Hybrid and Optimized Approach for Resource Allocation in Optical Networks Secured by Quantum Key Distribution

Keefiat Ahmad Shah[1], Shaheen Naz[2]
[1]*M.Tech Scholar, Department of Electronic and communication, Sharda University*
[2]*Asst. Prof, Department of Electronic and communication, Sharda University*

Abstract: Optical network security is catching eyes for enhancing research attention as an optical network could affect a large number of users and services due to occurrence of loss of confidentiality during data transfer. Data encryption is an effective way to enhance the optical network security. QKD is found as secure mechanism to present fundamentals for data encryption at the endpoints of an optical network. This paper introduces the resource allocation issue in an optical network security by QDK. Firstly, we discuss a feasible architecture for a QDK-enabled optical network, in which three types of channels (TDCh, QSCh and PICh) over different wavelengths exploiting WDM. We chose to adopt OTDM to allocate multiple QSChs and PIChs over the existing wavelength for defending wavelength resources. For three types of channels, an OSTBC encoding algorithm is designed to allocate wavelength and time slot resources. Different security levels are included in the OSTBC encoding algorithm by considering different key updating periods. Illustrative simulation results demonstrate the impacts of various security-level configuration plots on resource allocation.

Introduction:

Quantum key appropriation (QKD) speaks to a future-evidence answer for assurance secure key appropriation as it depends on quantum mechanics. The basic principles of quantum mechanics, for example, quantum no-cloning theorem and the Heisenberg uncertainty principle, can be utilized to demonstrate that two remote endpoints of an optical connection can produce a mutual irregular secure key known just to them by utilizing explicit quantum communication protocols. The most critical and Extraordinary element of QKD is that the two imparting endpoints are capable to recognize the nearness of any outsider endeavoring to pick up learning of the key, and this component can essentially improve the security of the key dispersion framework. For each optical association with be built up in the system, notwithstanding the conventional information channel (TDCh), QKD requires a quantum signal channel (QSCh) and a public interaction channel (PICh) for secure key synchronization. Up until this point, no investigations have showed up on systems administration viewpoints and algorithmic arrangements identified with QSCh and PICh allocation in the fiber range. Utilizing wavelength-division multiplexing (WDM), QSChs and PIChs can have the equivalent fiber with TDChs to monitor fiber resources in optical systems. Since fiber spectral resources are limited, novel methodologies for powerful resource usage in QKD-empowered optical systems are important. In this paper, we examine the resource allocation issue that emerges when mutually serving the previously mentioned three kinds of channels, and we propose a powerful algorithmic answer for the issue. QKD and Qpsk modulations using OSCTBC encoding for performance evaluation in terms of blocking evaluation probability and key updating failures.

Resource Allocation Problem in QKD-Enabled Optical Networks

To depict the fundamental thought of QKD, Fig. 1 appears the point-to-point QKD framework for information encryption furthermore, decoding dependent on the most generally utilized QKD Convention (i.e.,BB84 [7]). Note that in long-remove systems, BB84 ought to be actualized in light of a polarization coding plan joined with a distraction technique, and in our framework demonstrate, we expect that vacuum states are embraced as decoy states.

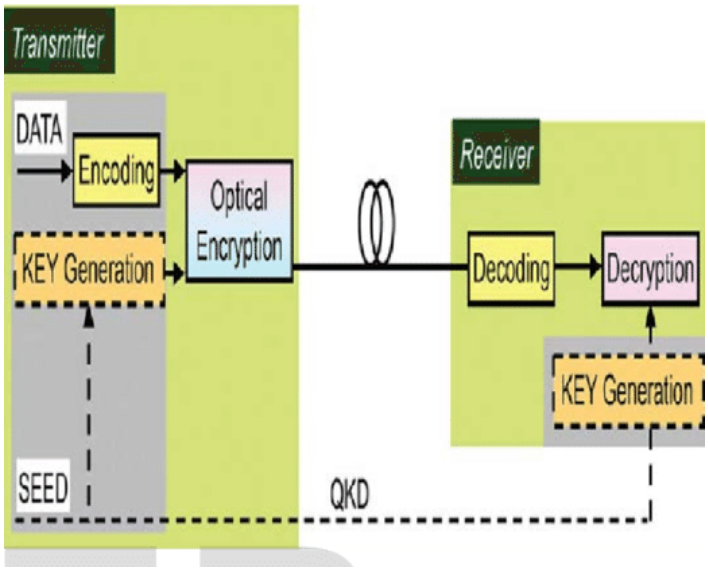


Fig -1. QKD Encryption and Decryption

The most important and unique feature of QKD is that the two communicating endpoints are able to detect the presence of any third party trying to gain knowledge of the key, and this feature can significantly enhance the security of the key-distribution system.

QKD-Enabled Optical Network Architecture

To incorporate QKD into existing optical networks, Fig. 2 demonstrates the proposed QKD-empowered optical organize design. It comprises of four planes: (application) plane, control plane, QKD plane, and information plane, in top-down request. The application plane creates association demands. The control plane is executed utilizing a SDN controller, and is responsible for resource the board furthermore, allocation for the QKD plane and information plane. Presenting SDN is helpful for overseeing the whole system's resources by means of logically centralized control. The QKD plane and information plane share fiber range resources utilizing WDM innovation to develop QSCh, PICh, and TDCh.

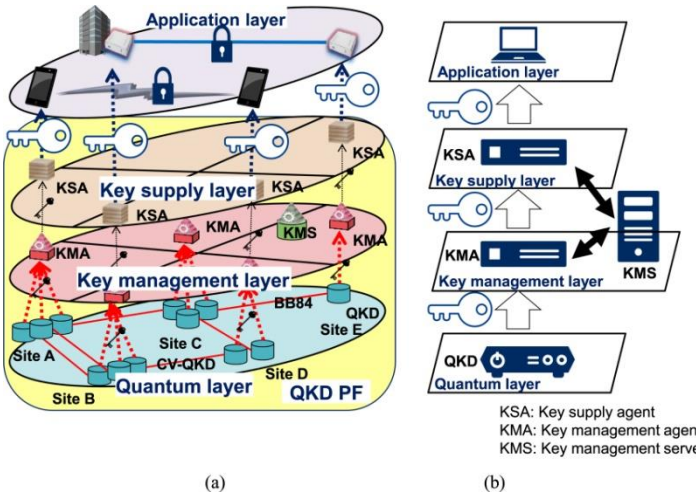


Fig-2. QKD Enabled Optical Network Architecture

Association demands with various security requests require the allocation of three kinds of channels. Since wavelength resources in an optical fiber are constrained and the greater part of the wavelengths ought to be used to help substantial private data transmission, we research an answer in which QSCh and PICh share wavelength limit utilizing optical time-division multiplexing (OTDM).

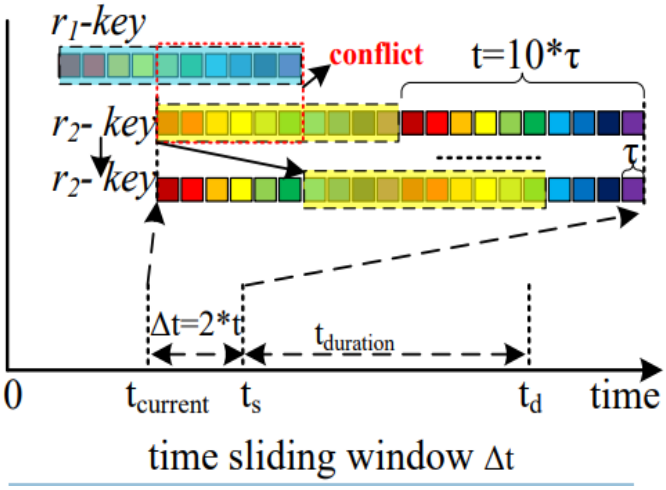
Literature Survey

Peter J. winger et al [1] in his book he describe the role of optical fiber communication technologies is to ensure that cost-effective network traffic scaling can continue to enable future communications services as an underpinning of today's digital information society. J. Zhu et al [2] mentioned in his paper that a malicious client can launch cross-domain attacks in the physical layer, the security issues in multi-domain EONs should not be overlooked. M. P. Fok et al [3] in his survey paper discussed the security threats in an optical network as well as present several existing optical techniques to improve the security. L. J. Wang et al [8] demonstrate the realization of quantum key distribution (QKD) when combined with classical optical communication, and synchronous signals within a single optical fiber.

Technical Analysis:

1. **RWTA in QKD-Enabled Optical Network:** In a QKD-empowered optical system, aside from TDChs, two extra channels, called QSChs and PIChs, are required to help secure key synchronization. The most effective method to dispense arrange resources to QSChs, PIChs, and TDChs is rising as a novel issue for the plan of a security-ensured optical system. This article tends to the resource allocation issue in optical systems secured by QKD. We initially talk about a conceivable design for a QKD-empowered optical system, where a SDN controller is responsible for dispensing the three kinds of channels (TDCh, QSCh, and PICh) over various wavelengths abusing WDM. To spare wavelength resources, we propose to embrace OTDM to assign numerous QSChs and PIChs over a similar wavelength. A RWTA calculation is intended to designate wavelength and schedule opening resources for the three sorts of channels. Diverse security levels are incorporated into the RWTA calculation by thinking about various key refreshing periods (i.e., the period after which the secure key between two endpoints must be refreshed). Illustrative simulation results demonstrate the impacts of various security-level configuration plots on resource allocation.
2. **Time- Sliding Window:** In a QKD-enabled optical network, a connection request is denoted as r (s, d, t s , td , Δt), Δt is the TSW. t is defined as key configuration time including key transmission, QKCh switching and setup. t current is the current time, t s =t current+Δt. Δt can be set as 0, t, or any value larger than t. When Δt is set as 0, it shows that r has no security requirement. When Δt is set as t, the related QKCh must be built immediately upon receiving the connection request. When Δt is larger than t, the related QKCh can start being built within the [0, Δt-t]. Here, we set Δt=2*t as an example. τ is the smallest time granularity of the TSW, which means that control plane can choose when to start building QKCh by setting the start time of the TSW within [0, Δt-t] and sliding the window by integral multiples of τ to the right. We set t=10*τ as an

example, within Δt, there are ten possible positions for r to find a time-slot of size t to build the QKCh.



3. **RWTA algorithm with TSW:** A RWTA calculation is proposed with TSW for a QKD-empowered optical system, which comprises of three stages.In stage 1, TDCh is distributed on the physical topology as indicated by K-briefest way (KSP) directing calculation and First Fit (FF) wavelength-assignment calculation. W(P) in this progression is characterized as the arrangement of accessible wavelength resources on the chose course of a connection. Resource allotment for PICh is same as QSCh in light of the fact that they all possess availability for secure key synchronization as depicted in Section 2. Note that every connection request designates a whole wavelength for TDCh, and a vacancy for QSCh (PICh). In stage 2, Dijkstra calculation is utilized to process and choose a particular course of QSCh (and PICh) on the physical topology, and FF calculation is utilized to assign schedule openings for QSChs (and PIChs). Not quite the same as stage 1, schedule vacancies are allotted for each connection request with secure key demand in stage 2, and diverse estimations of TSW can be utilized for various connection requests. Stage 3 is utilized for key refreshing for the connection request. Dijkstra calculation is likewise utilized for directing calculation. In stages 2 and 3, WT(P) is characterized as accessible schedule vacancy set on the wavelengths saved for QSCh through the processed course. In this calculation, Δt and T can be set as various qualities to assess related execution.
4. **WDM Technology**: WDM is an innovation that empowers different optical signals to be transmitted by a solitary fiber. Its standard is basically equivalent to Frequency Division Multiplexing (FDM). That is, a few signals are transmitted utilizing distinctive bearers, involving non-overlapping portions of a frequency spectrum. If there should be an occurrence of WDM, the spectrum band utilized is in the district of 1300 or 1550 nm, which is two wavelength windows at which optical fibers have exceptionally low signal loss.

Methodology:

Initial specifications of an optical network system are performed by Nodes deployment, wavelength assignment and Qpsk modulations. Quantum key distribution is done using OSTBC encoding. Performance evaluation is evaluated in terms of blocking probability and key updating failures.

Results:

Below are the various approaches implied to meausre the results of QKD.

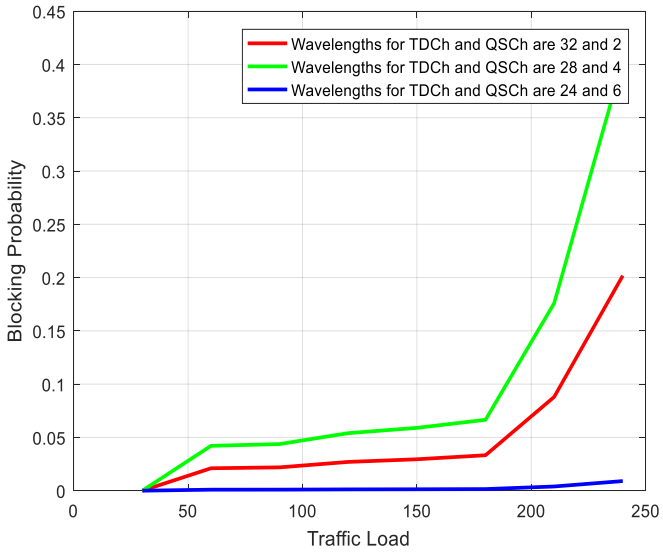


Fig 3.

In fig 3, Traffic load is calculated against blocking probability where three different wavelengths for TDCh and QSCh are calculated such as (1) 32 and 2, 28 and 4 & 24 and 6. Blocking probability must be low to make it more secure for which we have used base approach using quantum key approach. The lowest probability is measured for wavelength 24 & 6 of TDCh and QSCh.

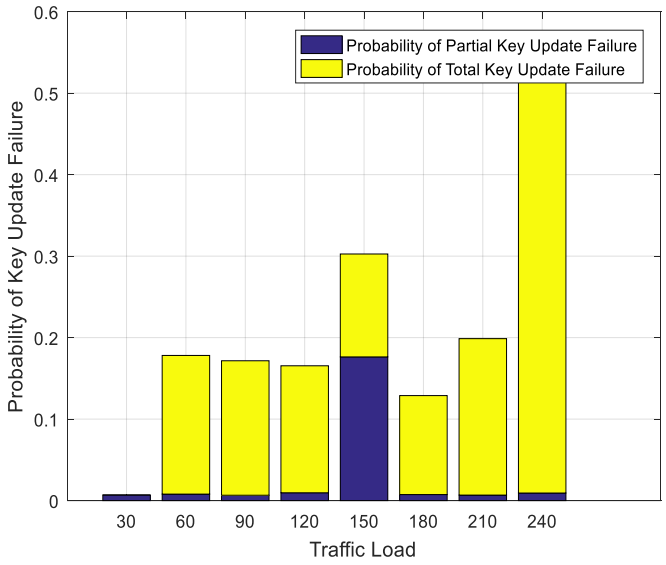


Fig 4.

In Fig 4, the probability of key update failure is calculated where yellow color is showing the total key update failure and blue color is showing the partial key update failure and it is near about 0.08 using base approach.

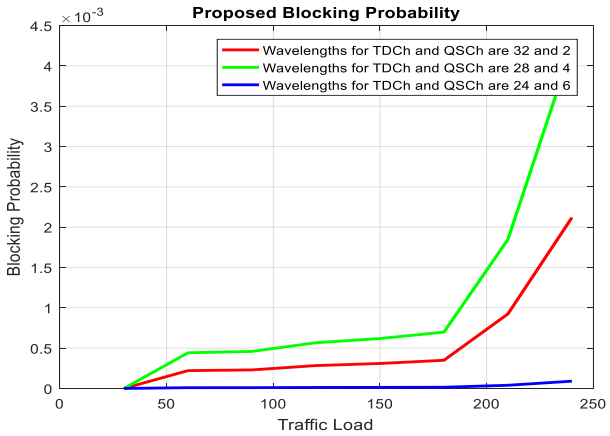


Fig 5.

In Fig 5, proposed blocking probability is calculated of base approach using quantum key + OSTBC encoding approaches to make it more secure and it must be low. Lowest value is measured for wavelength 24 & 6 of TDCh and QSCh.

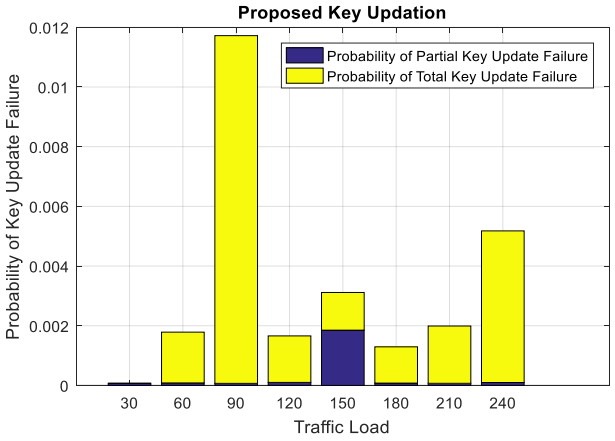


Fig 6.

In Fig 6, Proposed key update failure is calculated using quantum key + OSTBC encoding. The yellow indication using probability of failure of total key update and blue shows the partial key update failure. It is observed that it is highly low than base approach used in fig 3.

We have used OSTBC encoding using proposed approach.

Conclusion:

In this research paper, here we shows the blocking probability of base approach while using quantum key+ OSTBC encoding is very low which makes it more secure than using quantum key with base approach without using OSTBC encoding.

References:

[1]. P. J. Winzer, "Scaling Optical Fiber Networks: Challenges and Solutions," Optics and Photonics News, vol. 26, no. 3,Mar. 2015, pp. 28–35.

[2]. J. Zhu et al. ,"Attack-Aware Service Provisioning to Enhance Physical-Layer Security in Multi-Domain EONs," J. Lightwave Tech., vol. 34, no. 11, June 2016, pp. 2645–55.

[3]. M. P. Fok et al., "Optical Layer Security in Fiber-Optic Networks," IEEE Trans. Info. Forensics and Security, vol. 6, no. 3, Sept. 2011, pp. 725–36.

[4]. P. Jouguet et al., "Field Test of Classical Symmetric Encryption with Continuous Variables Quantum Key Distribution, "Optics Express, vol. 20, no. 13, June 2012, pp. 14,030–41.

[5]. S. Debnath et al., "Demonstration of a Small Programmable Quantum Computer with Atomic Qubits," Nature, vol. 536, Aug. 2016, pp. 63–66.

[6]. H.-K.Lo et al., "Quantum Cryptography, "Encyclopedia of Complexity and Systems Science, vol. 8, Springer, 2009, pp.7265–89.

[7]. A. V. Gleim et al.,"Secure Polarization-Independent Subcarrier Quantum Key Distribution in Optical Fiber Channel Using BB84 Protocol with a Strong

Reference," Optics Express, vol. 24, no. 3, Feb. 2016, pp. 2619–33.

[8]. H.-K. Lo et al., "Secure Quantum Key Distribution," Nature Photonics, vol. 8, July 2014, pp. 595–604.

[9]. L. J. Wang et al., "Experimental Multiplexing of Quantum Key Distribution with Classical Optical Communication," Applied Physics Letters, vol. 106, no. 8, Feb. 2015, pp. 081108.1–4.

[10]. S. Bahrani et al., "Optimal Wavelength Allocation in Hybrid Quantum-Classical Networks," Proc. 24th Euro. Signal Processing Conf., Budapest, Hungary, Aug.–Sept. 2016.

[11]. N. A. Peters et al., "Dense Wavelength Multiplexing of 1550 nm QKD with Strong Classical Channels in Reconfigurable Networking Environments," New J. Physics, vol. 11, no. 4, Apr. 2009, pp. 045012.1–17.

[12]. M. Peev et al., "The SECOQC Quantum Key Distribution Network in Vienna," New J. Physics, vol. 11, no. 7, July 2009, pp. 075001.1–37.

[13]. B. Wen et al., "Routing, Wavelength and Time-Slot Assignment in Time Division Multiplexed Wavelength-Routed Optical WDM Networks," Proc. IEEE INFOCOM 2002, vol. 3, New York, June 2002, pp. 1442–50.

[14]. M. Taha et al.,"Key-Updating for Leakage Resiliency with Application to AES Modes of Operation,"IEEE Trans. Info. Forensics and Security, vol. 10, no. 3, Mar. 2015, pp. 519–28.

[15]. Z. Zhu et al.,"Dynamic Service Provisioning in Elastic Optical Networks with Hybrid Single-/Multi-Path Routing," J. Lightwave Tech., vol. 31, no. 1, Jan. 2013, pp. 15–22.