IJETAE
EXPLORING RESEARCH AND INNOVATIONS

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 8, Special Issue4, April 2018)

Quantum Networks: Possibilities of Hacking in an Unhackable Network

Shipra Sarkar[1], Dr.Shaligram Prajapat[2]

[1]Shipra Sarkar, Student, International Institute of Professional Studies
Devi Ahilya University, Takshashila Campus
Khandwa Road, Indore-452001, INDIA

[2]Dr.Shaligram Prajapat, Associate Professor, International Institute of Professional Studies
Devi Ahilya University, Takshashila Campus
Khandwa Road, Indore-452001, INDIA

Abstract **- As the network is growing at a very fast speed, stronger communication systems are required. The threat to the security of the network has increased the pressure on the companies to protect their most valuable asset i.e. data. The technical intruders leave no chance to either harm the data or steal the data. In this situation, quantum network has appeared as a boon to the network security. The use of qubits to represent information and use of very secure non-hackable key in quantum cryptography has boosted the security of the network. The quantum cryptography has emerged as an immense technology that has become a milestone in network security. But, there is a very popular saying that any code made by human can be broken by human. Following this concept, quantum cryptography in quantum network can also be cracked and systems can be hacked. Quantum networks are very secure and cannot be hacked as said by the top physicist. The emphasis of this paper is on how the security of the quantum network can be broken and what parameters can help the intruders in breaking the security of quantum network.**

Keywords **– Quantum Network, Quantum Cryptography, Quantum Key Distribution, Qubits, Speed, Eavesdropping, Network Security, Worm and Trojan Horse Attack, Phishing, WHA, Malvertisement.**

II. INTRODUCTION

Quantum computing processes information using law of quantum mechanics.Computers developed using quantum theories works on quantum bits(qubits)to denote zero and one with distinguishable quantum states.These computers are recommended for computation which need exponential amount of time require only linear amount of time using quantum computers.Using quantum computers would exponentially increase the speed of cryptographic computations. However, quantum computers are yet to see reality.

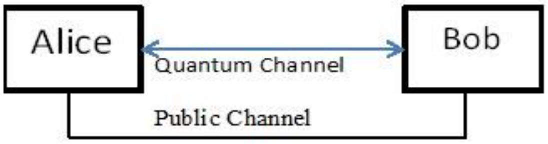


Fig 1.1 Communication between Alice and Bob.

Fig. 1.1 Alice and Bob has a two-way quantum channel which is using qubits for secure transmission.Quantum networks allow the transmission of qubits, between physically separated quantum machines securely using quantum cryptography. Quantum cryptography is based on the usage of the individual particles of light that is photons and their intrinsic quantum properties.[1]

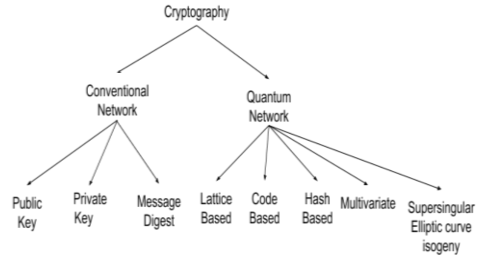
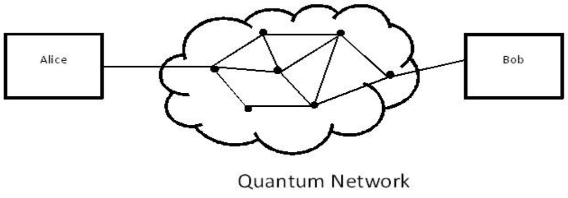


Fig 1.2 Types of Cryptography

Quantum cryptography makes use of Heisenberg's Uncertainty Principle for ensuring secure cryptography.



$$Key(C_i,t) * Plaintext(C_i,t) = h$$

Fig 1.3 Heisenberg's Uncertainty Principle in Quantum Network

Let C_i be the Cipher Text. $f(C_i,t)$ = Hacker's function attempting to extract key of Cipher Text C_i at time t. $g(C_i,t)$ = Hacker's function attempting to reveal Cipher Text Ci at time t. (decoding for plaintext) Then according to Heisenberg's Uncertainty principle : $f(C_i,t) * g(C_i,t) \leq h$. (1)

For perfect security, time variable key is essential, Thus Quantum Cryptography ensures data security.It uses QKD (Quantum Key Distribution) to generate secure keys which actually follows the non-violable laws of quantum mechanics. It has been considered most secure of all but 100% security is impossible in any network so quantum network can also be intruded. Quantum key is distributed among all those users who wish to communicate in a network. Several algorithms are used in quantum key distribution.

But still networks are vulnerable. The possibilities of phishing, clickjacking attacks, waterhole attack(WHA), eavesdropping and Worm and Trojan attack will increase in quantum networks although till now quantum cryptography has been proved to be one of the most secure cryptosystem of the century.

Table 1.1 Alice and Bob sharing secret key.

Alice's random bit	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**
Alice's random sending basis	+	+	×	+	+	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
Shared secret key	**0**		**1**			**0**		**1**

Quantum Networks are complex as they implement the transfer of qubits which are 100 times faster than any other network. The complexity of the network can be assumed by the fact that the quantum computers can operate at a speed that is much higher than classical computers i.e. 20 qubits can store million values in parallel. Quantum network is the resultant of interconnection of elementary quantum circuits. The property of 'quantum entanglement' has secured the network and provides fast speed. Quantum entanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. The determination of qubits for breaking the key is challenging since it is faster and also QKD uses unique keys which cannot easily break since qubits can exist either in 0 or 1 state or in both states at the same time. This property of qubits gives rise to challenge in determination of the key. Although key cannot be determined but can be destroyed. The speed of the qubits can give rise to errors in data. The data that need to be secured can be destroyed by the intruders. To secure the data, the speed of the qubits needs to be controlled. Else, chances of loss of data will increase. Another important factor is that quantum cannot travel a longer distance easily as they are energy packets. And energy packets can lose energy in middle of the path. This needs advanced system for the operation of quantum networks. The purpose of this research paper is to draw the possibilities of hacking in a quantum network which has been termed as unhackable.

III. RELATED WORK

In network security, encryption plays a vital role in secure transmission of data. In a QKD system, two system who want to communicate need to generate secret keys using random function. Many protocols have been introduced to solve the problem of communication system using quantum cryptography. The first protocol for quantum network was introduced by Charles H.Bennet and Gilles Brassard in 1984 named as BB84 [1]. The protocol was based on Heisenberg's Uncertainty principle. Later on, all the protocols that were introduced based on Heisenberg's Uncertainty Principle. Sender can transmit random secret key to Receiver by sending qubit string where qbits of secret key are encoded in the polarization of the photons. Since an eavesdropper cannot measure the photons and hence, qbit transmission occurs safely.

A. Types of Attack

Hacking can be possible in any type of network. It must be very difficult to hack but not impossible. There are several ways that the quantum network can be harmed:

1) *Eavesdropper:* While generating the secret key, an eavesdropper would try to listen to the key generated on random basis by sender. If he fails then receiver will get warning that someone else is present in the network. The probability of getting access to the right key is 1/3 and the probability of getting access to the wrong key is 2/3 [2]. But if the eavesdropper continuously tries to access the key then it is very much likely for the eavesdropper to detect the right key and gain access to the data and the receiver will also be fooled [3]. Another way the eavesdropper can listen to the key by using the entanglement property of the quantum. The eavesdropper can change the key by inserting its own qubit alternatively in the sequence of the key generated and hence disturbing the key. Trying this process again and again will result in generation of errors in the key and hence the data will be discarded and even now will affect the network channel since every time new key will be generated and hence may block the channel and decrease the performance of the network. Gradually this increases may lead to crashing of the system since this eavesdropping may increase, vulnerability to the system and worm attack may increase and lead to loss of data.

2) *Malware* : Quantum networks are vulnerable to Worm and Trojan Horse attacks. The tremendous speed of the quantum network makes it susceptible to Worm and Trojan Horse attack. As analyzed by the researchers, general Trojan Horse attacks on quantum key distributions via quantum channel can result in security breach in quantum network [4]. If worm is installed in quantum computers or while generating the key it will replicate the key and will break the security of the quantum keys. The worm can make the system susceptible to hacking. As the worm will send the duplicate keys to the intruder who has installed the worm in the system will gain access to that infected system. Because the speed of the quantum network is very high, worm can easily attack the network. Since, worm can replicate easily, the speed of quantum network will make the replication of worm easy. Moreover, the worm attack can destroy the network at a faster rate since their replication will

become faster in the quantum network. The Trojan Horse attack is more treacherous than any other attack since it does not replicate but is malicious. Quantum networks are more vulnerable to worm than any other virus since the implementation and maintenance of the quantum network is a strenuous job. It is very much vulnerable to attacks. Worms can even destroy and also crash the system and slow down the network and affect the network and may lead to huge loss of data. If worms are attached with the emails or any hyperlink then they spread in the network and infect other computers and hence may damage or block the quantum network and result in huge loss of money and data. Trojan Horse are more dangerous for quantum network since they cannot be detected easily, may lead to severe damage.

3) *Phishing:* It is an attack in which an attacker called phisher is engaged in malware activities. The phisher actually impersonates himself as a trustworthy third party like a known bank or company website and trick receivers into divulging sensitive information such as bank account number, credit card number, login password etc. The best way of the attack is submission of forms [5]. This type of attack by phishers in the quantum network is having very high risk if it is supported by worm attack, then the key can be easily gained. Thus, access to secret information becomes easier for phishers. If the secret information is gained through phishing than information security will be at risk. A security breach is there, that while trying to login, at that time only the phisher can keep track of the password and use it for fraudulent acts. Phishing technique is most sneaky way of hacking. Quantum networks are prone to phishing attack if some mechanism is not implemented to secure the data and quantum network. Even the quantum key distribution is the strongest one as quoted by the experts but more efforts are needed to make it more secure in the near future. If the website is used for phishing attack then the user must be alarmed about the malicious code attached with the website. The prevention from phishing is technically possible only if the QKD can be made used for websites also.

4) *Clickjacking Attacks:* Clickjacking is an attack that tricks a web user into clicking a button, a link or a picture, etc. that the web user didn't intend to click by overlaying the web page with an iframe. The attacker places clean advertisement on trusted websites so that user cannot detect the intruder. Cybercriminals are opportunistic and looks for weak link in a network that they can exploit [6]. Quantum networks are very secure but cybercriminal can be advantageous as with the increase in quantum computing users power will increase. Since quantum computers will strengthen the people, they will become more vulnerable to the attack. Users need to become more careful while using the internet as cybercriminals can easily trick the users with the help of malvertisement that can lead to attachment of greater number of malicious codes in the system. Within smallest fraction of seconds, users would be able to visit numerous websites and if they unknowingly visit such web pages that contain advertisement which has some attached code within it can result in interruption in the normal working of the systems and eventually can spread from one system to another and then systems get corrupted and data is lost. The network will be affected since if cybercriminals flood the network with malvertisement then the network will crash or block and results in huge loss of data.

5) *WHA (Waterhole Attack)*: Waterhole Attack is a type of attack that targets particular group of organization, industry and region. In this type of attack, the attacker guesses which website the group repeatedly uses and then infects that website with malware and in this way they hack the company/group [7]. The way this attack takes place, in quantum network this attack can create mess as if the hacker gets successful in attaching the malicious code then it will be easy for the hacker to

hack the group or company systems. Quantum network is vulnerable to waterhole attack since the attacker can get into the network of the group or organization and can steal the secret data and later on can destroy the network by attaching other malicious code and also gaining access to the systems may lead to other critical problems other than technical problem. Since the attackers can hack the group or organization, then can pave way for other intruders or hackers to insert malicious codes in the systems and then result in crash of the systems and network. Waterhole attack is a way through which other attackers can gain access to the systems and make it easier for them to get the secret data. The quantum network is safe but if a single security breach is found then it will become the biggest loophole in the system and will make it possible for the attackers to easily attack the network and a single failure in quantum network can create havoc in the organizations. This type of attacks just uses the fingerprints and gets their job done. The people could not recognize them and the job is secretly done. All these attacks can lead to either block the quantum network or may result in crashing of the systems or may damage the network. The security of the quantum network needs to be implemented carefully.

Type of Attack	Parameter	Degree of Severity	Possible Remedies	Key Issues
Eavesdropper [11]	Man in middle	Low	Encryption	How to block the eavesdropper?
Worm [4]	self replicating files	Medium	Using software removal tools	Stopping the replication of files
Trojan Horse Attack [4]	Getting access to exploited machine remotely	High	Antivirus and security awareness	Detection of Trojans in system is not easy..
Phishing on websites [5]	Getting information through fake representations of websites	Medium	By detecting fake urls which seems to be legitimate	Illegitimate Replication of legitimate websites
Clickjacking attack [6]	Malicious advertisement	Medium	User need to be careful while h clicking on such links	Detection of malicious advertisements and blocking them
Waterhole Attack [7]	Infecting websites	High	Frequent security audits.	Hide the search history.

Table 1.2 Results of various attacks on Quantum Network

The above table 1.2 derives the result of the various attacks where the parameters define the factors that are used to hack the network. Degree of severity defines how intensely systems can be infected. Possible remedies are meant to provide solutions to the hacking and key issues identify the major problem with the type of attack.

3. CONCLUSIONS

The quantum network are not implemented at large scale and the problem of different types of hacking are unseen yet as they will appear with the expansion and large scale implementation only, so this paper focuses on the problem of hacking in quantum network in future. From Table 1.2 we can conclude that different types of hacking techniques will result in different level of vulnerability to the quantum network. Although, the security of the quantum network is very high but every security settings has a loophole and the speed of the quantum can be treated as the biggest loophole by the cybercriminals. As the speed of the computers increases, the possibilities of the attack also increase. Hence, with the same concept, we can conclude that quantum network are also not 100% secure and cybercriminals can pave their way to hack the network, affect and steal the data and destroy the network in the nearby future.

Acknowledgement

I acknowledge my parent’s, my faculties for their support and guidance.

References

[1]Sneha Chouhan, D.H. Kulkarni, “Quantum Key Distribution using Different Techniques and Algorithm*”, International Journal of Engineering Research and Technology*, vol. 3 Issue 11, November-(2014).

[2]Cornell University Library.[Online].Available: https://arxiv.org/(1997)

[3] IEEE Xplore Digital Library.[Online]. Available: http://ieeexplore.ieee.org/(2016)

[4] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems”, *Physical Review A,* vol. 73 Issue 2, February-(2006).

[5] Dr.Radha Damodaram, “Study On Phishing Attacks And Antiphishing Tools”, *International Research Journal of Engineering and Technology (IRJET),* vol. 3 Issue 1, January (2016).

[6] Dr.P.B.Pathak, “Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks”, *International Journal of Advanced Research in Computer Science*, vol. 7 Issue 2,March-April (2016).

[7] N.Krithika, “A Study On WHA (Watering Hole Attack) – The Most Dangerous Threat To The Organisation”, *International Journal of Innovations in Scientific and Engineering Research (IJISER)*, vol. 4 Issue 8, August (2017).

[8] Top 10 Common Hacking Techniques You Should Know About.[Online]. Available: https://fossbytes.com/hacking-techniques/(2017)

[9]Quantum Networks in Space Closer to Reality.[Online]. Available: https://spectrum.ieee.org/(2017)

[10]Quantum Network Theory. [Online]. Available: https://johncarlosbaez.wordpress.com/(2013)

[11]Defeating eavesdropping with quantum illumination[Online]. Available : https://dspace.mit.edu/handle/1721.1/71512#files-area(2012).