh, New Delhi - 110026, India

[4] Delhi University, Department of Mathematics, Bharati College, C4, Janakpuri, New Delhi - 110058, India

[5] Delhi University, Department of Mathematics, IP College for Women, Civil Lines, New Delhi - 110054, India

Abstract: ***Wireless network is one of most important modes of communication. So providing security to the information being communicated through wireless networks is very important issue. Classical cryptography provides conditional security which has many loop holes whereas quantum cryptography promises to be unconditionally secure for wireless networks. In the present paper, we have implemented quantum cryptography in wireless communication systems using a quantum key distribution (QKD) protocol which is named as SARG04.***

Keywords: QKD, RSA, IEEE 802.11, IEEE 802.11i, SARG04 protocol.

1. Introduction

Cryptography is the technique for secure communication of data in the presence of third parties, called adversary. Classical cryptography is based on the complexity of some mathematical function which is a one way function. The security is as strong as difficult to revert it. It provides conditional security. The main weakness of classical cryptography is that it does not provide any method to sender and receiver to find out the presence of adversary. Since the most often used classical cryptographic method is RSA which is based on difficulty of factorization of a number obtained by product of two large primes. As quantum computer becomes functional all types of classical cryptosystem become breakable while keeping all these shortcomings in classical cryptosystem in mind, people started to think beyond it for securing future electronic communication. Quantum cryptography deals with almost all loopholes found in classical cryptosystem. For the first time in cryptography, quantum mechanical forces have been used to obtain an unconditionally secure cryptosystem. In first part we discuss some classical cryptosystems and their weaknesses, second part involves the discussion about the quantum computing and quantum cryptography, and in third part we give a brief introduction of wireless LANs and security mechanisms. In last part, we implement the quantum cryptography in wireless LAN.

2. Classical Cryptosystems and Their Weaknesses

2.1 Classical Cryptosystems

Generally there are two broad classifications of classical cryptosystems:

(a) Symmetric Cryptosystems
In such type of cryptosystems we use same key for encryption and decryption. It is also known as secret key cryptosystem

{b) Asymmetric Cryptosystems
In the asymmetric, we use two keys, one public key known publicly and other is private key known to recipient only. A very important property of public key cryptosystem is that the public and private keys are connected in such a way that anyone can use public key to encrypt message and only private key can be used to decrypt the cipher text. Now we mention two most famous examples (one for each type of cryptosystem respectively) of classical cryptography.

(1) One Time Pad (OTP)
One time pad symmetric cryptosystem is a type of cryptosystem that has been proved to be unbreakable if implemented carefully. Every character or bit of the plaintext is encrypted by using modular addition with a character or bit of a secret random key (or pad) of the same length as the plaintext, converting it into a cipher text. If any of the following condition is compromised OTP will no longer be unbreakable:

(i) The secret key is at least as long as the message or data that is going to be encrypted.
(ii) The key is truly random (not generated by a simple computer function etc.
(iii) The key or plaintext can be calculated using modulo 10(Decimal digits) or modulo 26(Letters) or modulo 2(binary)
(iv) Each key is used only once, and both sender and receiver must destroy after use (no repetition)
(v) There should only be two copies of the key: one for the sender and one for the receiver (with some exceptions for multiple receivers).

(II) RSA Asymmetric Cryptosystem

RSA is a public key cryptography system that is based on the assumption of difficulty of factoring large integers, the factoring problem. RSA is acronym for Ron, Rivest, Adi Shamir and Leonard Adelman, who are the inventors of this method. In general method goes as:

a) A user of RSA chooses and then publishes the product of two large prime numbers, along with some auxiliary value, known as public key
b) The prime factors of private key must be kept secret.
c) Anyone can encrypt a message by using public key then only anyone with knowledge of even one prime factor can decode the message. RSA cryptosystem is as hard as factoring of corresponding product of two large prime.

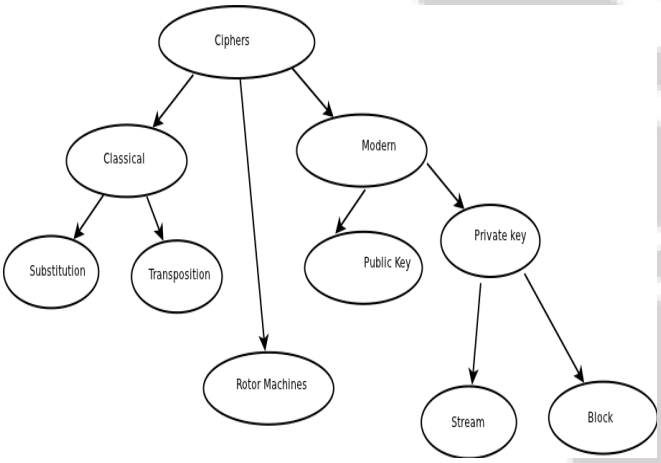

Figure 1: Pictorial representation of Cipher

2.2 Weaknesses of Classical Cryptosystems

The first and foremost problem which is faced by classical cryptosystem is the key distribution. There is no method in classical cryptosystem to find out tempering with key while transmitting it. To use OTP in its true sense is quite difficult .As quantum computer becomes functional, RSA system will no longer be trustworthy.

3. Quantum Computing and Quantum Cryptography

3.1 Quantum Computing

The main advantages of quantum computing can be listed as follows:

a) When quantum operations are performed on a suitable quantum data, then a classical problem can be solved in a much time efficient manner.
b) Due to having quantum mechanical properties a qubit can be used for multiple problems.
c) No cloning property of a qubit can be advantageous if the message sent through the qubit is secret and making a copy of it is undesirable.
d) Whenever a state of a qubit or its superposition is measured, the state is collapsed. This can be used to maintain privacy of the messages.
e) In a classical information system, digital signals are denoted by classical bits. These classical bits can be in either 0 or 1 state at a time to give rise to 2n number of bit vectors for a vector of length n. In same way, two possible states for quantum bits (qubits) are $|0\rangle$ and $|1\rangle$. The difference between qubits and bits is that qubits can be in states, which is also a superposition of $|0\rangle$ and $|1\rangle$ states. A superposition state $|\Psi\rangle$ can be denoted by $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

3.2 Quantum Cryptography

The main feature of the quantum cryptography is to detect the presence of eavesdropper trying to gain the key. Since quantum bits cannot be copied because a quantum state cannot be measured without disturbing the state. Suppose an eavesdropper Eve tries to intercept the message being transmitted between two parties. Then No-Cloning theorem gives effectiveness to the quantum cryptosystem. If eve wants to gain knowledge of two non-orthogonal states of a photon, it is impossible to obtain information gain without disturbing the state of at least one of them. It is clear from taking $|\Psi\rangle$ and $|\Phi\rangle$ to be non-orthogonal quantum states which Eve is trying to know about. If these states interact with a standard state $|V\rangle$ then

$|\Psi\rangle|V\rangle \rightarrow |\Psi\rangle|u'\rangle$ and $|\Psi\rangle|V\rangle \rightarrow |\Psi\rangle|u\rangle$

Eve would desire $|u\rangle$ and $|u'\rangle$ to be different, to know the identity of the state. Since inner products of two kets are preserved under unitary transformations and

$|u/u'\rangle\,|\Psi/\Phi\rangle = |V/V\rangle\,|\Psi/\Phi'\rangle$ or

$|V/V\rangle = |u/u'\rangle = 1.$

Then $|u'\rangle$ and $|u\rangle$ must be identical and Eve will corrupt one of the two states in order to gain information.

3.2.1 Quantum Cryptography Protocols

There are many protocols to implement Quantum Cryptography like BB84, B92, E91 and SARG04 etc., are available today. The most popular protocol is BB84. In BB84, Alice (sender) and Bob (receiver) communicate in two different channels, quantum channel (optical fibers or free space) and public channel (internet etc.). Quantum key distribution task happens in two phases:

Via Quantum channel (one way communication)
Step1: Alice randomly chooses a string of bits and then encodes these bits by using random bases rectilinear or diagonal and Alice will transmit a photon for each encoded bit with corresponding polarization to Bob using quantum channel.
Step2: Bob receives those polarized photons with randomly chosen bases either using diagonal or rectilinear.

Via Public channel (two way communication)
Step 1: Alice uses public channel to inform Bob the polarization state has chosen for every bit she sent without informing actual bit value.
Step 2: Bob compares the list of polarization states he got from Alice with the one he obtains using random bases.

Step 3: Combination of these two lists can be used as their raw key which is not fully secret some bits may be intercepted by Eve during the transmission.
Step 4: The communication is still in continuation in public channel and can be divided into four main phases in order to get the correct key:

(a) Sifting raw key
(b) Error estimation
(c) Error correction
(d) Privacy amplification

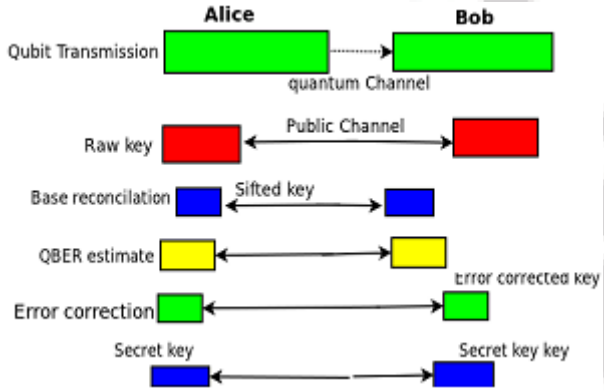

Figure 2: Phases of QKD protocol

4. Wireless Networks and Their Security Mechanism

- Wireless network is defined as a computer network that is not connected by any kind of physical media (cables etc.).
- Wireless networks provide the transport mechanism among devices and the conventional wired networks.
- Wireless networks are many but they are frequently classified into three categories based on their coverage range, WLANs, wireless wide area networks (WWAN), and wireless personal area networks (WPAN)

4.1 Wireless Standards

Wireless technologies follow a variety of standards and offer various levels of security features. Here discussion of wireless standards is confined to the IEEE 802.11.

4.2 802.11Wireless LAN Security

IEEE 802.11 provides the basic security services for the wireless LAN environment which are as follows:

(a) Authentication: A primary aim of WEP was to provide a security service to verify the identity of communicating client stations.
(b) Confidentiality: Confidentiality or privacy was a second task of WEP. It was developed to provide privacy equivalent to a wired network.
(c) Integrity: WEP was a security service developed to make sure messages are not tampered in transit between the wireless point and access point in an active attack.

4.3 Security Problems with the IEEE 802.11 Standard

There are some serious weaknesses of WEP:

Several users in a wireless network sharing the same key for long periods of time, is well-known security vulnerability. This drawback is due to the lack of any key management facility in the WEP protocol. The initializing vector (IV) in WEP is a 24-bit field sent along with text portion of a message. This 24-bit string, employed to initiate the key stream which RC4 algorithm generates, is a relatively a small field used for cryptographic purposes. Repetition of the same IV produces identical key streams for data protection, and small IV guarantees that they will repeat after a short span of time in a busy network. Moreover, the 802.11 protocol does not tell how the IV is set or changed, and individual wireless NICs from the same vendor may all generate the same IV sequences, or some wireless NICs may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to encrypt the cipher-text.

4.4 RSN and IEEE 802.11i

IEEE 802.11i standard is made to provide enhanced security in MAC layer for the network 802.11. It defines two classes of security algorithms: Robust Security Network Association (RSNA) and Transition Security Network (TSN).IEEE 802.11i describes two new confidentiality algorithms to address those two cipher suites, namely Temporal Key integrity Protocol (TKIP) and Counter-mode/CBC-MAC Protocol (CCMP) respectively.

IEEE 802.1X offers an effective framework for authenticating, managing keys and controlling user traffic to protect large networks. It employs the Extensible Authentication Protocol (EAP) to allow a wide variety of authentication mechanisms, which we are going to keep it in our current work. It, is noted that 802.1X authentication process happen among three main elements. The Authenticator or the Access Point gives permission to only the supplicants who are authorized by the authentication server to gain access to the network. RSNA defines two types of key hierarchies to divide initial key material into useful keys. The two key hierarchies are: Pair wise key hierarchy, which is used to protect unicast traffic and, Group key hierarchy which is used to protect multicast and broadcast traffic. We can show the Pair wise key hierarchy.

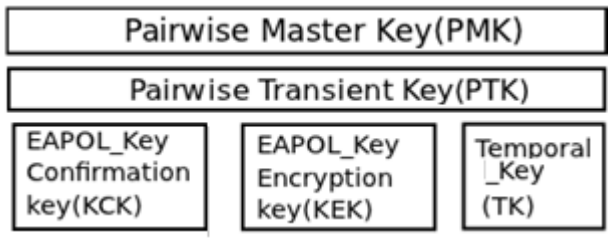

Figure 3: Pair wise Key hierarchy

Figure shows the pair wise Key hierarchy .The PMK received from the Authentication server throughout 802.11 authentications is employed to generate PTK by applying Pseudorandom Function (PRF).The PTK gets divided into

three keys. EAPOL-Key Confirmation Key (KCK) is the first key. 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 in encryption of Group Temporal Key (GTK).The third key is the Temporal Key (TK),is used by the data privacy protocols for encryption unicast data transfer.

5. Quantum Cryptography Implementation in Wireless Network

As our main objective is to offer secure key distribution in wireless networks using Quantum Cryptography, we have found that IEEE 802.11 family (Wi-Fi) best suits to get married with QKD, the environmental changes 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.

5.1 Proposed Protocol

The quantum key distribution protocol SARG04 is implemented as shown in flows 3 - 6 of Figure

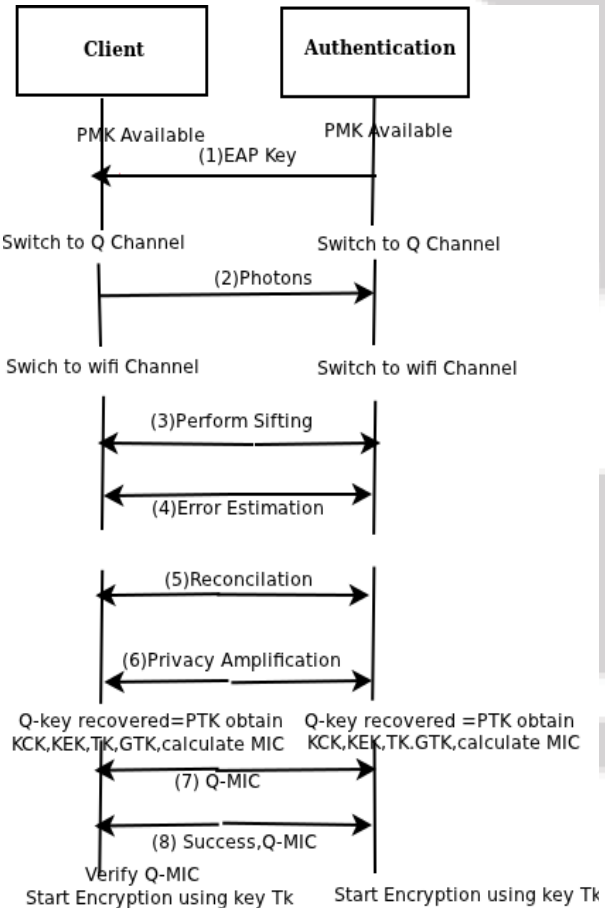

Figure 4: The proposed 4-phase Handshake protocol

At first PMK is shared, then the transmission process gets switched over to the quantum channel. Requester would keep track of all the photons that is received and length of bases it used to measure the photons. As soon as transmission of photon finishes, the wireless channel takes charge for the rest of the protocol implementation. The key obtained by both parties will have errors due to eavesdropping etc. The next 3 stages of QKD remove all the error in order to obtain the final encryption key. The sifting process removes all the bits which were recorded against using wrong bases .The error correction process ascertains the amount of error level within the threshold level so as to continue communication.

For completing this, quantum transmission should make sure to send sufficient number of photons so as to improve quantum key at least equal or greater than the PMK. In case of CCMP, PTK is 256bits, while TKIP uses 384 bits for PMK. Hence, at this stage, we remove any extra bits of quantum key so that it has same length as PTK. Now we have this stripped quantum key as the PTK. Once PTK is there, we can repossess the key picking order having all other keys using the PRF. From PTK, we derive other keys such as KEK, KCK and TK, from KCK, MIC can be derived. We employ this MIC in our ongoing protocol messages for mutual authentication. At this stage, XOR operation is performed with the MIC and the first part of bits of equal length in PMK. We name this MIC as Quantum MIC (Q-MIC).

Q-MIC = (MIC) XOR (first bit of PMK equivalent to the length of MIC)

Supplicant releases Q-MIC to authenticator as shown in flow 7 of figure 4. While receiving Q-MIC, authenticator checks the Q-MIC. Since the authenticator possesses all the key hierarchy, it can find out its own MIC and compares with the one came from the supplicant. If they match the supplicant is authenticated. We find out some of the flaws of 4-wayhandshake. It was explored that the message 1 of 4-way handshake may fall prey to Denial of Service (DOS) attacks. Intruders can send a huge bulk of message to the supplicant after the 4-way handshake has finished, that may cause system to fail. Since QKD protocol is used, nonce values used in the message flow are not required. Current hardware devices for quantum transmission need Line of Sight (LOS) between the supplicant and the authenticator for photon transfer although; there has been lot of new research happening in this area to remove the need of LOS for quantum transmission. Kedar and Arnon did one such research work by using wireless sensor network to have nonline of Sight (NLOS) system for optical communication.

5.2 Privacy Amplification

Privacy amplification is used to enhance the correlation between their key strings by reducing the information of Eve about the result to the desired level of security in QKD protocol. Privacy amplification is used to remove all error bits present in their individual keys to get the final matching keys. Unlike other handshake phase protocol, the number of communication flows required in privacy amplification is not known in advance. Since the number of cycles required depends upon level of errors present in the key and the privacy amplification protocol. The time to complete the privacy amplification work in this simulation model depends upon several key factors:

(i) Main key length
(ii) Initial block size length of partition
(iii) Cycle count parity check will run for

Throughout this model error rates of different levels for different keys and lengths have been sent into the Simulink model. The graphical representations of observations are as follows:

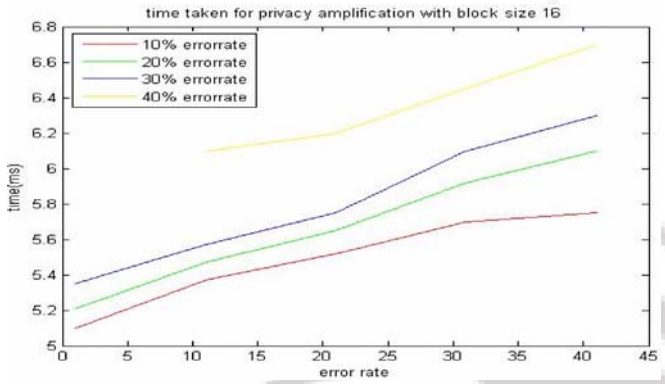

Figure 5: Time to complete privacy amplification for error rate.

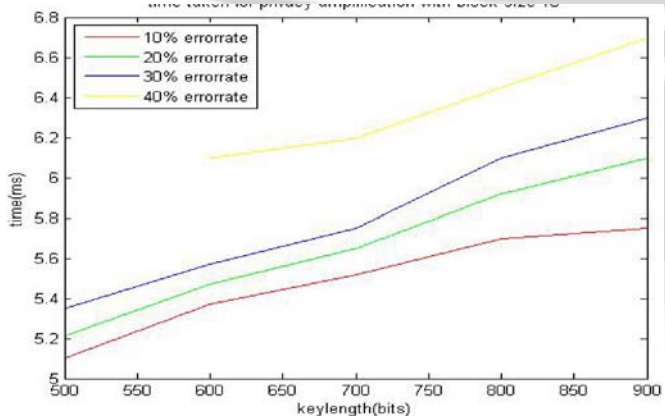

Figure 6: Time to complete privacy amplification for key length

6. Conclusion

The benefit of quantum cryptography over classic cryptographic systems is that it provides unconditional security to combine with IEEE 802.11 networks. For a small wireless networks IEEE 802.11, QKD suits more as compared to other present secure data communication mechanism. Modifications nature proposed in this work is focused on the process while the key is being distributed. Here QKD based 4-phase handshake protocol has been brought in place of the 4-way handshake protocol of IEEE 802.11. Modification is done only in the key distribution portion while remaining IEEE 802.11 protocol remains unchanged. The objective is to observe the behavior of the modified key distribution process under various input conditions.

References

[1] 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.

[2] 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

[3] 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.

[4] 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.

[5] Valerio Scarani Antonio Acin Gregoire Ribordy, Nicolas Gisin, "Quantum cryptography protocols robust against photon number splitting attacks".APS, Phys.Rev.Lett, Vol. 92, 2004.
Rivest R., Shamir A., and Adelman L., "On Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979)

[6] IEEE 802.1X, IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control, December 2004

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

[8] Naik, R.,Dr P.Chenna Reddy, U. K., and Dr.Y.V.Narayana. International Journal of computer Networks and wireless communication 1(1) Dec 2011

Author Profile

Jarrar Ahmed has received the MTech degree in Computer Applications from Indian Institute of Technology Delhi in 2012 and did Msc in mathematics from CCS University Meerut.