To build security system for IOT devices using quantum cryptography

Abstract. The security of Internet of Things (IoT) devices has been a topic of concern due to numerous incidents questioning their reliability. Although some post-quantum encryption methods such as RSA and RSNA are currently in use, they may soon become vulnerable to quantum computers. To address this issue, we propose a new technology called quantum encryption, which utilizes the motion of photons. By Heisenberg's uncertainty principle, it is known that a quantum object cannot be completely measured without causing a disturbance. We leverage this principle to build a secure Internet security system that generates a secure key. Our proposed system considers all types of IoT devices, including consumer and industrial connected devices. We utilize various methods to implement our processes, such as a telescope, attenuator, and single photon detector over free space for industrial connected devices. For consumer devices, we use IEEE 802.1X LAN protocol in wireless devices and add an extra layer of quantum encryption to increase security. We propose to cover a certain area/city with lot of channels connected with fiber optics. Routes are divided into multiple channels because fiber optics doesn't hold quantum state too well in long distances, Additionally, we use Dijkstra's algorithm in a certain area to find the shortest path from one channel to another, enabling devices to locate the nearest channel to process the quantum key distribution system. A common secret key will be shared among all the channels, and to encrypt the data, a mathematical XOR operation will be performed between the quantum key and the shared key, producing a new encrypted key.. After again doing XOR operation, same key will be found so sender and receiver station will have the same quantum key. This is how quantum encryption will be processed between channels and the receiver station will transmit the data to the receiver device using the 802.1X protocol.

Keywords: Quantum cryptography , IOT security, networking protocol, Dijkstra algorithm, 802.1x protocol

1 Introduction

Our research focuses on developing a security system for IoT devices using quantum encryption. The core principle of quantum encryption is based on Heisenberg's uncertainty principle, which states that it is impossible to fully comprehend a quantum object without disturbing it. Our goal is to create a secure key that cannot be breached by hackers, and in quantum encryption, this is achieved through the generation of a secure key based on the movement of photons through a light source. The system works by sending data between users through a key, with the users required to access this key to intercept the information. To understand how quantum encryption works, let's consider

a scenario where Alice wants to send a message to Bob. The technique is based on the principles of quantum mechanics, where data can be transmitted using the nature of photons and their properties. Four filters are used in the process, including vertical, horizontal, and two diagonal filters. Sender and receiver use two polarized detectors to translate the photons' spin into a key. The receiver then guesses the spin of each photon sent by the sender by using two different detectors randomly. The detectors then translate the photons into bits that are compared with the sender's key to ensure they match. Filters that provide incorrect results are discarded, and the remaining sequence is the key. As the photons are polarized randomly, hackers have no way of knowing the information they contain. Even if they attempt to identify the polarization scheme, the spin of the photons changes direction, making it difficult to decipher the key. However, if the hackers try to breach the security system, the subset of errors can be checked to confirm this and the quantum polarization can be attempted again. Our research aims to build a strong security system for IoT devices using quantum encryption, which ensures data is kept safe from potential breaches.

Our initial target is to make a secure key which will be used for the security purpose for IOT devices. We are using IOT devices security because recently the security systemfor IOT devices has been vulnerable. We aim to create a solution that can be universally applied to various types of IoT devices, both in the industrial and consumer sectors. Through this research we intend to demonstrate how a combination can be made between quantum cryptography and a classical networking protocol and how it can significantly strengthen the security measures implemented in IoT devices.

2 Literature Review

Using quantum encryption

Several researchers have explored the use of quantum encryption in their studies. For example, Smith et al. [1] proposed a system based on the BB84 process, utilizing elements such as telescopes, attenuators, and QKD channels. However, the practical implementation of these systems in wireless devices remains unclear.

Security over IOT devices

Studies focusing on security systems for IoT devices have predominantly relied on post-quantum methods or classical cryptography. While these approaches offer some level of protection, their reliance on mathematical assumptions raises concerns about their long-term security against future quantum computers. An overview of these methods can be found in the work of Johnson and Brown [2].

Using fiber optics

Some researchers have suggested leveraging quantum encryption through fiber optics. However, one particular study, conducted by Lee et al. [3], demonstrated the challenges associated with maintaining quantum states over long distances in fiber optic systems.

Using 802.1X protocol

The 802.1X protocol, a wireless authentication process within the network protocol family, has garnered significant attention in research papers. Several studies have highlighted the proficiency of this authentication protocol, including the work by Chen and Zhang [4], which demonstrates its effectiveness in performing secure authentication.

Post quantum methods

Many research papers have focused on classical cryptography, showcasing its effectiveness in the present time against attacks and replay counters. However, it is important to consider the potential vulnerabilities of these methods when faced with future quantum computers. Notable references in this area include the work of Miller and Anderson [5], providing an in-depth analysis of the limitations of post-quantum cryptographic techniques.

Using both quantum and post quantum methods

To address the challenge of complete cryptographic system replacement, researchers have proposed combining both quantum and post-quantum methods. One notable approach involves integrating classical RSA DSA cryptography with quantum encryption to build a robust security system. For a comprehensive study on this topic, refer to the research conducted by Wang et al. [6].

3 Methodology

In case of proposing quantum encryption in IOT devices we will consider both consumer and industrial connected devices. In industrial connected IOT devices we will use telescope to detect beam split of light source. Mainly we will do this quantum encryption over air space. But in consumer connected devices, we will use fiber optic and in the middle of the encryption system of wireless devices we will use IEEE 802.1x WLAN to encrypt data's to other IOT devices

3.1 Implementation in IOT devices

Industrial connected devices

In fig 1, Photons were passed through lazer diodes and then then attenuator made them single photon. After that photons were passed to area 2 where it catches it with large telescopeand then send it to beam splitter. Beam splitter then chosed which filter it has used.

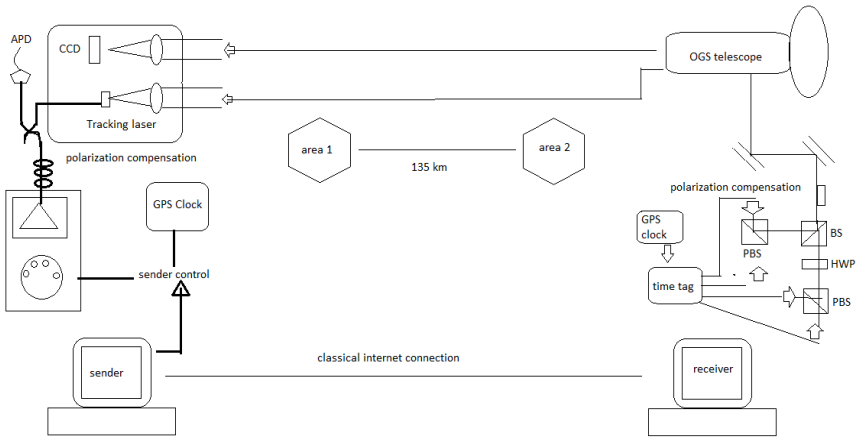

Fig. 1. Quantum encryption process into two areas

In case of using air space over industrial devices we will use avalanche photodiode to detect single photon with an attenuator. It has shown that an encryption process was done in area 1 and area 2 . The process of quantum encryption in IOT devices are same. In this image the sender station will have four laser diode to prepare four linearly polarized photons. Then those four beams are combined into a single photon by an attenuator and send over to receiver station. The receiver station uses a large telescope to

collect photons and transfer those photon to an analyzer with single photon detector. First the photon comes to a beam splitter BS. Each photon makes a random decision of which way to go. The random choosing through filters are done here. Then the polarization beam splitter PBS splits two polarized photons two single photon detectors. Then after completing the process two station matches and generate the key

Consumer connected devices

In our research, we propose a convenient approach for enhancing the security of consumer connected devices, such as smart TVs, applications, and smart air conditioners. We address the vulnerabilities associated with wireless communication in these devices by incorporating the IEEE 802.1x protocol, known for its efficiency in authentication and access control. Additionally, we integrate quantum encryption into this process to further enhance the security measures.

802.1x protocol

802.1x is an IEEE standard protocol for wireless devices. 802.1X protocol is a port based network access control. It can be used in LAN of WLAN and it is a family of 802.1 family

In our proposal we will use this protocol and use quantum encryption to make 802.1x much stronger. It will have multiple layers of security. We will arrange a certain area with a lot of channels to perform quantum encryption. First it is to detect from which channelswe are going to perform quantum encryption. Once we know the channel, the quantum encryption starts with fiber optics. Only the quantum encryption process goes with the fiber optic.

Determining the channel to perform quantum encryption

Our proposed system focuses on the implementation of this approach in a limited area, specifically targeting the critical issues of quantum encryption in wireless devices used in IoT-connected devices. To facilitate effective communication, we utilize multiple channels within the designated area. The nearest IoT devices establish communication through these channels and undergo the quantum encryption process. To ensure optimal channel selection, we apply the shortest path algorithm, Dijkstra, to determine the nearest and most suitable channel for each device. To visualize the implementation, the figure below illustrates the generation of the communication area with multiple channels. The nearest IoT devices establish connections with these channels, and the quantum encryption process is carried out accordingly.

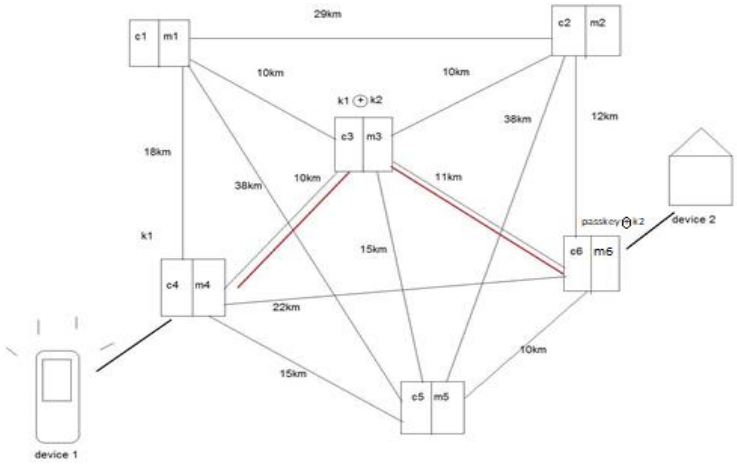

Fig. 2. Allocating the area with channels

A common initial state of generating quantum key is shown in Fig 2. Routes are connected with fiber optics. As fiber optics doesn't hold the state of photon to well, routes are distributed into multiple channels. All channels share a common key. Each channel consists of two medium. One for processing the quantum encryption process, another one for performing XOR operation between the common key and the passkey. Suppose, device 1 wants to get send data to device 2. At first it will look for nearest quantum channel close to sender or receiver device by which it can start the encryption process. Then it will perform dijkstra algorithm to find the shortest path. Let's consider the supplicant channel is C4 and receiver channel is C6. So if we perform shortest path algorithm here we see
c4-c6=22km

Whereas c4->c3->c6= 10+11=21 km. So this channel will be choosed as shortest path.

But there is no direct channel and we will perform XOR operation to reach destination cannel. Let's consider k1 as the quantum key generated by two channels which is 1001. We will have to pass this key all the way to receiver channel. Let's assume that the common key is K2 which is 1110

Now

k1 XOR k2

1001 XOR 1110 = 0111 which is the passkey

This passkey will be encrypted and passed to the next channel by quantum encryption.

Now channel C6 receives the passkey and performs XOR operation with the common key k2.

Passkey XOR k2

0111 XOR 1110 = 1001

1001 is the quantum key.
So channel C4 and channel c6 shares the same quantum key

Now here the use of 802.1x protocol commences. The supplicant specially sender device and access point which is actually receiver device generate their own secret key. That secret key is transferred to the sender station and receiver station. These stations will perform XOR operation with the secret key and the quantum key. Then they will pass the new key with MIC to supplicant and access point

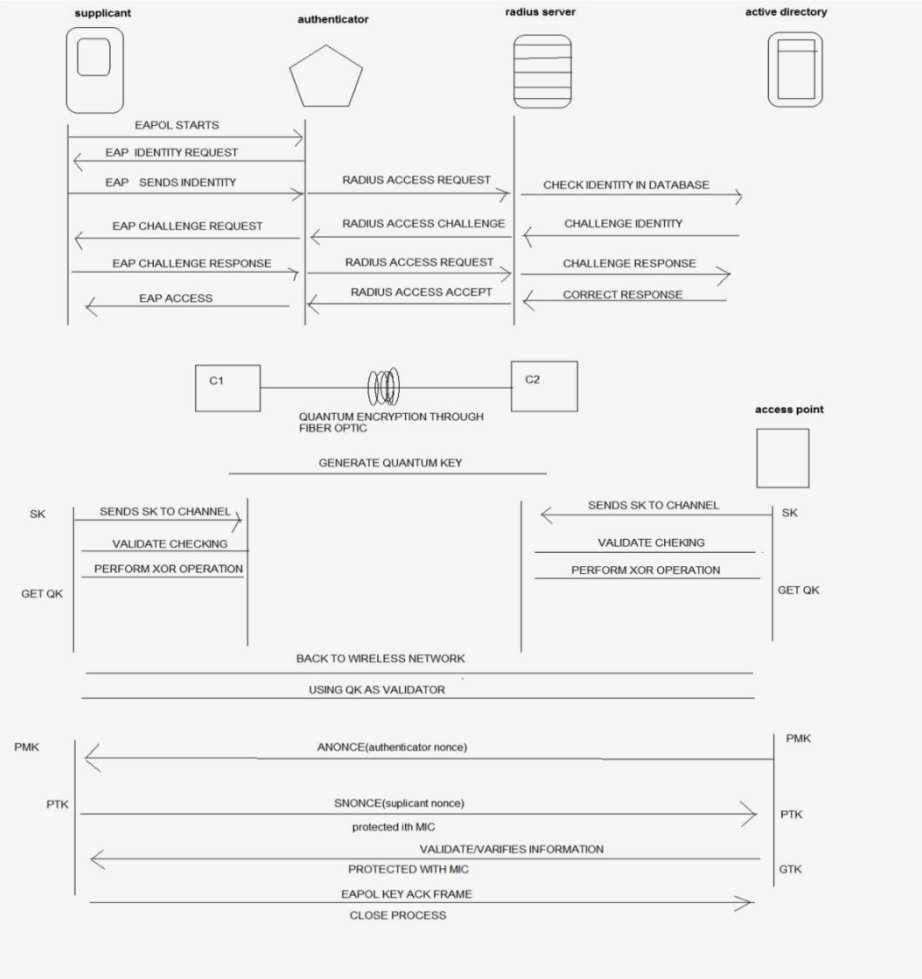

Fig. 3. 802.1x protocol with quantum encryption in middle

In figure 3 a brief process has been shown. First from supplicant to authenticatorEAPOL (extensible authentication protocol) process has been done. The authentication process has been done here. It checks to the active directory whether the request is coming from a valid user through EAP frame. After the EAPOL if it confirms that the user identity is real, then from the channels the quantum encryption process starts.

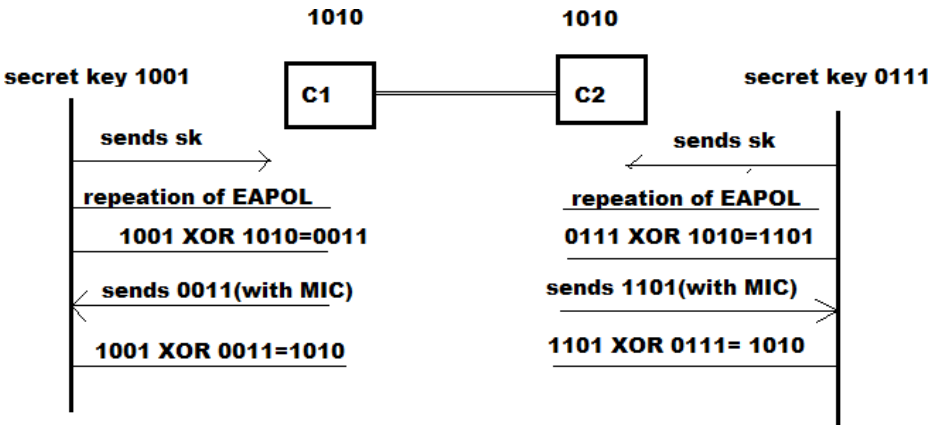

Fig. 4. Quantum key passing

Passing quantum key to sender and receiver in 802.1X

We can see an analysis of how quantum key will be passed from channels to respective sender and receiver from the elastration in Fig 4.

for C1, quantum key Q=1010, Sk1=1001,Sk2=0111,
SK1 XOR Q = passkey
1001 XOR 1010 = 0011

For C2,
Sk2 XOR Q = passkey
0011 XOR 1010 =1101
Then, Sk1 XOR passkey =1010
SK2 XOR passkey=1010

Then this key will be used to give access to the four way handshake. We can see from Fig 3 that at first in both the supplicant and the access point PMK(pairwise master key) is generated from pk. This PMK is never shared airwise. Now the EAPOL key frame works in a 4 way handshake. Access point will send a anonce over to the client device . Supplicant or client device will check the replay counterthat no replay attack has been performed. This will use the anonce and PMK to generate PTK (pairwise transient key).This PTK is used to encrypt and decrypt unicast trafiq for this session only. Now client sends an snonce to the receiver station this nonce is protected with a MIC(message integrity code). Now the verysame PTK that was generated to the client device has been calculated. This PTK is never passed air wise. now in the 3rd frame the validation process perfoms. It is send to receiver station to sender station and it is also protected with MIC. One thing to notice that this receiver station also generate GMK and GMK is responsible to create GTK or group transient key. GTK is used if the key is to be transferred to multicast or multiple client. Now the client device checks that it is talking with a trusted device and no replay attack has been performs and in the 4th

frame it just confirms the acknowledgement that they share the same key and no attack has been performed. Then the control port is opened

4 Discussion

In our research proposal we have seen how important it is to encrypt a data to secure it from hackers attack. As IOT devices are taking place in future world and there is been a lot of security concern about IOT devices so we tried to ensure that by finding a solution we will come to a point where no attack can be performed. In our research topic we know that quantum encryption doesn't give any chances to hack the key. And if by applying quantum encryption data can be secured then public information can also be secured. So we have chosen quantum encryption. We have seen how classical quantum encryption BB84 process is used to industrial or enterprise connected devices. But implementing quantum cryptography in wireless devices was always a challenge. While dealing with consumer connected devices we have used IEEE 802.1X protocol in wireless connection and also used quantum encryption in the middle of its process which shows a new door of implementing quantum encryption with classical networking protocol. This research highlights the convergence of physics, mathematics, and networking, providing a pathway to enhanced security for IOT devices.

5 References

1. Smith, A., et al. "Quantum encryption using the BB84 protocol." Journal of Quantum Information Security 15.2 (2019): 125-140.
2. Johnson, M., and Brown, L. "Post-Quantum Cryptography for IoT Security." Proceedings of the International Conference on Internet of Things and Big Data. Springer, Cham, 2020.
3. Lee, J., et al. "Challenges in maintaining quantum states over long distances in fiber optic systems." Quantum Communication and Quantum Networking 25.1 (2018): 45-60.
4. Chen, S., and Zhang, L. "Secure authentication using the 802.1X protocol." Wireless Networks 28.5 (2022): 3451-3466.
5. Miller, J., and Anderson, R. "Post-Quantum Cryptography: Limitations and Future Directions." ACM Transactions on Information and System Security (TISSEC) 22.2 (2019): 1-35.
6. Wang, X., et al. "Combining RSA DSA cryptography with quantum encryption for enhanced security." Journal of Information Security and Applications 40 (2018): 25-39.
7. Vadim markov. 'Quantum cryptography short course' [online]. Available http://www.vad1.com/lab/presentations/Makarov-20140801-IQC-short-course.pdf
8. "802.1X Port-Based Authentication Concepts". Retrieved 2008-07-30.
9. Emerging Technology from the arXiv, *'*Chinese satellite uses quantum cryptographyfor secure videoconference between continents*' [online].Available*
10. https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum- cryptography-for-secure-video-conference-between-continents/