# Analysis of Network Performance Using Aspect of Quantum Cryptography

Nisarg A. Patel, Hiren B. Patel

***Abstract***—Quantum cryptography is described as a point-to-point secure key generation technology that has emerged in recent times in providing absolute security. Researchers have started studying new innovative approaches to exploit the security of Quantum Key Distribution (QKD) for a large-scale communication system. A number of approaches and models for utilization of QKD for secure communication have been developed. The uncertainty principle in quantum mechanics created a new paradigm for QKD. One of the approaches for use of QKD involved network fashioned security. The main goal was point-to-point Quantum network that exploited QKD technology for end-to-end network security via high speed QKD. Other approaches and models equipped with QKD in network fashion are introduced in the literature as. A different approach that this paper deals with is using QKD in existing protocols, which are widely used on the Internet to enhance security with main objective of unconditional security. Our work is towards the analysis of the QKD in Mobile ad-hoc network (MANET).

***Keywords***—QKD, cryptography, quantum cryptography, network performance.

## I. Introduction

IN today's era, everyone wants their necessary data to be handy, portable and accessible from almost every place they visit throughout the day and this is made possible by using wireless networks. Wireless networks [1], as the name suggests, are those networks that are not connected by any physical means such as Ethernet cables and thus provide the user with great mobility and convenience. Also, it saves one from the expenses on the cables that would be required if wired network is chosen as well as makes it easier for moving the base of the devices from location to another by just moving the machine along with the wireless network card [7].

A wired network helps in point to point transfer, that is, sends data between any two devices that are connected with each other through an Ethernet cable but in case of wireless networks, the transfer of data is a broadcast service where the data are sent to all possible directions in the medium within a limited range as the medium of data transfer is air here and not cables. Wireless networks consist of four basic components: Transmission of data using air waves, access points (AP) to establish a connection to the public or private (organization) network and the wireless client operated by the user. Fig. 1 shows the basic wireless networking components.

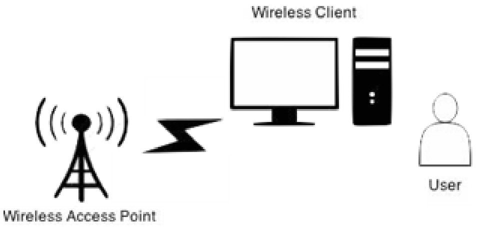

Fig. 1 Wireless networking components

## II. Security Issues in Wireless Networks

Wireless networks do not promise quality of service during transmission, and chances of intrusion into such networks are very high since the transmission here takes place through the medium of air and not cables [3]-[5]. So, it does not only require protection against uninvited users from accessing the network but also needs to secure the users' private data that are being transmitted. The general security issues for wireless networks are as follows [2]:

1) *Confidentiality*: The data being sent across the network is encrypted during transit so as to ensure that the information is read only by the intended user and hence authentication of the receiver is required as well who will be given the key for the decryption of the received data [6]-[8].
2) *Integrity*: Wireless networks are exposed to attacks that would harm the data's integrity.

The integrity prevention methods applied are similar to the ones used in wired networks [9], [10].

3) *Availability*: Wireless networks are vulnerable to denial of service attacks. Radio jamming can be used to restrict the availability of network. Another attack called, battery exhaustion attack is also arisen where unauthorized users repeatedly send messages or data to connected devices and hence runs down the device's battery [22].
4) *Eavesdropping and Authentication*: Wireless networks are broadcast as mentioned earlier, hence there are a higher number of access points, and these access points can be used to enter the network. Preventing this eavesdropping is necessary [15].
5) *Blue Snarfing or Blue jacking*: These are the attacks made using Bluetooth in order to tamper data or data theft [21].
6) *War Driver*: Another type of security attack where a wireless device (like laptops) somehow tries to connect to unprotected network and could record the private data of the user connected to the same network [20].

Nisarg A. Patel (Research Scholar) is with the Faculty of Technology and Engineering, C. U. Shah University, Wadhwancity, Surendranagar, Gujarat, India (e-mail: nisargpatelce31@gmail.com).
Hiren B. Patel (Professor & Head) is with the Department of Computer Engineering LDRP Institute of Technology & Research, Gandhinagar, Gujarat, India (e-mail: dp.project31@gmail.com).

## III. Literature Review

Quantum cryptography [7] is an evolving technology that provides safety and security for network communication by performing cryptographic tasks using quantum mechanical effects [18]. QKD is a technique that is an application of quantum cryptography that has gained popularity recently since it overcomes the flaws of conventional cryptography. QKD makes the secure distribution of the key among different parties possible by using properties of physics [14].

The quantum states of photons are used and the security key information is transmitted via polarized photons that contain the message denoted by bits (0 or 1) and each photon contains one bit of quantum information called as Qubit [17]. The sender sends the polarized photon to the receiver. At the receiver end, the user determines the photon polarization by passing it through a filter and checks for any modifications in the received bits of photons when compared to the bits measured by the receiver. Any modifications found would show that there has been an intrusion from a third party because the intrusion would irreversibly change the encoded data in the photon of either the sender or the receiver [11], [12]. This method is based on the Heisenberg's uncertainty principle that states that the quantum state cannot be measured without disturbing the state of either the sender or the receiver and hence introducing an anomaly in the quantum system that can be noticed by users as an intrusion [3].

Thus, Quantum cryptography applies the principles of physics governed by the laws of quantum mechanics for distributing the secret cryptographic key among the parties involved in the cryptosystem in a manner that makes it next to impossible for a third party to eavesdrop [13], [14].

### BB84 QKD Protocol

In order to facilitate QKD many protocols exist such as: BB84 [8], B92, Six-State, SARG04 [9], Ekert91. Among these protocols, BB84 is the most popular and widely used protocol for key distribution in practical systems.[24]

Bennett and Brassard proposed BB84 protocol in 1984. The protocol consists of two main channels used for transmission [16]:

1) Quantum channel: One-Way communication.
2) Classical channel: Two-way communication.

BB84 allows two parties conventionally a Sender and a Receiver to establish communication by a common key sequence using polarized photons [19].

Key exchange and key sifting are done as follows. Using Quantum channel (Raw Key Exchange):

- The Sender encodes the information in random bits of 0 & 1 and uses randomly selected bases (rectilinear or diagonal) to transmit bits in it as shown in Fig. 2. Bases for each photon is chosen at random and the sender repeats this in order to send all the photons to the receiver [18].
- The receiver at the other end selects the basis (rectilinear or diagonal) at random to measure the received photons being unaware of the bases used to encode the photons by the sender [8].

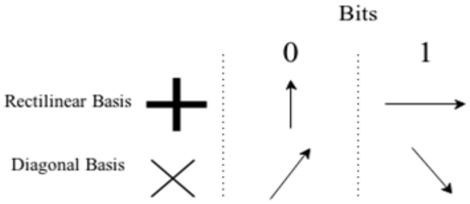

Fig. 2 Photon Polarization using Bases

After receiving all the photons, the receiver now communicates with the sender using the public channel for key sifting [11].

Using Classical channel (Key Sifting):

- Receiver informs the Sender what bases he used to measure the photons and Sender responds by saying if it matched the bases used [10].
- Both agree on to the correct matching of the bases used and without announcing the actual value of information. After discarding all the data on the polarizer bases that did not match, both are left with two key strings of shorter sequences, known as the raw keys [12].

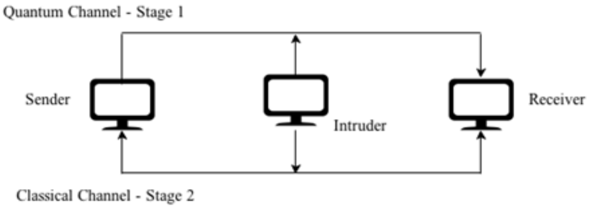

Fig. 3 QKD Setup

The bits that match make up the secret raw key which is not complete key and the communication still continues between the two comprising of the following steps: [5]

1) *Error estimation:* In order to check if any eavesdropping has occurred, the raw keys are compared. If intrusion takes place, error would be introduced in one of the raw keys and the two keys on comparison will not match [3]. Hence, the errors are to be estimated and if the error rate exceeds the threshold QBER (Quantum Bit Error Rate) for quantum transmission, the key is aborted and they try sending data again [4], [20].
2) *Error correction (Reconciliation):* Performed to get the common key by removing the errors in the raw key by using a protocol from the many available protocols. The most widely used protocols are Cascade (based on optimal linear codes, uses and releases less data, end by performing parity based error correction), Winnow (based on exchange of parity and helps correcting single errors using hamming hash function) [9].
3) *Privacy Amplification:* In the end both Sender and Receiver will hold, not completely private but identical strings of bits the information of which can be partially obtained on eavesdropping by a third party. The privacy

amplification step helps remove this partially obtained information by the third party and hence make a correct secured secret key [11].

## IV. Proposed Protocol

In order to overcome the security issues of key distribution this paper employs new QKD protocol, which is an improved version of BB84 [16]. Fig. 4 shows the proposed QKD protocol being implemented in the proposed 4-way handshake protocol [19].

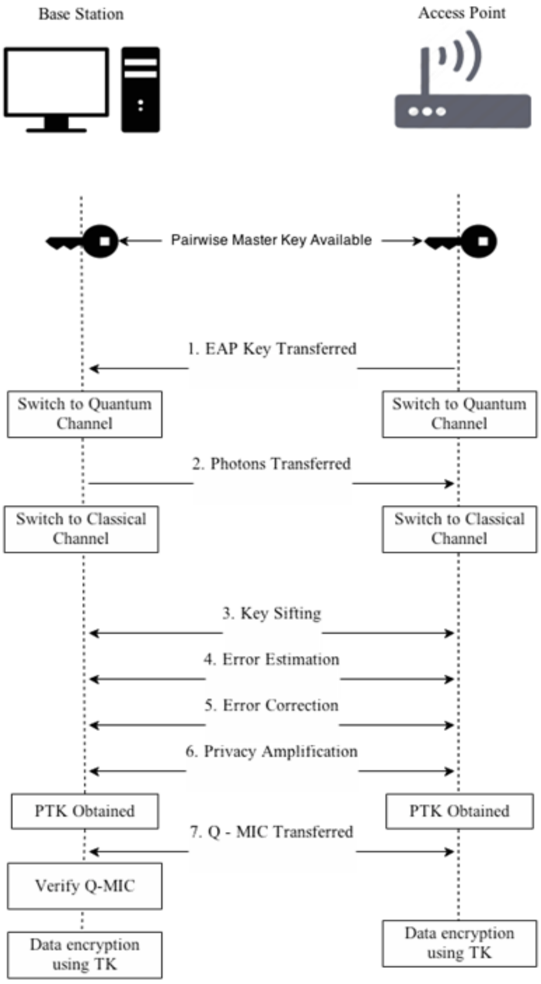

Fig. 4 Proposed 4-Way Handshaking Protocol

The steps involved in the proposed protocol are as follows:

1. Initially the PMK is shared between the BS and the AP. Then, the transmission process is switched to the quantum channel.
2. BS sends all the polarized photon to the AP using bases at random. As soon as the transmission of photons are finished, the channel is switched to classical [1]-[3].
3. The next three stages of QKD are applied to remove all the error and obtain the final encryption key.

In order to have secure communication, quantum transmission should make sure to send sufficient number of photons so as to improve the quantum key. PTK key (256 bits) is obtained by stripping the quantum key (384 bits) to match the number of bits. Once the PTK key is obtained the normal 4-way handshake protocol is followed wherein the MIC is derived for mutual authentication. The MIC is operated using an XOR operation and the first part of bits of equal length in PMK. This MIC is called as Quantum MIC (Q-MIC)

Q-MIC is transferred between both parties and verified, after which the temporal key is used to start encryption and communicate. Since the QKD protocol is used, Nounce values used in the original handshake are not required. Other advantages of applying this protocol are specified in the following section.

## V. Advantages of Quantum Cryptography in Wireless Networks

Quantum cryptography is still a long way from being used in information transfer, since the real-world implementation is far from the theoretical technique. But still, there is no debate that quantum cryptography is a true breakthrough in network security. Some of the advantages of applying quantum cryptography in wireless networks are as follow [12]:

- Quantum Cryptography approach does not depend on mathematics models but instead is based on physics principles for decoding an encoded data making it virtually non-hack able and requires few resources for its maintenance.
- QKD is found useful for different categories of wireless networks as a means for connecting devices to different access points in close proximity. Hence making it more efficient for communication with fewer cables [21].
- Intrusion-eavesdropping can be detected or prevented from the vision of users only since the range under the coverage of wireless networks is not too large in case of WPAN networks while for WLANs, the 802.11 wireless networks expand to the larger areas taking much benefit of the Quantum Cryptography [22].

Wi-Fi network usage is developing day by day also including the usage of hot-spot services very often. Since varied services (fields of national defense, aircraft communication etc.) are performed using Wi-Fi and hotspot its security is very important for all level of users and QKD has the ability of providing this security at the highest levels [15].

## VI. Conclusion And Future Enhancement

The main goal of this research work is to show a method to improve the security aspect of WLANs. It has been shown that the integration of Quantum Cryptography in Wireless Networks has great prospective in terms of better network security.

Key management and distribution are difficult using classical cryptographic algorithms, but the proposed approach provides a better solution for this problem. Research has shown that use of QKD to distribute network key raises the security and makes it harder for an eavesdropper to interrupt communication. With the proposed modification, this research has achieved the main objective of improving security of WLANs.

## References

[1] Mohammed Moizuddin1, Dr. Joy Winston, and Mohammed Qayyum, "A Comprehensive Survey: Quantum Cryptography" IEEE International Conference on Advanced Computing, 2017.

[2] Ms. V. Padmavathi, Dr. B. Vishnu Vardhan, and Dr. A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey" IEEE 6th International Conference on Advanced Computing, 2016.

[3] S. Meier, C. Cremers, and D. Basin, "Efficient Construction of Machine-Checked Symbolic Protocol Security Proofs," J. Computer Security, vol. 21, no. 1, 2013, pp. 41–87.

[4] B. Schmidt et al., "Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties," Proc. 25th IEEE Computer Security Foundations Symp. (CSF), 2012, pp. 78–94.

[5] Hidema Tanaka, Security Analysis of Generalized Confidential Modulation for Quantum Communication International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013.

[6] 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.

[7] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," International Journal of Next-Generation Networks (IJNGN), vol. 1, pp. 1-10, 2009.

[8] Symmetric key cryptography using random key generator, A. Nath, S. Ghosh, M.A. Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2, P-239-244.

[9] Nur Atiqah Muhamad and Zuriati Ahmad Zukarnain, "Implemetation of BB84 Quantum Key Distribution Protocol's with Attacks", European Journal of Scientific Research, Vol.32, No.4, 2009, pp. 460-466.

[10] IEEE Std 802.11, 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 O(MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2007.

[11] ANSI/IEEE 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

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

[13] IEEE Std 802.11, 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 O(MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2007.

[14] Floriano De Rango, Dionogi Lentini, Salvatore Marano, Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i, EURASIP Journal on Wireless Communications and Networking archive, Volume 2006 Issue 2, April 2006.

[15] Ghernaouti-Helie, S., et al., Using quantum key distribution within IPSEC to secure MAN communications. MAN 2005 conference, 2005.

[16] Nguyen, T. M. T., M. A. Sfaxi, and S. Ghernaouti-Hélie, 802.11i Encryption Key Distribution Using Quantum Cryptography. Journal Of Networks, 2006. 1(5): p. 9.

[17] Le, Q. C. and P. Bellot, Enhancement of AGT Telecommunication Security using Quantum Cryptography. Research, Innovation and Vision for the Future, 2006 International Conference on, 2006: p. 7-16.

[18] Elliott, C., "The DARPA Quantum Network", Quantum Communications and Cryptography, 2006.

[19] Bhagyavati, Wayne C. Summers, Anthony DeJoie;"Wireless Security Techniques: An Overview"; InfoSec Conference, September 2004.

[20] J.-C. Chen, M.-C. Jiang, and Y.-W. Liu, "Wireless LAN Security and IEEE 802.11i", IEEE Wireless Commun., vol. 12, pp.27 -36 2005.

[21] Nur Atiqah Muhamad and Zuriati Ahmad Zukarnain, "Implemetation of BB84 Quantum Key Distribution Protocol's with Attacks", European Journal of Scientific Research, Vol.32, No.4, 2009, pp. 460-466.

[22] Symmetric key cryptography using random key generator, A. Nath, S. Ghosh, M.A. Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2, P-.