Chapter II

Literature Survey

The review of related literature involves locating, reacting to, evaluating the researchers, observations and opinions that are related to any research problem, to be explored. This intends to help the researcher to have a thorough understanding and insight into the work already undertaken and key areas to explore further. No research endeavor is unique in descriptive research and variables under investigation are studied in different combinations to understand the dynamics of cause and effect relationship underlying the phenomena. Every researcher reviewed the related literature from the different resources that includes research journal, articles, books, magazines, encyclopedias, dissertations, abstracts, international year books, thesis and most important in the present era the internet access. The detailed account of review of related literature pertaining to variables under study, namely Network Security, Conventional Cryptography, Quantum Computing and Quantum Algorithms presented here under.

2.1 Network Security and Secure Models

David L. Mills et al. (1993) has described the Network Time Protocol (NTP), specifies its formal structure and summarizes information useful for its implementation. NTP provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. It uses a returnable time design in which a distributed subnet of time servers operating in a self organizing, hierarchical master slave configuration synchronizes local clocks within the subnet and to national time standards via wire or radio. The servers can also redistribute reference time via local routing algorithms and time daemons.
Liu, S et al. (2001) says that as the Internet has matured, so has the threats to its safe use, and so must the security measures that enable its business use. Traditional piecemeal, single-layer, single-dimensional security approaches are no longer adequate. These approaches can create a false sense of security and create as many problems as they attempt to address. They propose a multifaceted framework to prevent, detect, and respond to ever more sophisticated threats to enterprise IT information and assets. They outline a practical implementation approach to building enterprise IT security mechanisms in an incremental and continuous fashion. They believe that enterprises should adopt a similar multifaceted framework, following a practical but disciplined implementation approach. Enterprises must treat IT security as a required business enabler rather than just a costly item with low priority.

Rothe, J. (2002) gives brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. They discuss the notion of one-way functions both in a cryptographic and in a complexity-theoretic setting. They also consider interactive proof systems and present some interesting zero-knowledge protocols. In a zero knowledge protocol, one party can convince the other party of knowing some secret information without disclosing any bit of this information. Motivated by these protocols, we survey some complexity theoretic results on interactive proof systems and related complexity classes.

Kyoung Lae Noh et al. (2008) This article proposes an energy efficient clock synchronization scheme for Wireless Sensor Networks (WSNs) based on a novel time
synchronization approach. Within the proposed synchronization approach, a subset of sensor nodes are synchronized by overhearing the timing message exchanges of a pair of sensor nodes. Therefore, a group of sensor nodes can be synchronized without sending any extra messages. This paper brings two main contributions: First is development of a novel synchronization approach which can be partially or fully applied for implementation of new synchronization protocols and for improving the performance of existing time synchronization protocols. Second is to design of a time synchronization scheme which significantly reduces the overall network wide energy consumption without incurring any loss of synchronization accuracy compared to other well known schemes.

Christopher B. McCubbin (2009) analyzed the security of IPsec against a class of attacks known as the IV attacks, which are based on modifying the initialization vector (IV) of a CBC encrypted packet during transmission. They show that IV attacks can be a serious threat for IPSec if IPSec is not used carefully. They also discuss the defense methods against these attacks. The result shows that IV attacks can be a serious threat for IPsec, if IPsec is not used carefully. In the absence of authentication, an attacker may be able to totally defeat the IPsec encryption by the techniques. Although there are many ways to prevent these attacks, they recommend always using authentication whenever encryption is used. There conclusion is also supported by other attacks on IPsec, most importantly those discovered by Bellovin, which also make use of the fact that IPsec permits encryption to be used without authentication.

S. Jajodia et al. (2009) says that network administrators rely on labor intensive processes for tracking network configurations and vulnerabilities. This requires a great deal of expertise, and is error prone because of the complexity of networks and associated
security data. The interdependencies of network vulnerabilities make traditional point
wise vulnerability analysis inadequate. They describe a Topological Vulnerability
Analysis (TVA) approach that analyzes vulnerability dependencies and shows all possible
attack paths into a network. From models of the network vulnerabilities and potential
attacker exploits, they compute attack graphs that convey the impact of individual and
combined vulnerabilities on overall security. TVA finds potential paths of vulnerability
through a network, showing exactly how attackers may penetrate a network. From this,
they identify key vulnerabilities and provide strategies for protection of critical network
assets.

Bou Harb, E. et al. (2010) proves that operation and control of the next
generation electrical grids will depend on a complex network of computers, software, and
communication technologies. Being compromised by a malicious adversary would cause
significant damage, including extended power outages and destruction of electrical
equipment. Moreover, the implementation of the smart grid will include the deployment
of many new enabling technologies such as advanced sensors and metering, and the
integration of distributed generation resources. Such technologies and various others will
require the addition and utilization of multiple communication mechanisms and
infrastructures that may suffer from serious cyber vulnerabilities. These need to be
addressed in order to increase the security and thus the greatest adoption and success of
the smart grid. In this article, they focus on the communication security aspect, which
deals with the distribution component of the smart grid. They discuss the security and
feasibility aspects of possible communication mechanisms that could be adopted on that
subpart of the grid. By accomplishing this, the correlated vulnerabilities in these systems
could be remediated, and associated risks may be mitigated for the purpose of enhancing
the cyber security of the future electric grid.
**NTT Communication (2012)** this white paper explores the scope, characteristic targets, and consequences of DDoS attacks. It also discusses the keys to mitigating such attacks, and discusses the attributes that differentiate NTT America’s approach to solutions. Nearly limitless connectivity, information flow and transactional freedom of the digital age defy hyperbole and opportunities are practically boundless for businesses, organizations, governments and individuals. But such online opportunities come with a cost an expanded potential for ill intentioned destruction of network assets. Establishing and developing an online presence carries with it a certain amount of vulnerability. Many leading global companies, prominent government entities, advocacy groups and small businesses alike have fallen prey to virtual attacks that exploit such vulnerability. Distributed Denial-of-Service (DDoS) attacks are among the most prevalent and costly forms of such attacks, posing a serious threat to e-commerce and online businesses. During a DDoS attack, remote attackers or assailants generate a flood of traffic to a specific destination to disrupt a targeted website or server. The attack can come from one or multiple compromised machines or large networks of infected computers to flood the target with high volumes of illegitimate traffic. As the targeted systems strain to keep up with the inundation, the ensuing slowdown or shutdown blocks legitimate users from access. The goal of most DDoS attacks is to force the targeted computing resources completely offline. They frequently succeed. The business costs of such attacks are substantial. They range from monetary damage directly associated with the disruption itself to the longer term implications for the company’s reputation, competitiveness.

**Michael Rossberg (2012)** this particular paper describes the essential parts of VPN implementation. Authors have tested NTP protocol for time synchronization and further explain the denial of service attack condition with frog boiling attack. Particular paper is very helpful in shaping up our problem and we consider this issue as our research
problem. They have proposed to securely exchange data over public networks, such as the Internet, organizations often utilize Virtual Private Networks (VPNs). However, relying on these potentially large overlay networks makes them vital targets for Denial-of-Service (DoS) attacks. Thus, recent approaches for VPN auto configuration address DoS resistance by employing distributed management algorithms. Nevertheless, there is no satisfying solution for time synchronization within VPNs that is designed for resistance against DoS as well as internal attacks. For example, Network Time Protocol (NTP) relies on hierarchical structures, and cannot comply with DoS resistance. Thus, in this article they present a novel, fully distributed and fault tolerant time synchronization approach, which is designed to be transparently integrated in VPN gateways. Combining diffusion based roundtrip synchronization with internal attacker detection, the proposed mechanism is making a contribution to resilient VPN design.

Ben Youssef et al. (2012) recommend that network security requirements are generally regarded once network topology is implemented. In particular, once firewalls are emplaced to filter network traffic between different Local Area Networks (LANs). This common approach may lead to critical situations: First, machines that should not communicate could belong to a same LAN where the network traffics do not pass through the firewall for being filtered. Often overwhelmed by the complexity of security requirements and the growth of networks, network administrators are struggling to resolve such design faults while ensuring not to cause further vulnerabilities. Second, according to network security policy, the required number of LANs, and therefore the number, range and thus, the cost required for both network and security equipments, can be much more reduced than that originally proposed by the network administrator. In this paper, they present an automatic approach that consists on proposing a network topology which is both safe and optimal by taking into account
the network security policy, given in a high-level language. The safety property ensures that every prohibited traffic has to cross the firewall to be filtered. The optimal property allows deducing the necessary and sufficient resources (Sub networks, network switches, and firewalls range) to be used. To best knowledge, such problematic has not been explored in previous works, despite the importance of these challenges. There method has been implemented using Graph Coloring Theory. The first results are very promising. Experiment conducted on large scale networks demonstrates the efficiency and the scalability of approach.

Zebo Feng et al. (2012) shows that the foundation of network security has not been paid enough concentrations and the comprehensive considerations for the solution models in network security have not been explored thoroughly. In this research paper, they make the first attempt to establish several models for the security of network protocols. They divide the security of network protocols into two folders: the implementation security of network protocols, and the design security of network protocols. Four models are proposed to clarify the security problems: software vulnerability model, scalability model, authentication model, and covert model. They also propose several defense principles for all models. The security reduction is also proposed to transform the solution method for security problems to other available security verification and testing approaches. For example, the implementation security of network protocols is reduced to the security of software implementation for parsing protocols, so that the fuzzy test can be used for verification. The pressure tests are used for scalability model. The exploration of the paper can help to stimulate the further discussions on the foundations of network security, especially the design security of network protocols.
Huayang Cao et al. (2013) notify that networked critical infrastructures improve our lives, but they are attractive targets for adversaries. In such infrastructures, to secure sensitive data is vital, as the information system is a foundation of today critical infrastructures, and data security is a main concern in such systems. Cryptography is an approach for data security, but this method should be altered according to various features of infrastructure networks. Since complex and distributed critical infrastructures usually spread over large geographic areas, different parts of those infrastructures have different levels of perimeter defense. Devices in weakly protected zones are more likely to be captured than those in well protected zones. If an adversary captures devices, they can bypass cyber security measures and obtain secret information directly. Such a threat requires a layered security mechanism that can prevent adversaries from invading the whole infrastructure network from these weak zones. In this article, they propose a layered encryption mechanism based on hash chain technology for protecting sensitive data. Besides showing the layered defense, the mechanism is also lightweight and has convenient key management. It can be used independently or as a supplement to existing security measures.

2.2 Conventional Cryptography and Algorithms

R. Rivest, et al. (1978) present an encryption method with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: (1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only they can decipher the message, since only they know the corresponding decryption key. (2) A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later
deny the validity of their signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems. A message is encrypted by representing it as a number $M$, raising $M$ to a publicly specified power $e$, and then taking the remainder when the result is divided by the publicly specified product, $n$, of two large secret primer numbers $p$ and $q$. Decryption is similar; only a different, secret, power $d$ is used, where $e \times d \equiv 1 \pmod{(p - 1) \times (q - 1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, $n$.

W. Stallings (1998) proves that simple network management protocol (SNMP) is the most widely used network management protocol on TCP/IP-based networks. The functionality of SNMP was enhanced with the publication of SNMPv2. However, both these versions of SNMP lack security features, notably authentication and privacy that are required to fully exploit SNMP. A recent set of RFCs, known collectively as SNMPv3, correct this deficiency. This article outlines the overall network management framework defined in SNMPv3, and then looks at the principal security facilities defined in SNMPv3: authentication, privacy and access control.

Wunnava, S.V et al. (2002) proves that with the explosion in Internet based electronic commerce, there is an increasing need to secure data and commercial transactions. While there are several encryption methodologies, such as the DES(Data Encryption Standard) and the RSA (Rivest, Shamir, Adleman) algorithm, there is a continuous need to develop other algorithms, especially taking into consideration the recent advances in hardware and storage technologies and software distributed computing capabilities. The purpose of this paper is to present the results of investigations conducted by the authors regarding the emerging data security methodologies. Emphasis is placed on the applicability of these algorithms in the academic, industrial and commercial
environments. Of the several methodologies considered for the AES (Advanced Encryption Standard), MARS (Multivariate Adaptive Regression Splines) has become one of the front running and adaptable methodologies for data security over global networks. Initiated by NIST (National Institute of Standards), the MARS cipher was developed by IBM as an alternative to the existing DES methodology; MARS is expected to be more secure.

**Young, A.** (2003) shows that in general the amount of computational power used to subvert a particular cryptosystem determines the expected time it takes to recover an encryption message. This determines that it takes much longer to subvert highly sophisticated systems such as AES today than it will take in a couple of decades. Therefore, encrypted messages in this system can only be considered secure for a limited period of time. For this reason, many efforts have been made by scientists to develop a new cryptosystem mechanism to resolve this issue. One of these efforts has led to the development of quantum cryptography.

**Yan Wang et al.** (2009) proposed a new timing evaluation model based on random number generating mechanism to analyze the time consuming of the known cryptographic algorithms: triple-DES, AES and RSA. In this model for evaluation, there are two evaluating modes: different plaintexts in the same key (DPSK), the same plaintext in different keys (SPDK). As the basis of the evaluating model, the plaintext and the corresponding key are both generated by random numbers. The results show that, under the same key length and for the same size of the processed data, RSA is about several hundred times slower than AES, triple DES is about three times slower than AES, and there are other runtime characteristics which further highlights the difference between
these three cryptographic algorithm and provides a reference value of for people’s rational using.

Caliskan, D (2011) shows that in transferring data secretly between two people who are far away from each other Public Key Cryptosystem can be used and RSA is one of the famous Public Key Cryptosystem. If data contains very long information, encryption and decryption process take long time in RSA. In such situation hybrid systems are used. Chosen Public Key Cryptosystem is used for transferring key and a chosen Secret Key Cryptosystem is used for encrypting and decrypting data. In this article a method for applying RSA for transferring date is proposed. In this method, selected RSA modulus $n$ is used in the encryption and decryption process. So this system may be assumed as a modification of RSA to semi-hybrid RSA.

Braun, J.; Buchmann, J. (2012) describes that Encryption is used in order to achieve confidentiality in today’s and future IT systems. However, the security of commonly used encryption methods depends on unproven assumptions. Thus, due to unforeseeable advances in computing power and cryptanalysis, current state-of-the-art encryption schemes (RSA and AES for example) might be broken without premonition. Furthermore, all currently applied public key encryption available. This paper proposes an infrastructural solution called Perfect Confidentiality Network, to allow information theoretically secure key agreement. The keys can either be used for One Time Pad encryption providing perfect confidentiality or as keys for symmetric encryption thus providing resistance against quantum computers.

Woungang et al. (2012) indicates that in Emergency MANETs (eMANETs), the broadcasting nature of the wireless medium, the lack of pre established trust
relationship among nodes, and the frequent topology changes, cause some serious security challenges, making the network vulnerable to malicious attacks such as wormhole attacks. The paper investigates a recently proposed Advanced Encryption Standard (AES) based routing algorithm (so called AODV-Wormhole Attack Detection Reaction - here referred to as AODV-WADR-AES) for securing AODV-based eMANETs against wormhole attacks. The proposal consists of substituting the AES part of the scheme by the Triple Data Encryption Standard (TDES), yielding the AODV-WADR-TDES routing algorithm, with the goal to study the performance of the algorithm where mobile devices that are incompatible with AES are part of eMANET nodes. In doing so, markers in the form of hash codes are included in the data packets to help consolidating the data integrity. Simulation results are presented to validate the proposed AODV-WADR-TDEA scheme. It is also shown that the AODV-WADR-AES scheme outperforms the AODV-WADR-TDES scheme in terms of end to end delay, packet delivery ratio and number of packets traversing through the wormhole link.

Weiqiang Liu (2012) refers that Quantum dot cellular automata (QCA) technology is expected to offer fast computation performance, high density, and low power consumption. Thus, researchers believe that QCA may be an attractive alternative to CMOS for future digital designs. Side channel attacks, such as power analysis attacks, have become a significant threat to the security of CMOS cryptographic circuits. A power analysis attack can reveal the secret key from measurements of the power consumption during the encryption and decryption process. As there is no electric current flow in QCA technology, the power consumption of QCA circuits is extremely low when compared to their CMOS counterparts. Therefore, in this paper an investigation into both the best and worst case scenarios for attackers is carried out to ascertain if QCA circuits are immune to power analysis attack. A QCA design of a sub module of the Serpent cipher is
proposed. In comparison to a previous design, the proposed design is more efficient in terms of complexity, area, and latency. By using an upper bound power model, the first power analysis attack of a QCA cryptographic circuit is presented. The simulation results show that even though the power consumption is low, it can still be correlated with the correct key guess, and all possible sub keys applied to the Serpent sub module can be revealed in the best case scenario. Therefore, in theory QCA cryptographic circuits would be vulnerable to power analysis attack. However, the security of practical QCA devices can be greatly improved by applying a smoother clock. Moreover, in the worst case scenario, the design of logically reversible QCA circuits with Bennett clocking could be used as a natural countermeasure to power analysis attack. Therefore, it is believed that QCA could be a nice technology in the future for the implementation of security architectures resistant to power analysis attack.

2.3 Quantum Computing and Quantum Algorithms

Bennett, C. H. (1992) proves that the security of quantum key distribution relies on the inviolable laws of quantum mechanics, and the impossibility of perfect cloning of non-orthogonal states implies the security of this protocol. Also, quantum cryptography technology makes extensive use of the Heisenberg uncertainty principle for ensuring secure cryptography. Quantum cryptography exploits the laws of quantum physics to guarantee in an absolute fashion the confidentiality of data transmission. Quantum cryptography constitutes a revolution in the field of network security. This research paper explores the quantum cryptography technology in network security.

Elliot, C (2002) show how quantum key distribution (QKD) techniques can be employed within realistic, highly secure communications systems, using the internet architecture for a specific example. They also discuss how certain drawbacks in existing
QKD point-to-point links can be mitigated by building QKD networks, where such networks can be composed of trusted relays or untrusted photonic switches.

Schartner, P et al. (2009) illustrates that among the various proposals for quantum network design, the trusted node model is still the most flexible one for delivery of messages over arbitrary long distances. However, the outstanding security features of these networks are equally well defeated by the trusted relay. In brief this means, that messages sent over a certain node become completely insecure as soon as the node is compromised and the attacker hence knows the keys stored within this node. In this paper they propose a simple technique to reduce the damage in case of a compromised node. More precisely they are trying to show, that none of the messages handled by the compromised node becomes insecure, as long as the compromised node is shut down in a certain time interval after detecting the attack. Additionally, their approach reduces the memory needed to store key material inside the nodes by 50%, whilst increasing security.

Sharbaf, M.S. et al. (2009) refers that Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. Quantum cryptography was born in the early seventies when Steven Wiesner wrote "Conjugate Coding", which took more than ten years to end his paper. The quantum cryptography relies on two important elements of quantum mechanics the Heisenberg Uncertainty principle and the principle of photon polarization. The Heisenberg Uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper can not copy unknown qubits i.e.
unknown quantum states, due to no-cloning theorem which was first presented by Wootters and Zurek in 1982. The research paper concentrates on the theory of quantum cryptography, and how this technology contributes to the network security. The research paper summarizes the current state of quantum cryptography, and the real-world application implementation of this technology, and finally the future direction in which the quantum cryptography is headed forwards.

Tien-Sheng Lin et al. (2010) suggest that in the wireless communication networks, quantum message integrity can be applied with quantum authentication and quantum signature if the source and destination are indirect communication. Eavesdroppers and malicious nodes may exist in the routing path from the source to the destination. There is major threat in the indirect communication. Based on quantum nature, they design quantum permutation model to verify quantum transmission sequence of a quantum transmission frame if an attacker wants to crack the content of a quantum transmission frame. Quantum permutation model can determine the real position of data qubits and verification qubits. However, Eves is not able to obtain the position of date qubits because quantum permutation switching cannot be owned by Eve. So quantum transmission sequence can be reserved. The receiver has the capability to verify it and obtains the content of data qubits.

Mehrdad S. Sharbaf (2011) discusses the uses of computer communications networks technologies. Because of these incidents, most organizations facing pressure to protect their assets. Most digital networks generally rely on modern cryptosystems to secure the confidentiality and integrity of traffic carried across the network. The current modern cryptosystems based on mathematical model introduce potential security holes related to technological progress of computing power, the key refresh rate and key
expansion ratio, the most crucial parameters in the security of any cryptographic techniques. For that reason efforts have been made to establish new foundation for cryptography science in the computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics. This work concentrates on quantum cryptography, and how this technology contributes to the network security. The scope covers the weaknesses, and the security pitfalls in modern cryptography, fundamental concepts of quantum cryptography, the real world application implementation, finally the future direction in which the quantum cryptography is headed forwards.

Xu Huang et al. (2011) states that wireless technology is rapidly evolving and is playing an important role in the lives of people throughout the world. Due to the nature of open guide medium of wireless communications, it is possible for an adversary to snoop on confidential communications or modify them to gain access to the wireless networks more easily than with wired networks, which has been drawing great attentions. In this paper, they focus on improving the security of IEEE 802.11 networks through secure key distribution using Quantum Key Distribution (QKD) which offer unconditional security between two communication parties. In their previous research work, we have demonstrated a novel protocol using quantum cryptography for secure key distribution in IEEE 802.11 networks. In this paper, they have analysis the experimental results which were obtained in previous research works, which will be focusing on the reconciliation phase of this protocol.

Al Hadhrami et al. (2012) gives the modification concept of Hilbert space of multi-partite system. Entanglement in multi-particle system is quantified and examples
are provided. Application of entangled tri-particles in cryptography is introduced. It is shown that sending information using a tri-partite entangled system is more secure than sending them using an entangled pair of particles.

**Pattaranantakul, et al. (2012)** in conventional security mechanism, security services based on symmetric key cryptography assume keys to be distributed prior to secure communications. The core function of exchanging and sharing a secret key between two endpoints are the secure key management methodology which is one of the most critical elements need to be more concerned when integrating cryptographic functions into the system. In case the key management mechanisms is weak can lead to the vulnerability holes or a potentially fatal outsider attacks as the harmful effects to the system. Since, there is still no standardized architecture or protocol that can provide cross application symmetric key management services. Therefore, this paper approaches a secure key management model and its custom protocols to build quantum trusted network with offers simultaneous quantum key distribution to multiple user overtime. Consequently, the proposed technique has also overcome the limitation of quantum point-to-point key sharing. Based on the discussion of key management security requirement, deal with generic key management concepts and designing the new custom protocols to close the possibility loopholes to offers reliability and convenience of use as well as to introduce a secure and efficient key management technique for quantum cryptography network in where any communication services can take place.

**Sakhi, Z et al. (2012)** presents some cryptographic applications of quantum algorithm on many qubits system. They analyze a basic concept of Grover algorithm and it's implementation in the case of four qubits system. Paper show especially that Grover algorithm allows as obtaining a maximal probability to get the result. Some
features of quantum cryptography and Quantum Secret Sharing protocol based on Grover's algorithm are also presented.

Tsurumaru, T. (2013) they introduce the concept of dual universality of hash functions and present its applications to quantum cryptography. They begin by establishing the one-to-one correspondence between a linear function family $F$ and a code family $C$, and thereby defining $\varepsilon$-almost dual universal$_2$ hash functions, as a generalization of the conventional universal$_2$ hash functions. Then, they show that this generalized (and thus broader) class of hash functions is in fact sufficient for the security of quantum cryptography. This result can be explained in two different formalisms. First, by noting its relation to the $\delta$-biased family introduced by Dodis and Smith, we demonstrate that Renner's two-universal hashing lemma is generalized to our class of hash functions. Next, they prove that the proof technique by Shor and Preskill can be applied to quantum key distribution (QKD) systems that use our generalized class of hash functions for privacy amplification. While Shor-Preskill formalism requires an implementer of a QKD system to explicitly construct a linear code of the Calderbank-Shor-Steane (CSS) type, this result removes the existing difficulty of the construction of a linear code of CSS code by replacing it by the combination of an ordinary classical error correcting code and our proposed hash function. They also show that a similar result applies to the quantum wire-tap channel. Finally, they compare the results in the two formalisms and show that, in typical QKD scenarios, the Shor-Preskill type argument gives better security bounds in terms of the trace distance and Holevo information than the method based on the $\delta$-biased family.

Niemiec, M. et al. (2013) says that the interest in quantum based security methods has been growing rapidly in recent years. New implementations of quantum key
distribution and new network services supported by this solution are being introduced. The reason behind the growing popularity of quantum cryptography is its unrivaled security level: all eavesdroppers can be revealed through the application of the laws of physics. First of all, the rules of quantum mechanics ensure that any measurement modifies the state of the transmitted quantum bit. This modification can be discovered by the sender and the receiver. This makes passive eavesdropping impossible. Using protocols such as BB84, network users are able to send a string of bits coded by the polarized photons. After that, they can establish secure cryptographic keys through an unsecure channel using different key distillation methods. Major ongoing challenges include the control and management of security in systems using quantum cryptography, as well as tailoring security to specific end user's requirements and services.

**Humble, T.S. (2013)** describes the physical layer and how communication signals are encoded and transmitted across a channel. Physical security often requires either restricting access to the channel or performing periodic manual inspections. In this tutorial, they describe how the field of quantum communication offers new techniques for securing the physical layer. They describe the use of quantum seals as a unique way to test the integrity and authenticity of a communication channel and to provide security for the physical layer. They present the theoretical and physical underpinnings of quantum seals including the quantum optical encoding used at the transmitter and the test for non locality used at the receiver. They describe how the envisioned quantum physical sub layer senses tampering and how coordination with higher protocol layers allows quantum seals to influence secure routing or tailor data management methods. They conclude by discussing challenges in the development of quantum seals, the overlap with existing quantum key distribution cryptographic
services, and the relevance of a quantum physical sub layer to the future of communication security.

2.4 Inferences drawn from literature Survey

- Conventional technologies will require the addition and utilization of multiple communication mechanisms and infrastructures that may suffer from serious cyber vulnerabilities. These need to be addressed in order to increase the security and thus the greatest adoption and success of the Non conventional approaches such as Quantum Computing.

- Cryptography is an approach for data security, but this method should be altered according to various features of infrastructure networks. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for his paper instrument, each user must be able to produce message whose authenticity can be checked by anyone hence cryptography is prefer on these applications.

- After reviewing many papers it is found that Quantum Computing Algorithms are providing good solution for data communication over internet. Quantum computers share theoretical similarities with non-deterministic and probabilistic computers.

- The security of commonly used encryption methods depends on unproven assumptions. Thus, due to unforeseeable advances in computing power and cryptanalysis, current state-of-the-art encryption schemes (RSA and AES for example) might be broken without premonition.
• The current modern cryptosystems based on mathematical model introduce potential security holes related to technological progress of computing power, the key refresh rate and key expansion ratio, the most crucial parameters in the security of any cryptographic techniques. For that reason efforts have been made to establish new foundation for cryptography science in the computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics.

• The interest in quantum based security methods has been growing rapidly in recent years. New implementations of quantum key distribution and new network services supported by this solution are being introduced. The reason behind the growing popularity of quantum cryptography is its unrivaled security level.

• Quantum cryptography exploits the laws of quantum physics to guarantee in an absolute fashion the confidentiality of data transmission. Quantum cryptography constitutes a revolution in the field of network security. Two states of a single photon become related, rather than the properties of two separate photons. By entangling the photons the team intercepted, they were able to measure one property of the photon and make an educated guess of what the measurement of another property like its spin would be. By not measuring the photon’s spin, they were able to identify its direction without affecting it. So the photon traveled down the line to its intended recipient none the wiser.
2.5 Objectives

After briefly surveying the limitations of conventional cryptography and network security models following objectives were proposed

1) To study the conventional cryptography approaches.

2) To study the Quantum Computing effects like Quantum bits, Quantum Superposition and Quantum parallelism.

3) To develop a data communication security model using Quantum Cryptography

4) To evaluate the parameters like confidentiality, authenticity and integrity of data using Quantum key combinations.

5) To restrict the unauthorized user access using Quantum cryptography security model.