Secure in Telecommunication data Preservation: Wavelength Division Multiplexing and Quantum Cryptography

C.A.Senadheera , V.S.S. Kaushalya , S.M.R.D. Mahavewa , N. Sukanthan , C.A.J.A. Rogess , Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Pvt (Ltd), Sri Lanka

Abstract- Quantum cryptography is a modern technique in networking which is used as a component in making networks secure. Network security is a major problem in Telecommunication data Preservation. The storage of call detail records (CDRs) of telephony and internet traffic and transaction data (IPDRs) which are from governments and commercial organizations. It is often argued that data retention is necessary to combat terrorism, and other crimes. Data retention may assist the police and security services to identify potential terrorists and their accomplices before or after an attack has taken place.

With the use of quantum cryptography and Wavelength division multiplexing provide security by enabling the unconditionally secure transmission of a random binary key, which enable bi-directional communication as well as multiplication of signal capacity. This may useful to compress several request to a single wave via fiber optics. And capable of protecting bandwidth capacity. Proposed research is about how to ensure the security of telecommunication call detail record transactions with quantum key distribution, wavelength division multiplexing and ultrafast frequency combs.

Index Terms- Wavelength division multiplexing, Quantum cryptography, Quantum Networks, Quantum computers, Fiber optics, ultrafast frequency combs.

I. Introduction

Fundamental component of the economic and social infrastructures are telecommunications networks. Security for Telecommunications Networks is thus an important aspect which cannot be ignored. Protecting these networks from malicious attacks that could lead to loss or unavailability of confidentiality and integrity of network services, an effective and long lasting security program should be accomplished to protect telecommunication networks from such attacks.

In the field of telecommunications, data preservation generally refers to the storage of governments and commercial organizations call detail records (CDRs) of internet traffic and telephony i and transaction data (IPDRs). In the case of government data preservation, usually of telephone calls made and received, emails sent and received and websites visited usually store data. Location data is also collected. They must also store traffic data for a period which may be determined and it was argued that data retention is required to combat terrorism, and other crimes. And the hardware and software required to store all the retained data would be extremely costly. And Because of the economic frugality of the telecommunication industry, sharing of telecom infrastructure among competitive telecom service providers is becoming the requirement and process of business in the telecom industry to lower their increasing investments. Providing standard telecom services such as PSTN, ISDN and GSM services on phones. Telecom infrastructure contained both electronic and non- electronic devices. Base tower station, antennas, microwave radio equipment, switches, transceivers for signal processing and transmission includes in electronic infrastructure.

In brief, objectives of this research are provide security handling big data which generated by telecommunication with the Quantum key distribution. And compress several request to a single wave by using wavelength division multiplexing.

This research consists of six major sections. These are:

1) Abstract
2) Introduction
3) Background of related work
4) Our Approach
5) Conclusions
6) Future Work

II. BACKGROUND AND RELATED WORKS

Currently, several researches which based on conventional data transmission over installed fiber are used wavelength-division multiplexing (WDM) technology because this technology enables bidirectional communications over one strand of fiber, as well as multiplication of capacity. According to the Townsend et.al using quantum cryptographic key distribution can be help to reduce the network traffic which generated by multiple user requests. But this approach for constructing optical quantum networks does one node at a time, which lacks scalability. [1]

According to Roslund et.al with the concept of wavelength division multiplexing and the quantum domain demonstrate entanglement of frequency which occurs Quantum information processing. A single step to enhance the capacity by using ultrafast frequency combs. It is easily addressable and robust with De-coherence and scalability. [2]

Falahati & Meshgi research focuses on analyze the interests of using quantum technique for the distribution of encryption keys in 802.11 wireless networks and also propose a scheme for the combination of quantum cryptography and 802.11i establishment of the PTK (Pairwise Transient Key) is for security mechanisms for the . Quantum cryptography, simultaneously generate shared, two parties may,secret cryptographic key material using the transmission of quantum states of light. Key distribution is the problem of classical cryptography algorithm, and tends to provide safe channel to transport key. Quantum cryptography may distribute key in quantum channel. An intruder attacks on quantum channel QBER rate increases and it'll detected. Proposed system will use cryptography in telecommunication. [3]

Thayananthan & Albeshri research focuses on Enhancement of security and privacy in mobile data centers is challengeable with efficient security key management. Data centers need efficient quantum cryptography using Grover's algorithm and authentication techniques to solve this problem. Which are appropriate approaches to enhance the security and privacy with less complexity. Best approach is light which has same quantum properties, because people can see only the light not the data. Light based on quantum cryptography and PairHand protocols used in this research. [4]

The foundation research for this research is the BB84 research which is about a method to minimize the effect of interference of a third party via a communication channel. The researchers C. Bennett and G. Brassard who conducted the foundation research explains the concept of cubit, which is a two-state quantum-mechanical system, such as the polarization of a single photon. Then the researchers describe the method of forming polarized photons and about quantum public key distribution. Also the researchers describes about the possible situations the quantum public key distribution can bring to the stage. According to the researchers when the third party interaction gets minimum, quantum public key distribution method can be started. The describing research has simulated BB84 operation with several security attacks scenario and noise immune quantum key distribution in order to increase the security and reduce the noise interference. While most QKD simulation researches focused on protocol mechanics, this study focuses on hardware setup based on OptiSystem. But this simulation setup still needs vigorous testing and analysis. [5]

Tanaka et. al research is about ultra-fast, 84 quantum key distribution transmission at 625 MHz clock rate through a 97 km field-installed fibber using practical clock synchronization based on wavelength-division multiplexing. According to researchers QKD has recently been put to practical demonstration through field-installed fibbers. Step by step the researchers has designed methods with the intention of overcoming the problems like backscattered light noise, Trojan-horse attacks, thermo-optic effect and polarization sensitivity by designing, a bidirectional transmission (plug and play) scheme and applied it into the natural environment and a One-way transmission scheme with time-bin encoding. The nonlinear crosstalk could be suppressed by using the WDM scheme. The optical power of the clock signal through the fibber has been set as low as possible to suppress those unwanted noise generations. However this system's detection efficiency is low and clock frequency is below 3GHz. [6]

Rarity et. al research is about using the quantum cryptography for secure key exchange between a ground station and a satellite .a key Exchange system using Quantum cryptography could provide the highest security method for exchanging keys between any two points on the globe. The method of Quantum cryptography has its security based on the laws of nature and is, absolutely secure against any computational improvements, in principle. The research resulted that there are no technical obstacles to building a system that could exchange keys at kilo baud rates between a meter diameter telescope on the ground and a 10 cm diameter lightweight telescope with a satellite. [7]

Bennett et. al research describe about apparatus and protocol designed to implement quantum key distribution. Exchange a random quantum transmission, very faint flashes of polarized light of consisting ,discussion of the sent and received versions of this transmission if this estimate is small enough, distil from the sent and received versions a smaller body of shared random information the system depends on the uncertainty principle of quantum physics, instead of the usual mathematical assumptions such as the difficulty of factoring, it remains secure against an adversary with unlimited computing power. [8]

Tanaka et.al research paper is about the system called high-speed quantum key distribution (QKD) system. The system developed to generate secure key in a rate of 1-Mbps 10-dB transmission loss. For the purpose of speeding-up all processes in high-speed quantum key distribution system the research team apply a wavelength-division-multiplexing technique using the colorless interferometry technique and a key distillation hardware engine. The research team provides a novel WDM scheme, sharing interferometers and temperature regulators over multiple channels, which enables us to increase the number of channels with a small impact on system cost and size. User to execute key distillation with 1-Mbit code length in real time in order to generate a secure key while satisfying both high speed and high security, the team develop a key distillation Hardware engine. The research team experimentally evaluated the performance of the developed system. System achieved key generation rate of over a 14.5-dB transmission loss greater than 200 kbps. [9]

Zhang et al. research on High-dimensional quantum key distribution which offer the possibility of high secure key rate with high information of photon efficiency. Consider High dimensional quantum key distribution (HDQKD) based on the time energy entanglement produced by natural parametric down conversion and show that secure against collective attacks. Its security rests upon visibility data obtained from Franson and compound interferometers that probe photon-pair frequency correlations and arrival-time correlations. From these measurements, an upper bound can be established on the eavesdropper's Holevo information [10].

III. OUR APPROACH

In this research focused on quantum network for the telecommunication area with the quantum computing and quantum cryptography systems.

In the field of telecommunications, data retention (or data preservation) generally refers to the storage of call detail records (CDRs) which is a data record produced by a telephone exchange or other telecommunications equipment which documents the details such as a telephone call or other communications transaction (e.g., text message) that passes through that facility or device. The record contains various attributes of the call, such as time, duration, source number, destination number, and completion status. It is the automated equivalent of the paper toll tickets that were written and timed by operators for calls which take long distance in a manual telephone exchange of telephony and internet transaction data (IPDRs) and traffic by governments and commercial organizations. It is often argued that data retention is necessary to combat terrorism, cyber and other crimes. Data retention may assist the police and security services to identify potential terrorists and their associate before or after an attack has taken place.

One of the most used technology is Unispeed Blue Shield Management System Figure 4. Unispeed Data retention devices consistent more than 10 million concurrent sessions in memory and delivers more than 500.000 records per second. In Unispeed proprietary log storing the CDR records format significantly reduces the storage requirement. No central data repository is required and no data transfers to mediation system, as both can be handled by each retention device remotely.

The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or guess to be impossible using only classical. Difference between classical cryptography and Quantum cryptography is Quantum cryptography use separate channel to distribute keys. Quantum networks allow physically separate quantum systems for the transportation of quantum information. In addition using quantum key distribution algorithms can have a secure communication. It enables to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages, as it is the most well-known example of the group of quantum cryptographic tasks. Quantum cryptography elegantly provide security by enabling the unconditionally secure transmission of a random binary key between Data discovery and pattern analysis from call detail records data warehouses and other data analytic devices. The big data which are from call detail records from any telecommunication users' needs some privacy controls because staff dealing with this specific big data should be honest and trustable person. Quantum cryptography provides maximum protection and increases the storage capacity and security strength of the big data with less complexity. As a consequence referenced as Quantum Key Distribution is the security of the transmission is ensured by the no-cloning theorem that prohibit the perfect reproduction, or cloning, of a quantum system without disturbing.

Quantum key distribution Figure 2 which the security of encryption that uses relies on the foundations of quantum mechanics, in opposite to traditional public key cryptography, which depend on the computational difficulty of certain mathematical functions, and cannot provide any sign of intruder at any point in the communication process, or any mathematical evidence as to the actual complexity of turn other way round the one way functions used. Within the network information processing can be done using quantum logic gates. A quantum gate or quantum logic gate is an imperfect quantum circuit operating on a small number of cubits. They are the analogues for quantum computers to classical logic gates for conventional digital computers.

Uses of frequency comb which is a spectrum consisting of a series of discrete, equally spaced elements Frequency combs can be created by a number of mechanisms, including amplitude modulation (AM) of a continuous wave laser or counter balancing of the pulse train generated by a mode locked laser. And Wavelength division multiplexing (WDM) the technique modulating numerous data streams, optical carrier signals of varying wavelengths of laser light, onto a single optical fiber. It enables bi-directional communication as well as multiplication of signal capacity. This may useful to compress several request to a single wave. Figure 1. A WDM system uses a multiplexer at the transmitter to join the number of signals together, and a demultiplexer at the receiver to split them apart. With the right type of fiber it is possible to have a device that does both simultaneously, and can function as an optical add-drop multiplexer.

In telecommunications companies wavelength division multiplexing systems are more popular, because they allow them to expand the capacity of the network without prefer more fiber. By using WDM and optical amplifiers, they can accommodate several generations of technology enlargement in their optical infrastructure without having to repair the backbone network. Capacity of a given link can be developed simply by upgrading the multiplexers and demultiplexers at each end.

IV. CONCLUSION

Security is a major problem in telecommunication field. It produces a lot of negative effects and those effects can cost millions of dollars, or even billions and it can effect even for life security. We have studied about securing telecommunication field using Quantum Cryptography, Quantum Networks and Fibre optics to reduce Eve attack and secure important data in the warehouses Figure 3. Quantum Cryptography use separate channel to transport keys. Eves can't easily get the keys. Best way to secure data is use Quantum Cryptography.

V. FUTURE WORK

Quantum systems need to be isolated from the rest of world in order to work. Quantum cryptography is absolutely secure in theory. However, practical implementations often different from the theory description, there can have paths to break the security for eavesdropping. By openly publishing all this research results, we ensure hardening of quantum communication technology against all possible attacks. And have practical implementation on quantum cryptography in telecommunication.

APPENDIX

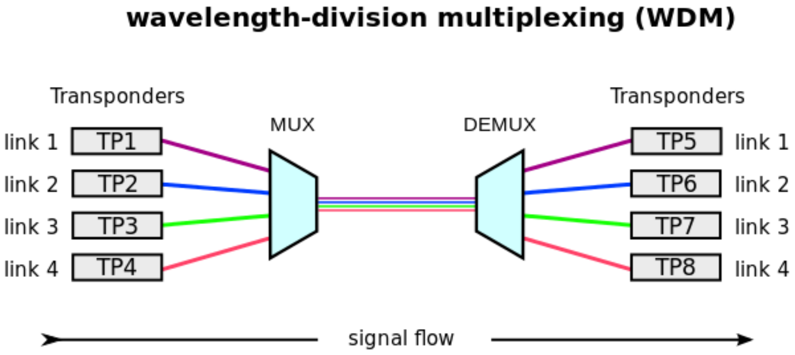


Figure 1 Wavelength Division Multiplexing

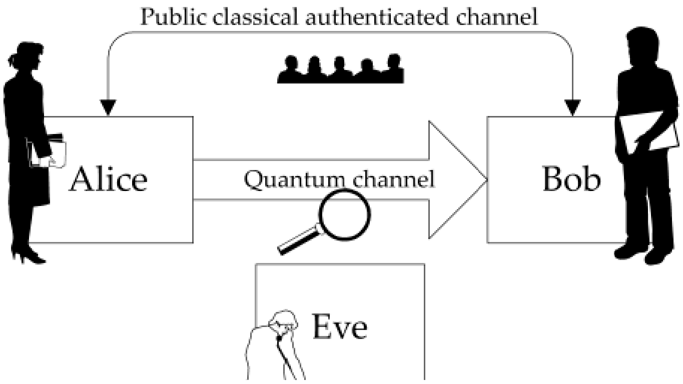
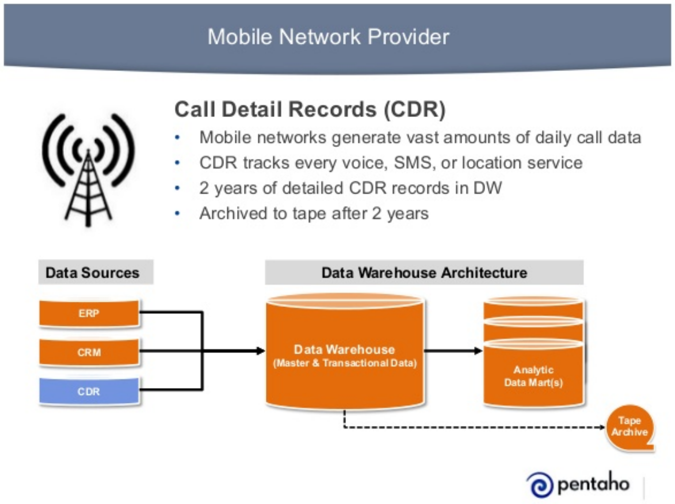


Figure 2 Quantum key distribution comprises a quantum channel and a public classical authenticated channel.


Mobile Network Provider

Call Detail Records (CDR)

- Mobile networks generate vast amounts of daily call data
- CDR tracks every voice, SMS, or location service
- 2 years of detailed CDR records in DW
- Archived to tape after 2 years

Figure 3: Call Detail Records (CDR)

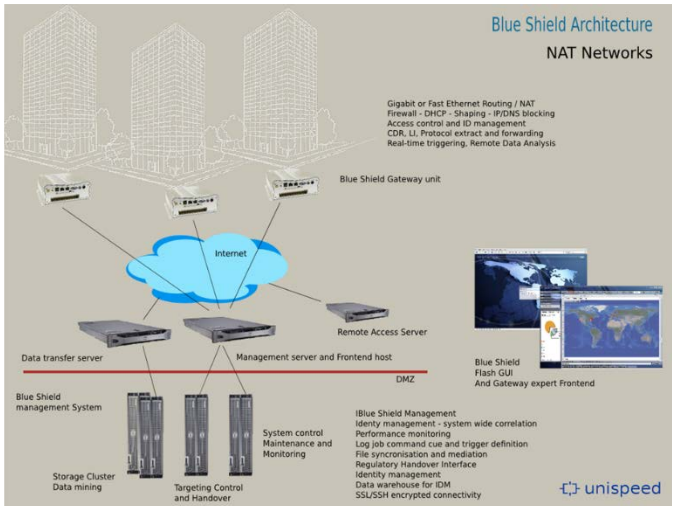

Blue Shield Architecture
NAT Networks
Gigabit or Fast Ethernet Routing / NAT
Firewall - DHCP - Shaping - IP/DNS blocking
Access control and ID management
CDR, LI, Protocol extract and forwarding
Real-time triggering, Remote Data Analysis
Blue Shield Gateway unit
Internet
Remote Access Server
Data transfer server
Management server and Frontend host
DMZ
Blue Shield
Flash GUI
And Gateway expert Frontend
Blue Shield
management System
System control
Maintenance and
Monitoring
Storage Cluster
Data mining
Targeting Control
and Handover
IBlue Shield Management
Identy management - system wide correlation
Performance monitoring
Log job command cue and trigger definition
File syncronisation and mediation
Regulatory Handover Interface
Identity management
Data warehouse for IDM
SSL/SSH encrypted connectivity
unispeed

Figure 4: Unispeed Blue Shield Management System

ACKNOWLEDGMENT

Our sincere thanks goes to the lecturer in charge Computer Networks Design and Implementation, Mr. Dhishan Dammearatchi of Sri Lanka Institute of Information Technology and authors we referred in this research paper.

REFERENCES

[1] P. Townsend, B. Labs and U. Ipswich, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing", Electronics Letters, vol. 33, no. 3, pp. 188 - 190, 2002.

[2] J. Roslund, R. de Araújo, S. Jiang, C. Fabre and N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs", Nature Photonics, vol. 8, pp. 109–112, 2013.

[3] Falahati and H. Meshgi,” Using Quantum Cryptography for Securing Wireless LAN Networks”, International Conference on Signal Processing Systems, 2009

[4] Thayananthan and A. Albeshri,” Big data security issues based on quantum cryptography and privacy with authentication for mobile data center”, Procedia Computer Science, pp. 149 – 156, 2015

[5] A. Buhari, Z.A. Zukarnai, S.K. Subramaniam, H. Zainuddin, and S. Saharudin, “BB84 and Noise Immune Quantum Key Distribution Protocols Simulation: An Approach Using Photonic Simulator”, International Conference on Computer and Intelligent Systems & International Conference of Electrical, Electronics, Instrumentation and Biomedical Engineering, December, 2012.

[6] A. Tanaka, M. Fujiwara, S. W. Nam, “Ultra-fast quantum key distribution over a 97 km installed telecom fibber with wavelength division multiplexing clock synchronization”, in “Optics Express”, vol. 16, pp. 11354-11360, 2008.

[7] J. Rarity, P. Tapster, P. Gorman and P. Knight, "Ground to satellite secure key exchange using quantum cryptography", New Journal of Physics, vol. 4, pp. 82-82, 29 October 2002

[8] C. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology, vol. 5, no. 1, January 1992

[9] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki and A. Tajima, "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation", IEEE Journal of Quantum Electronics, vol. 48, no. 4, pp. 542-550, 2012.

[10] Z.Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, "Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry", Research Laboratory of Electronics, Vol. 112, 2014.

Figure 1
Available: https://upload.wikimedia.org/wikipedia/commons/thumb/9/9b/WDM_operating_principle.svg/400px-WDM_operating_principle.svg.png

Figure 2
Available: http://gva.noekeon.org/QCandSKD/Figures/AliceBobEve.png

Figure 3
Available:
http://image.slidesharecdn.com/verizonfinaldeck-130625193946-phpapp01/95/exclusive-verizon-employee-webina

Figure 4
Available:
http://www.unispeed.com/en/images/architecture_accessp_lan.png

AUTHORS

First Author – C.A. Senadheera, Sri Lanka Institute of Information Technology (Pvt) Ltd, Sri Lanka,
anupama.s1126@gmail.com

Second Author – V.S.S. Kaushalya, Sri Lanka Institute of Information Technology (Pvt) Ltd, Sri Lanka,
sandli.kaushalya@yahoo.com

Third Author – S.M.R.D. Mahavewa, Sri Lanka Institute of Information Technology (Pvt) Ltd, Sri Lanka,
smrdmahawewa@gmail.com

Fourth Author - N. Sukanthan**,** Sri Lanka Institute of Information Technology (Pvt) Ltd, Sri Lanka,
sukanthan2011@gmail.com

Fifth Author - C.A.J.A. Rogess, Sri Lanka Institute of Information Technology (Pvt) Ltd, Sri Lanka,
anonrogess@gmail.com

Correspondence Author – Dhishan Dhammearatchi,
dhishan.d@sliit.lk