International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229214

Distance Enhancement of Quantum Cryptography through MANET

R. Priyavani, Dr. N. Kowsalya
Assistant Professor, Sri Vijay Vidhyalaya College of Arts and Science, Nallampalli, Dharmapuri, India

Article Info
Volume 9, Issue 2
Page Number : 86-93

Publication Issue
March-April-2022

Article History
Accepted : 05 March 2022
Published : 20 March 2022

ABSTRACT

In the modern technology world, the cryptographic techniques are plays a major role. There are so many modern cryptographic algorithms are used to secure information through message transformation. Quantum cryptography evolved from the merging of physics and cryptography to reduce the threat that encryption encounters. It is one of the emerging fields in the computer technology. The primary objective of quantum cryptography research is to develop cryptographic algorithms and protocols that are resistant to quantum computer attacks and increase the communication distance. The various quantum cryptography protocols are demonstrated, as well as how this technology has led to the establishment of secure communication between sender and the receiver through using of MANET. We will look at the properties of quantum cryptography and the benefits of MANET it can provide in the future internet. One of the best ways for increasing the distance of message transmission over the internet is to use MANET in the field of quantum cryptography. An Ad hoc on demand distance vector (AODV) is a routing protocol for Mobile Ad hoc networks.

Keywords : Quantum cryptography, Quantum communication, Internet Security, MANET, AODV.

I. INTRODUCTION

Information Technology and Communication has advanced rapidly in recent decades. Cryptography is a method that is used to protect communication between parties from intruders. Security and cryptography are essential for every day communication via many networks. Traditional encryption methods for traditional networks are vulnerable to a variety of cyber attacks that cannot be utilized with quantum computers, and they require sophisticated mathematical calculations. Quantum cryptography was brought to light when European Union member recently declared a massive investment of $15million in the construction of a communication system that will not be vulnerable to advances in computing power and mathematics. For the time being, quantum cryptography is the only viable choice [8-9]. Many existing public key encryption algorithms (RSA, ELGamal[11], Elliptic Curve Cryptography (ECC) [12] will be rendered insecure in the quantum computer due to the quantum computer's characteristics. The field of quantum cryptography is still in its early stages. Its significance, however, cannot be overlooked or overestimated [8-9]. In 1994, a well-known mathematician named Shor devised quantum cryptography techniques for solving integer factorization problems in polynomial time. QKD protocols vary in terms of modulation techniques, encryption and decryption methods, and the way quantum channels are established. The initial QKD system, known as DVQKD, employs discrete variables and converts them using photon polarization. Mobile ad-hoc network (MANET) is a multi-hop wireless network that self-organizes and configures itself, with the network structure changing constantly. Each node in the MANET uses wireless communication network so easily can transmit the photons through infrastructure less network. Quantum cryptography is the only encryption system now available that is practically difficult to crack with any type of computer, even quantum computers.

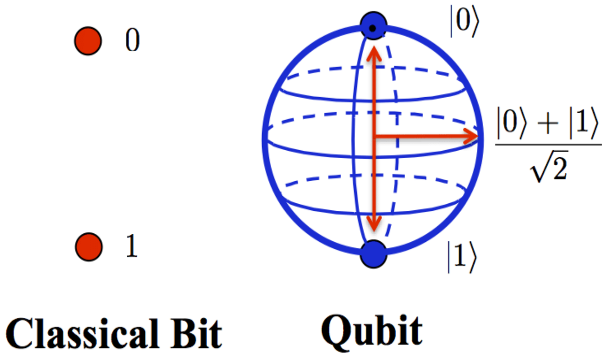
1. Overview of Quantum cryptography:

History

Stephen Weisner initially suggested quantum cryptography in the early 1970's with his paper “Conjugate Coding”. Bennet and Brassard, two scientists who were familiar with Weisner's views, were ready to publish their own. They developed the "BB84," the first quantum cryptography protocol, in 1984. In June 2003, a team from the University of Vienna used free space to send entangled photons across the Danube. The first quantum key-encrypted money transfer took place in April 2004 between two Austrian banks.

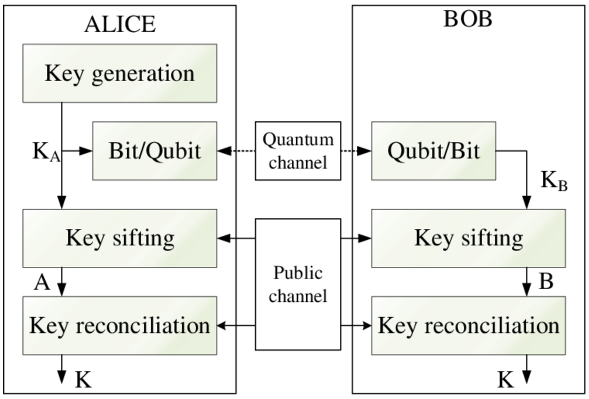
Quantum key distribution (QKD)

Quantum cryptography is built on traditional encryption concepts, but with the addition of a quantum key distribution scheme. Quantum key distribution (QKD) is a technique for developing secure communication. It allows you to distribute and share secret keys, which are required for cryptographic protocols. The study of secure communications systems that enable only the sender and intended recipient of a message to read its contents is known as cryptography. To make a system safe, cryptographic methods and protocols are required, especially when interacting across an untrusted network like the Internet. Traditional data-encryption cryptosystems rely on the complexity of mathematical algorithms, whereas quantum communication relies on physical laws to provide security. QKD allows two parties to generate and exchange a key that may be used to encrypt and decode messages. QKD works by sending numerous light particles, or photons, between two parties over fiber optic lines. Ones and zeros are made up of a stream of quantum states known Qubits' (Quantum bits). In quantum channels the entire message will be sent as Qubits from sender to receiver.



Process of quantum key distribution:

Quantum cryptography is based on two key principles of quantum mechanics: the Heisenberg Uncertainty Principle and the Photon Polarization Principle. Asymmetric key exchange can be used to exchange the actual key, as in the Diffie-Hellman key exchange protocol [19]. If implemented appropriately, QKD for key distribution in conjunction with the one-time pad provides the greatest possible security level.



The QKD consists of following steps,

- Quantum transmission
- Sifting
- Error estimation
- Error correction
- Privacy amplification

Quantum transmission:

The Qubits are exchanged between Alice and Bob. Alice and Bob will also require reliable sources of photons are required for transmission. Alice must select the bits and basis at random, whereas Bob must choose his measurement basis. Quantum mechanical processes, which are inherently unpredictable, are an excellent source of randomness.

Sifting:

Bob tells which photons he observed and on what basis he assessed. Because his basis decision did not correspond to hers, Alice advises him which measures to delete. These bits, as well as those not identified by Bob, are then discarded by Alice. Alice and Bob now have the identical string of bits in the absence of faults. The string name is called sifted key.

Error estimation:

To estimate their quantum bit error rate (QBER), Alice and Bob publicly compare a randomly chosen portion of the sifted key. To estimate accurately, the number of compared bits should be large enough. Eve's key information may be determined after the QBER is known. Even if the fault might be due to experimental flaws rather than Eve's presence, all errors would be assigned to her. Depending on how much information she has, the sifted key will either be rejected or processed further. This is called the error estimation.

Error correction:

The goal of error correction is to turn an error-prone sifted key into an error-free key via public communication without revealing any information about the concrete value of any single bit to an eavesdropper.

Privacy amplification:

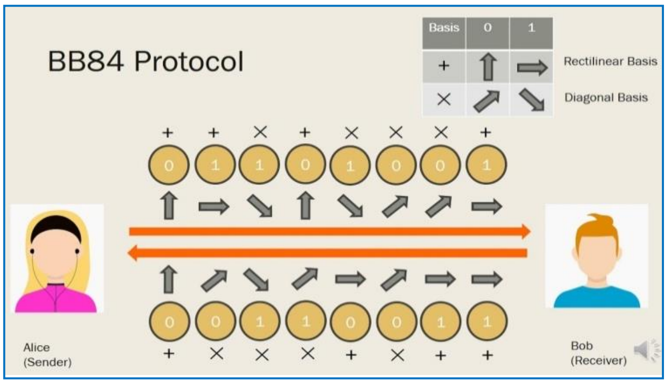
The privacy amplification procedure is implemented as a crucial stage in QKD by using universal hash functions. These hash functions, on the other hand, are usually built using mathematical complexity and are thus computationally secure.

2. Quantum key distribution protocols

There are so many Quantum key distribution protocols are available.

BB84 Protocol: [20]

Charles Bennett and Gilles Brassard (C.H. Bennett and G. Brassard, 1984) created this protocol. Heisenberg's Uncertainty Principle lies at the heart of its design. It was first described utilizing photon polarization states to transfer information, and was given the name BB84 after its creators and year of publication.



1. Alice and Bob communicate across a Quantum Channel in the first stage. Alice chooses an equal-length string of bits and bases (rectilinear or diagonal) at random.

2. Alice and Bob communicate on a traditional public channel in the second stage. Bob explains the measurement bases he used for each photon to Alice. In response, Alice notifies Bob with the bases for measuring the encoded bits that he correctly estimated.

B92 Protocol:

Charles Bennett created a simpler version of the BB84 protocol in 1992, encapsulating bits in photons with only two states. On a rectilinear basis, binary 0 is represented by 0°, whereas binary 1 is represented by 45°. The bases Alice must use to encode the bits are determined by the bits themselves. To measure the polarized photons, Bob still picks bases at random. He won't acquire any measurements this time if he selects the incorrect base. Transmissions over the quantum channel are used in the first phase of B92, whereas transmissions over the traditional channel are used in the second phase.

The EPR Protocol:

The EPR quantum protocol has three states. The polarisation states of an EPR photon pair are used to define this protocol. EPR stands for Einstein, Podolsky, and Rosen, who published a famous paradox in their essay in 1935. They challenged quantum physics' basis by showing up a "paradox." According to the authors, there are geographically separated pairs of particles known as EPR pairs whose states are linked in such a way that measuring one's selected observable A automatically dictates the outcome of the other's measurement. The protocol is divided into two stages, similar to the BB84 and B92 protocols. The first phase of the EPR protocol is carried out over a quantum channel, whereas the second phase is carried out over a conventional channel across a public channel for a fraction of a second.

COW Protocol:

Nicolas Gisin and colleagues developed the Coherent One-Way Protocol (COW protocol) in 2004 as a new protocol for effective quantum cryptography (Gisin N, 2004). It's been designed for use with weak coherent pulses. The key is retrieved using a fairly basic time-of-arrival measurement on the data line, as well as an interferometer created on an extra monitoring line, according to the protocol's description. The objective of this line is to allow the existence of a terrorist who would cause coherence to be broken by her attack to be monitored.

SARG04 protocol:

SARG04 is a quantum cryptography protocol that is based on BB84, which was the first of its type. BB84 has four states which can be used to create a new information encoding algorithm for the SARG04 protocol (V. Scarani, 2004). When the laser is attenuated, single-photon sources are replaced by pulses which are more reliable algorithm. The SARG04 protocol is used in situations where information is being emitted from a Poissonian source producing weak pulses and received by an imperfect detector.

II. An implementation of MANET in Quantum Cryptography

A mobile ad hoc network (MANET) is a network containing numerous free or autonomous nodes, commonly made up of mobile devices or other mobile components, which can rearrange themselves in a variety of ways and operate without the need for traditional top-down network administration. There are several configurations that may be classified as MANETs, and the possibility for this form of network is currently being researched. It is used in military project and DARPA (Defense Advanced Research Projects Agencies). Device in MANET is free to move in any direction independently. The network is established, controlled, and structured entirely by the nodes themselves, with no help from a centralized third party or fixed infrastructure. Apart from serving as a stand-alone network, ad hoc networks may also be linked to the Internet or other networks, therefore expanding connection and coverage to regions with no fixed infrastructures. Easy interaction, adaptability, efficient communication, and flexibility in infrastructure-less situations are some of the primary benefits given by MANETs. The quantum cryptography communication can be done through internet in the long distance in a secured manner.

The main objectives of research work are

- To Implement the MANET's Network Security using Quantum Cryptography through internet.
- To implement the QKD Technique in Network Data Transmission.
- The Packet Delivery Ratio will be examined.
- To calculate the throughput of various Network Scenarios.

3. Characteristics of MANET:

No fixed infrastructure: MANET is a network without any infrastructure. Making connections between nodes does not involve the use of any specific hardware. Through the wireless link, all nodes communicate with one another.

Multi hop routing: When a node attempts to transfer data to another node that is beyond of its communication range, the packet should be routed through one or more intermediary nodes.

Terminal autonomy: Each mobile node in a MANET is an autonomous node that may act as a host or a router.

Broadcast Communication: MANETs use a broad cast for communication. As a result, if ten nodes are within range of the source, all of them will receive the information. These nodes then forward the message by relaying it to the nodes within their transmission range.

Dynamic topology: Because nodes are allowed to travel freely in any direction at varied speeds, the network design can alter at any time. The nodes in the MANET dynamically build routing among themselves as they move around, producing their own network.

Routing at a high cost: Because MANETs no fixed infrastructure or access points, each node must perform the task of routing, which is time-consuming. Furthermore, when the destination is a long distance away, the routing cost has increased even more. As a result, neighboring contact is emphasized in MANETs.

Advantages:

- The major advantage of implementing a mobile ad hoc network is that it allows you to connect to the internet without the use of a wireless router. As a result, running an ad hoc network can be less expensive than running a regular network.
- MANET allows for connection failures since routing and transmission protocols are intended to deal such instances.
- MANETs may be more cost effective in some circumstances since they eliminate fixed infrastructure expenses and minimize power usage at mobile nodes.

Disadvantages:

- Resources are restricted due to a variety of restrictions such as noise, interference situations, and etc.
- There are no authorization facilities.
- Because of the lack of physical security, they are more vulnerable to attacks.

III. Security issues in MANETs

The mobile ad hoc network, or MANET, is an infrastructure-free network in which each node acts as a router, allowing the network to have a dynamic topology with nodes moving freely. MANET is vulnerable to malicious attacks and security breaches due to its lack of physical organisation. These attacks might be either internal or external in origin. Denial of service, congested connections, and misleading routing information assaults are examples of external attacks, whereas malicious nodes impersonating regular nodes to acquire secret information are examples of internal attacks. There are some attacks in MANET.

Denial of Service attack: A denial-of-service (DoS) attack is a type of network attack that restricts or prevents authorized users from accessing system resources.

Eavesdropping: When a hacker intercepts, deletes, or changes data sent between two devices, it is called an eavesdropping attack. To access data in transit between machines, eavesdropping, also known as sniffing or snooping, relies on unprotected network interactions.

Impersonation: An impersonation attack occurs when a hacker successfully assumes the identity of one of the legitimate participants in a system or communication channel. In the scenario that the verification process fails, the attacker can bypass it, acquiring access to private data as well as the ability to monitor network traffic. As a result of these security breaches, communications may be interrupted on a regular basis, reducing the network's efficiency. Regardless of the fact that so much research has been done in the domain of QoS (Quality of service), which includes analysing packet delivery ratio, latency, bandwidth, and other factors. Recent researchers have discovered the necessity for some hardware support or peer behavior evaluation to detect misbehaving nodes. The research community has already looked at common security techniques to solve the multiple security issues that MANETs experience.

IV. Quantum cryptography security in the internet

The most significant obstacle is the QKD mechanism's limited range of use. The reason for this is that when we try to transport the key over a long distance, the polarisation of photons may change owing to many reasons, such as when we try to amplify the Qubits, the state of polarization of these photons will be destroyed by the amplifier. Only a distance of 10 kilometers may be covered using QKD. Quantum cryptography techniques might be the first to be developed. At the single quantum information level, quantum mechanics is used.

In the future, internet security will be a top priority in the quantum cryptography. Because it is the aggregation of all information systems and the information environment for human life, the Internet should be safeguarded. Quantum cryptography is the first thought when it comes to the rising security dilemma in cyberspace. Using MANET will achieve the distance of transmission between sender and receiver. MANET provide infrastructure less network with limited resources. An intelligent routing strategy is required for efficient and reliable routing with limited resources, and it must be adaptable to changing network parameters such as network capacity, traffic density, and network partitioning so that different types of applications and consumers can have different degrees of QoS. The major benefit of utilizing a mobile ad hoc network is that it allows you to connect to the internet without the use of a wireless router. There are three types of routing protocols in MANET such as Proactive, Reactive and hybrid. Reactive protocols have a lower overhead but a higher latency, whereas proactive protocols have a higher overhead but a lower latency. These characteristics can secure cyberspace security in the future Internet.

V. CONCLUSION

Quantum cryptography is a new method of encryption that is based on quantum physics and classical cryptography. When compared to traditional cryptography, its most significant advantages are unconditional security and sniffer detection. One of the most difficult problems in MANET is safe routing. In order to improve efficiency, we use asymmetric key cryptography based AODV routing which uses the principle of public key cryptography to provide security requirements such as authentication, integrity, and non repudiation when establishing routes and transmitting data between MANET nodes. Ad-hoc On-Demand Distance Vector Protocol (AODV) is combination of destination sequence distance vector and data source routing protocol. It is used to discover and manage routes and also increase the distance of transmission through quantum cryptography. These qualities have the potential to solve a significant internet security challenge for the future Internet. Quantum cryptography ensures protection for a variety of applications in cyberspace (for example, the IOT and smart cities).

VI. REFERENCES

[1]. Tianqi Zhou, Jian Shen , Xiong Li, Chen Wang and Jun Shen “Quantum Cryptography for the Future Internet and the Security Analysis”, Hindawi Security and Communication Networks Volume 2018, Article ID 8214619, 7 pages https://doi.org/10.1155/2018/8214619.

[2]. Faisal Abbasi1, Pawan Singh, “Quantum Cryptography: The Future of Internet and Security Analysis”, Journal of Management and Service Science, 2021, Vol. 01, Iss. 01, S. No. 004, pp. 1-12.

[3]. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[4]. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[5]. M. Curty and D. J. Santos, “Quantum authentication of classical messages,” Physical Review A: Atomic, Molecular and Optical Physics, vol. 64, no. 6, 2001.

[6]. Laszlo Gyongyosi, Laszlo Bacsardi and Sandor Imre, “A Survey on Quantum Key Distribution“ in Info communications Journal, volume XI in June 2019.

[7]. Alharith A. Abdullah, Rifaat Z. Khalaf and Hamza B. Habib, “Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol”in 2nd Scientific Conference of Computer Sciences (SCCS), IEEE, 2019

[8]. Bennett, C. H., & Brassard, G. (1987). “Quantum public key distribution reinvented”, ACM SIGACT News, 18(4), 51-53.

[9]. Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). “Quantum cryptography”, Scientific American, 267(4), 50-57.

[10]. Bennett, C. H., & DiVincenzo, D. P. (2000). “Quantum information and computation”, nature, 404(6775), 247-255.

[11]. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[12]. Y.M. Tseng, “An efficient two-party identity-based key exchange protocol,” Informatica, vol. 18, no. 1, pp. 125–136, 2007.

[13]. C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, C. N. Asogwa, “An overview of Quantum Cryptography and Shor’s Algorithm”, C. H. Ugwuishiwu et al., International Journal of Advanced Trends in Computer Science and Engineering, 9(5), September - October 2020, 8397 – 8405.

[14]. Masahiro Takeoka, Mikio Fujiwara, Masahide Sasaki, “R&D Trends and Future Prospects of Quantum Cryptography”, New Breeze Winter 2019.

[15]. “Special issue: Quantum data communication”, Journal of National Institute of Information and Communications Technology, Vol. 64, No. 1 (2017).

[16]. Chainika Singhal , Ravinder Kr.Gautam , Lakshman Das, Manoj Kumar.Mishra , “Enhancement of Quantum Key Distribution Protocol”, IJESRT, ISSN: 2277-9655.

[17]. Alekha Parimal Bhatt,| Anand Sharma, " Quantum Cryptography for Internet of Things Security", Journal of Electronic Science and Technology, vol. 17, no. 3, september 2019.

[18]. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, no. 1, pp. 145-195, Jan. 2002.

[19]. Christof Paar and Jan Pelzl. Understanding Cryptography - A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg, 2010.

[20]. Mohamed Elboukhari, Mostafa Azizi, Abdelmalek Azizi, "Quantum Key Distribution Protocols: A Survey", International Journal of Universal Computer Sciences (Vol.1-2010/Iss.2) Elboukhari et al. / Quantum Key Distribution Protocols: A Survey / pp. 59-67.

[21]. Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Farhat Anwar, Athaur Rahman Najeeb, Mashkuri Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions", Indonesian Journal of Electrical Engineering and Computer Science Vol. 12, No. 2, November 2018, ISSN: 2502-4752,pp. 832~842.

Cite this article as :

R. Priyavani, Dr. N. Kowsalya, "Distance Enhancement of Quantum Cryptography through MANET", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 2, pp. 86-93, March-April 2022. Available at doi : https://doi.org/10.32628/IJSRST229214
Journal URL : https://ijsrst.com/IJSRST229214