Quantum Computing Networks against Hacking Threat

Ameena Sultana
Department Of CSE
Malnad College Of Engineering
Hassan , India

***Abstract*— As the technology is being more sophisticated and integrated these days, the cruel intensions of hackers to access our personal and private information is also exponentially increasing. The availability of information online on the tools and malware makes it easier for even non-technical people to undertake malicious activities. The importance of quantum computers has grown to a vast extent because of its advanced computing skills since it can store bits of information as either 0 or 1 or both simultaneously. Quantum systems are meant to provide the absolutely perfect secured data transmission but hacking of this transmitted information in this quantum computing world has also widely increased. Hence there is a need to secure and protect the transmitted information. One of the major threats these days is the cloning attack. But what if we use this cloning technique to perform hacking and secretly protect the data i.e., to make the external hacking easily detectable, large amount of information is encoded on a single photon so that the copies will get worse. So here the main idea is to discover clues that could help users protect quantum computing networks from the external attacks by building the first high-dimensional quantum cloning machine which will be capable of performing quantum hacking so that the message can be secured through the interception.**

Keywords*— *Quantum Cloning, Quantum hacking, Secure Quantum Message, Qubits, Interception

I. INTRODUCTION

Quantum computers have gained so much importance because of its property to hold bits of information as qubits, which can be 0, 1, or both simultaneously. These quantum computers are becoming trending as its importance to the world is gradually increasing. One of the best advantages of these computers is its advanced computing skills which has grabbed people's attention. The quantum computers which have the fast computing power can disrupt traditional businesses and can also challenge our cyber-security. People and the business makers need to be ready to see the quantum future which will emerge as a vast technology. In just less than the 10 years these quantum computers will surely begin to perform excellently everyday than the traditional computers, which may lead to the breakthroughs in artificial intelligence. Quantum technologies provide us, sensors of unprecedented precision, ultra-secure communications and computers that are very powerful than any other traditional or super computers we use. These technologies can actually help us in changing our lives, society and the way of accessing our data. Quantum computing is one such powerful tool through which most of the pressing questions that are very difficult to be answered can be undoubtedly solved. Well now coming to the concept of this cloning which actually involves the replication of the data, makes the hacking work easier. Just like when there is lot of easy availability of the information, it makes external attackers to easily get attracted towards it. Hacking has been one of the major threats to the society. Considering general stuff where the privacy of a person is considered, these days hackers have mastered in stealing one's identity .It may not affect just one person, sometimes it will also lead to the disastrous outcomes. We cannot give one reason for a person to evolve as a hacker but through one proper security concern most of the things that could go wrong can be prioritized and protected. Providing security is one of the significant reasons to the scientists to bring such kind of technologies which can help people to transmit their information without the fear of any threat. Quantum Computing networks are one such example which is surely going to be the best network security provider ever. But still there is a buzz that even this kind of security also needs protection as hackers are very well versed in breaking the securities. One of the main highlight of 2016 has been the US elections as there were speculations regarding the hacking of votes by the Russian hackers. Since these kind of stuff could actually have a great impact of its own on the human kind in future, it has to be prevented and taken care of. The complex world of quantum computing where the bits of information can be stored i.e., 0, 1 or both simultaneously, the threats to tackle these information has also become even trickier. But even after its security, hackers have found many ways to access our private and personal information. It has now become so important to actually protect all the confidential information while it is being transmitted or received. So here the main idea is to discover clues that could help users protect quantum computing networks from the external attacks by building the first high-dimensional quantum cloning machine which will be capable of performing quantum hacking so that the message can be secured through the interception. It can be guaranteed that this security measure can help in breaking the threats of any kind.

II. LITERATURE SURVEY

High-dimensional quantum cloning and applications to quantum hacking [1]: From this paper mainly we get to know that when cloning is done for a quantum system it always results in the imperfections. It happens in the no-

cloning theorem, which is the backbone of security for quantum communications. Since the perfect copies are prohibited in the quantum computing but still cloning is possible through a technique called the optimal quantum cloning. Hence by performing optimal cloning of high-dimensional photonic states by the symmetrisation method it can be shown that the universality of the technique by conducting cloning of numerous arbitrary input states which fully characterizes the cloning machine which can be performed by quantum state tomography on the cloned photons.

Experimental quantum cloning of single photons [2]:
Through this paper we can got to know about the copying of information in the quantum communication channel, which is actually impossible to get the perfect copies of any data but approximate cloning is certainly possible. Stimulated emission can be the easiest way to perform the quantum cloning mechanism. The quality of the quantum clones can be imposed by the actual ideology of the spontaneous emission of the photons. Here single photon stimulates the emission of the many photons which will lead to the production of quantum clones with near-optimal fidelity. So mainly here the activity of photons and the cloning can be known.

Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors [3]:
Through this paper basically the idea of eavesdropping attack was known and how the security of quantum key distribution can be easily be obscured if the eavesdropper can utilize technical imperfections in the actual implementation. Here, through a very simple demonstration the ideology of this attack has been signified. Interception means here we are allowing our hackers to secretly monitor the transmitted information which is being done in our paper. So basically when eavesdropping attack is done which is a highly effective attack that does not need to intercept the quantum channel at all. But in our paper we will intercept the quantum channel. Just to get exact idea of how the external attackers can actually try to deteriorate our date can be observed. However , a very similar and more effective way is being found to inhibit this and similar attacks.

Computer hacking and cyber terrorism: the real threats in the new millennium [4] :
We live in a society where the ideology of the society and the information technology actually matters a lot. This technology has provided us with many benefits; it also teaches us the new vulnerabilities that can be exploited by persons with the necessary technical skills. Hackers are the major threat by being responsible for damage to information systems and society as well. With this growing technology it has also led for some of the terrorists organizations to evolve as a strong threat. So basically it is important for us to stop these hackers from destroying the society and make our technologies threat free. By studying this paper the various problems speculated by the cyber terrorists groups and also the impact of these and how to preserve the future security of our society can be understood.

Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor [5]:
In this paper mainly it provides a software asset protection mechanism which is mainly based on the separation of the software that is be protected from executing that software. The main intension of this paper is to encrypt the messages in a cryptosystem using hardware based authorization and also using a secured coprocessor. However, the coprocessor will not perform these actions until and unless the right obtained by a user to execute is maintained by presentation of physically secured tokens. The physically secure token will provide us the coprocessor token data in the plain text form.

Quantum computing with realistically noisy devices[6] :
Through this paper we can get to know that the quantum computers have the ability to solve problems that are intractable on classical computers. When a quantum computer is constructed, it will be built with the capability of interacting with the noisy devices called 'gates'. These gates will help in the fault tolerance and provide a professional computing. The goal of so-called 'fault-tolerant quantum computing' is to compute perfectly even when the error probability per gate is high.

Quantum cloning machines and their implementation in physical systems[7]:
By referring this paper the basic ideas about the quantum computing machines for discrete variables was know. Basic knowledge on the most of the concepts like the difference between the various types of quantum cloning was known such as the approximate quantum cloning and the probabilistic quantum cloning ,the ideology of various types of quantum cloning machines PCCM, UQCM, RSCM,EPCC, and also how the implementation of the quantum cloning machines can be done is known .

Cloning Attack Authenticator in Wireless Sensor Networks[8]:
Through this paper basically the idea of how cloning attacks actually takes place and how to identify these through a machine using the wireless sensor networks can be known. The major problem in sensor network security is that sensors are susceptible to physical capture attacks. So once if a sensor compromises, then the attacker can easily launch clone attacks by replicating the compromised node, distributing the clones throughout the network, and starting a variety of insider attacks. So through this we can get the knowledge of how cloning attacks takes place and the precautionary steps to be taken to prevent these through applying various techniques. Wireless Sensor Networks actually offers us an excellent opportunity to observe environments, and obtain lot of interesting and useful applications.

III. PROPOSED SYSTEM

The main idea here is to build the first high-dimensional quantum cloning machine which will be capable of performing quantum hacking so that message can be secured through the interception. So here basically it means that we

are going to built a machine that can produce the replica of data and we are going to perform the hacking for the clones that are produced .Now when it is already hacked and is in our control and we are also trying to intercept the secured information just like it is the work of quantum hacking to silently copy the information. When all these things are done and the data is in our control, it will be very interesting to note that if suppose there is any external attack while the transmission of the data then it can be easily detected as the entire process will be in our control. This can help the data to be safe when attacked by the external server. Also when the external server tries to attack the data some noises will be created in the communication channel with the help of photons which will help in detecting the external attack. After performing experiments regarding this idea, it can be assumed that some very important clues to help protect quantum computing networks against potential hacking threats will be found.

The entire idea has been divided into three modules

1. Building a high dimensional cloning machine

2. Perform quantum hacking

3. Intercept a secure quantum message

Building a high dimensional cloning machine:

First of all Quantum Cloning is a process in which the data is being replicated and stored in a separate place as and when an adversary when wants to access it can easily get it without having the fear of losing the original data.

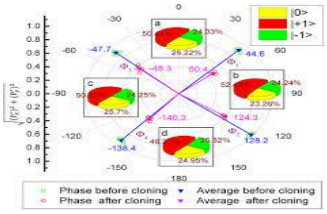

Fig 1 : Quantum Cloning Process

Cloning process and the need for a high dimensional cloning machine:

High-dimensional information is a promising field of quantum information science that has matured over the last years. Increase in the dimensionality of quantum systems is absolutely beneficial to quantum computation and communication protocols. It is known that, by using not only qubits but also qudits, that is, *d*-dimensional quantum states, it is possible to encode more information on a single carrier, increase noise resistance in quantum cryptography protocols and investigate fundamental properties of nature. Here, we adopt the OAM degree of freedom of single photons to achieve high-dimensional quantum cloning and perform quantum hacking on a high-dimensional quantum communication channel. Although perfect cloning of unknown quantum states is forbidden, it is interesting to ask how similar to the initial quantum state the best possible quantum clone can be. The answer is given in terms of the cloning fidelity $\mathcal{F}$, which is defined as the overlap between the initial state to be cloned and that of the cloned copies. This figure of merit is a measure of the accuracy of a cloned copy obtained from a specific cloner. Schemes that achieve the best possible fidelity are called optimal quantum cloning and play an important role in quantum information. For instance, an optimal state estimation yields a bounded fidelity of

$$\mathcal{F}_{\text{est}} = 2/(1+d),$$

Where *d* is the dimension of the quantum state. Optimal quantum cloning turns out to be a more efficient way of broadcasting the quantum state of a single system because it yields a fidelity that is always higher than that of optimal state estimation, which has been experimentally realized for low-dimensional photonic states . Moreover, this enhancement in fidelity grows larger with higher-dimensional quantum states, further motivating experimental investigations of high-dimensional quantum cloning. Hence, high-dimensional optimal quantum cloning machines are of great importance whenever quantum information is to be transmitted among multiple individuals without knowledge of the input quantum state. Here, we concentrate on the $1 \rightarrow 2$ universal optimal quantum cloning machine, for which the optimal fidelity of the two cloned copies is given by

$$\mathcal{F}_{\text{clo}} = 1/2 + 1/(1+d),$$

where *d* is the dimension of the Hilbert space of the states that are to be cloned .

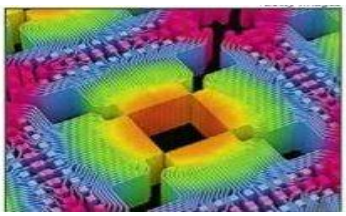

Fig 2: High Dimensional cloning machine

Quantum systems will provide us the perfectly secure kind of data when it is transmitted. When we try to copy the transmitted information, it will result in bad or deteriorated version of the actual information, which actually spoils the purpose of the initial hack. Traditional computing allows a hacker to simply copy and paste information and replicate it exactly, but this doesn't hold true in the quantum computing world, where attempts to copy quantum information-or quits-results in "bad" copies. When the cloning of the photons that transmit information is done , namely the single carriers of light known as qubits, as well as quantum theory also allows, meaning that the clones will be almost exact replicas of the original information. However, in addition to undermining what was previously thought to be a perfect way of securely transmitting information, the analysis will reveal promising clues into how to protect against such hacking.

Perform Quantum Hacking:

Being non-hack able is one of the big promises of quantum computers, and in the current climate of hacking for political gain, transmitting information safely has never been more important. Here it is about cloning photons carrying information about a quantum state. Hackers cannot just simply copy and paste quantum information like they'd do with the traditional computer file. Quantum information is affected by interactions with another systems, and so far there has been no way to clone the state and get information out. However now it will be possible. When it is possible to

create highly accurate copies but those were not that perfect, they were good enough to allow hacking. We also trying to do the cloning attack in the name of hacking. In clone attack, an adversary will capture a sensor node and copy the cryptographic information to another node known as cloned node. Then this cloned sensor node will be installed so that the information of the network can be easily captured. Now when we have the information, if the external adversary tries to inject false information, or manipulate the information by passing through cloned nodes, it can be easily detected through the continuous physical monitoring of nodes. Hence what we are actually trying to do is firstly we make the copies of data through the cloning machine and perform hacking i.e., we cover the data with our own way of attacks so that the entire data is in our control. Now when an external attacker tries to attack the transmitted information which is already ours then surely the external attack will be very much easier to detect. So considering that when large amount of quantum information is encoded on a single photon, the copies will get worse and hacking will become even simpler to detect. Here mainly the large amount of data will be encoded so that copies will get worse, in the sense a type of hacking is already being performed so that when cloning attacks occurs through a different source it will be easier to detect.

Fig 3: Quantum Computer

Intercept a secure quantum message:

Quantum cryptography is unlike any other form of public-key encryption out there in that is **provably secure**. If you and I share a reliable quantum channel of communication, we can have a fully encrypted conversation and get this: if someone tries to eavesdrop, the system will be able to detect intrusion and report so to us. Quantum cryptography will far outclass our current encryption schemes to the point where the balance will tip far the other way, as governments will no longer be able to eavesdrop on suspected criminals in emergency situations. Quantum transmission is a technique by which the information can be transmitted from one place to another, with the help of conventional communication and through previously shared between the sending and receiving location. Quantum communication is a field of applied quantum physics closely related to quantum information processing and quantum transmission. It will mostly help in protecting information channels against eavesdropping by means of quantum cryptography. The most well versed and advanced application of quantum cryptography is quantum key distribution (QKD). When larger amounts of quantum information are encoded on a single photon, the copies will get worse and hacking becomes even simpler to detect. Cloning attacks mainly introduces a specific and observable kind of noises in the secured quantum communication channel. When we ensure that photons contain the largest amount of information possible and we try to monitor these noises in a secure channel, it will surely help in strengthening the quantum computing networks against the potential hacking threats. The security and performance analysis indicate that this idea can identify clone attacks with a high detection probability at the cost of a low computation and communication and also storage overhead.

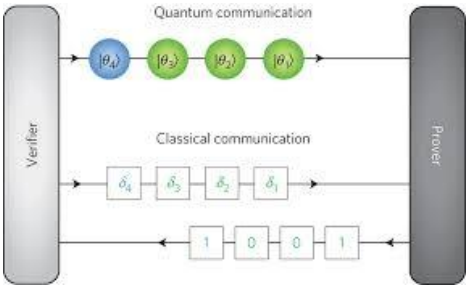

Fig 4 : Quantum Communication

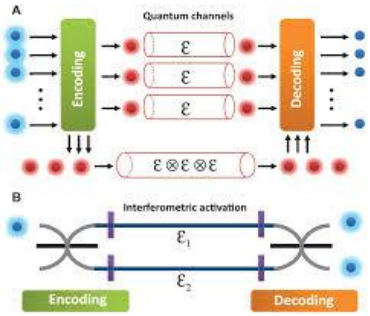

Fig 5: Quantum Transmission

Hence through this technique the entire process of actual transmission of data will be in our control and if any attack occurs it can be easily detected and data will also be secured through secretly intercepting the information.

IV. EXPECTED RESULT

The main intension of this paper is to provide a secured way of communication whether it is a classical or the quantum computer. No matter what it is important for us to secure our private information from the external attackers. Unlike the classical computers, the quantum computers are capable of providing more security but these days' attempts to hack these secured networks have also drastically increased. So the idea here is to build the first high-dimensional quantum cloning machine which will be capable of performing quantum hacking so that data will be able to secure through the interception. To help and protect the quantum computing networks against potential hacking threats some of the clues will be experimentally analyzed. After building that cloning machine, through the technique of the cloning attack, quantum hacking will be performed and entire process will be controlled and monitored. Later if suppose there is any kind of external attack, it will be easily detected as large amount of information will be encoded on photons and noises will be generated when external attacks occur.

This discovery will surely play an important role in the construction of quantum communication systems and how

quantum networks might behave. And it will also be able to show the theories of quantum information that will be tested more and more with real world problems. Quantum hacking efforts will help us to analyze quantum communication systems, and how the quantum information can travel across quantum computing networks.

V. CONCLUSION

Quantum computing is a practical tool for extremely complex predictive analysis, and machine learning where you need to assess many variables and many patterns and test models against it. Humanitarian problems like protein folding, flight routing, spam detection, drug discovery, and language translation will become easier. Quantum computing has got much more benefits which help this technological era to drastically increase its potential. Providing security has been so important these days that has been able to help people come up with unique ideas of security concerns in the communication process. Hence through this idea of building a high dimensional cloning machine which is capable of performing quantum hacking will help in securing the quantum messages through interception. Quantum computing networks have a very vast future in the technological field and it will be one of the biggest inventions in the future where as network security is concerned.

VI. REFERENCES

[1] Robert Fickler,Frédéric Bouchard, Robert W. Boyd, Ebrahim Karimi, "High-dimensional quantum cloning and applications to quantum hacking", Science Advances, 2017

[2] Christoph Simon, John C. Howell, Dik Bouwmeester,"Experimental Quantum Cloning of Single Photons" ,Science 296 5568 (2002)

[3] Weier1,4, Harald, Krauss1, Markus Rau1and Harald Weinfurter1,3 ,"Quantum eavesdropping without interception: an attack exploiting the dead time of

single-photon detectors ", Published 15 July 2011

[4] MJ Warren, SM Furnel, " Computer hacking and cyber terrorism: the real threats in the new millennium" ,UK

[5] Steve R Wright,Ashileshwari N Chandra, "Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor" , Mar 28, 1989

[6] E. Knill "Quantum computing with realistically noisy devices", USA

[7] Ye Liu, Fang Bao-Long and Wu Tao, "Quantum cloning machines and their implementation in physical systems" ,2013

[8] A Vanathi, B.Sowjanya Rani, "Cloning Attack Authenticator in Wireless Sensor Networks", Sp15, March 2012