A. M. Balamurugan*, A. Sivasubramanian and B. Parvathavarthini

QKD-Based Secured Burst Integrity Design for Optical Burst Switched Networks

Abstract: The field of optical transmission has undergone numerous advancements and is still being researched mainly due to the fact that optical data transmission can be done at enormous speeds. It is quite evident that people prefer optical communication when it comes to large amount of data involving its transmission. The concept of switching in networks has matured enormously with several researches, architecture to implement and methods starting with Optical circuit switching to Optical Burst Switching. Optical burst switching is regarded as viable solution for switching bursts over networks but has several security vulnerabilities. However, this work exploited the security issues associated with Optical Burst Switching with respect to integrity of burst. This proposed Quantum Key based Secure Hash Algorithm (QKBSHA-512) with enhanced compression function design provides better avalanche effect over the conventional integrity algorithms.

Keywords: optical burst switching, integrity, quantum key distribution, avalanche effect

PACS® (2010). 42.81.Uv, 42.79.Sz, 42.50.Nn

DOI 10.1515/joc-2014-0093
Received December 14, 2014; accepted February 12, 2015

1 Introduction

The rapid internet growth is facing limits from its own success. The number of internet users and variety of applications transported are growing at a higher rate. As a result of which the best growing paradigm is facing limits. Optical networks are high capacity telecommunication networks based on optical technologies that provide routing, grooming and restoration at the wavelength level as well as wavelength-based services. Optical networks use virtual fibres, they transfer data on to a single fibre at different frequencies [1]. Restoration that is done in optical layer is faster and efficient. Cost is reduced as optical signals can be transferred over a long distance by using optical fibre, without the need of amplifiers and converters [2]. WDM takes optical signals and converts it to a specific wavelength or frequency and then sends them down on the same fibre. The possibility of carrying IP traffic over WDM was achieved by the three switching technologies Optical Circuit Switching (OCS), Optical Packet Switching (OPS), and Optical Burst Switching (OBS). In optical circuit switching (OCS) a dedicated path is established for communication. A major issue with circuit switching is that all resources must be available and dedicated through the network session before the communication takes place. Otherwise, the communication request will be blocked. This can result in potential channel inefficiency. Optical packet Switching is not entirely optical. The signals are converted to electrical form before switching and processing. This means that the major disadvantage of optical packet switching is that the speed and efficiency are lost due to the O/E/O conversion. The biggest problem at the moment is the lack of optical Random Access Memory needed for buffering the packets. Additionally, very high switching rates are needed in packet networks which are causing problems [3]. OBS tries to combine the best features of both OCS and OPS, while avoiding the mentioned above said drawbacks. Due to the technological constraints optical burst switching (OBS) has been initiated. OBS granularity is between circuit and packet switching. There is a separation between control information (header) and data. Header and data are usually carried in different channels with a strong separation in time [4].

OBS architecture consists of two nodes: an edge router and a core router which is shown in Figure 1. Ingress node assembles the data packets from various sources into a burst. Egress node disassembles the burst into packets again. The process of combining packets from various sources at the ingress node is called burst assembly. In simpler form the size of each burst ranges between 40,000 to 1,200,000 packets.

For every data burst a control header will be generated. The control header contains the information which is required to route the data burst from source

***Corresponding author: A. M. Balamurugan,** St. Joseph's College of Engineering, Chennai 600119, Tamil Nadu, India, E-mail: bala_am2000@yahoo.com
A. Sivasubramanian, Tagore Institute of Engineering and Technology, Deviyakurichi, Aathur Taluk, Salem 636112, Tamil Nadu, India
B. Parvathavarthini, St. Joseph's College of Engineering, Chennai 600119, Tamil Nadu, India

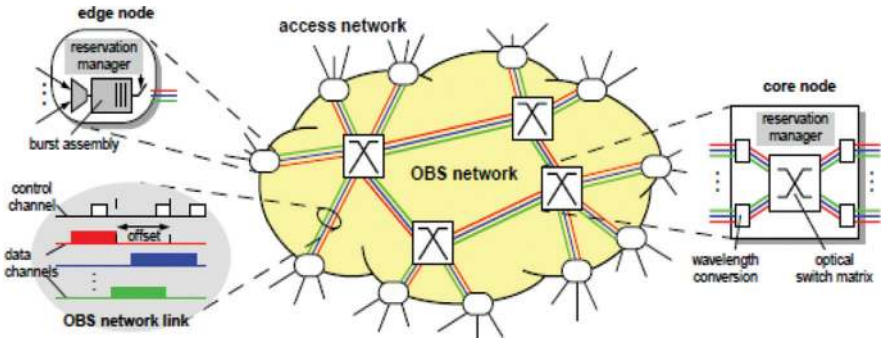

Figure 1: OBS network architecture [4]. Courtesy: Gaugher et al [4].

to destination. When the burst header reaches the OBS core router, it is converted to electronic signal and processed electronically; the OBS core router can make efficient scheduling decisions in selecting the outgoing WDM channels for data bursts by simply processing burst headers [5]. If at least one outgoing WDM channel is available for the duration of the burst, a channel will be selected to carry the data burst. Otherwise, the data burst will be dropped. Unfortunately, OBS networks suffer from security vulnerabilities. OBS networks can provide security services to traffic that do not necessarily have an IP layer. This will likely be the case for the majority of traffic served by the OBS layer. Any node under attack in a network exhibits an anomalous behaviour called the malicious behaviour. In this situation, the entire operation of a network gets disturbed. Several attacks like black hole, wormhole, rushing are to be defined and such behaviour of a node to be detected [6]. Therefore, it becomes mandatory to define the normal and malicious behaviour of a node. Whenever a node exhibits a malicious behaviour under any attack, it assures the breach of security principles like availability, integrity, confidentiality, etc.

2 Vulnerabilities in OBS networks

The burst header is responsible for making the WDM channel reservation for its corresponding burst. If the scheduling request is rejected at one of the OBS core routers, there will be no valid optical path setup for the arriving burst. Since the burst has been sent, it will arrive at the input of the core router. Then the burst is no longer connected with its header and becomes an orphan burst [7]. As a result, these orphan bursts can be tapped off by some undesirable party, thereby compromising its security.

The one-to-one correspondence between the burst header and its corresponding burst is indicated by the offset time present in the burst header. This one-to-one correspondence can be violated by sending a malicious header to the same burst. This results in the route and the destination for the burst being modified by the malicious header, even though a valid path has been set up by the authentic header, and this type of attack is called as redirection of data bursts. Replay attack refers to capturing a valid but expired burst and transmitting that at a later time, or by sending an expired burst header to make the optical burst to circulate in the OBS network, thereby delaying its delivery to the destination.

The intruders compromises any one node and copies and replicate its original burst address. The Duplicated Copies of the Burst address are then feed to the next intermediate node. Once the intermediate node receives the burst header it starts to reserve the resources for the duplicate copies. Due to this the intermediate nodes buffer may overflow. At last, it results in not permitting the intermediate node to reserve any resource even if they are legitimate burst header. This is called burst header flooding attack [8, 9].

Though an efficient network with all the advantages exists it suffers from security problems. In order to overcome the security black hole an advanced mechanisms are required. The various principles of providing this security are burst confidentiality at ingress and egress routers, per hop header authentication and effective key management [10].

3 Quantum cryptography

Quantum cryptography relays on Heisenberg's uncertainty principle. It states that, for certain pairs the physical properties cannot be calculated simultaneously [11].

This is because when one property is being calculated, the other gets disturbed and it is difficult to compute. A separate channel is used in quantum distribution to exchange secret key. The separate channel carries the Q bit which is photons of random polarization. The photons are not constant through out. They get altered when they are measured. Thus this fact makes the channel detection mandatory. Thus data through this channel cannot be intercepted without being detected. This is achieved by sender encoding the bits of the key as quantum data and sending them to receiver.

If third party tries to learn these bits, then the messages will be disturbed and both the Sender and Receiver will notice thereby making it unbreakable. The key is thus typically used for encrypted communication. The security of QKD can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something that is not possible with classical key distribution. This is frequently described as "unconditional security", even though there are some minimal assumptions required including that the laws of quantum mechanics apply and that Sender and Receiver are able to authenticate each other, i.e. Third party should not be able to impersonate Sender or Receiver as otherwise a man-in-the-middle attack would be possible [12].

The two popular protocols for quantum key generation are B92 and BB84. This proposed work uses Two Stage Quantum Key Distribution protocol. This protocol makes use of both B92 and BB84. In the first stage, Ingress node sends a random sequence of photon using B92, and in the second stage, Egress node will use BB84 to send the photons in which Egress node's measurement results are "N" in the first stage. The complexity order of the two stage protocol is almost equal to the B92 protocol and efficiency is almost equal to the BB84 protocol [13]. The shared quantum keys were stored in RAM. The initial value (IV) will be chosen from the permuted combination of the stored secret keys. This will result in turn provide more security for the proposed algorithm.

4 Burst integrity control

This proposed work mainly focussed on providing integrity control for the burst. Burst integrity is the ability to prevent an active attacker to modify the information in the burst without the end users notice. When the information becomes modified it proves that the message is not valid [14]. To prove the burst integrity certain algorithms have been emphasized. The two popular algorithms are SHA0 and SHA1. Though these algorithms have certain special features but these algorithms are more prone to linear and nonlinear attacks. To prevent these attacks SHA2 algorithm has been lighted. SHA2 algorithm has overcome the drawbacks in SHA0 and SHA1 algorithm. The SHA2 algorithm have led to 24 step attacks against SHA 256 and SHA 512 for making the burst secured from these attacks [15]. Although SHA 512 makes it compatible there are certain compression features that make it open for attacks.

The conventional algorithm is given below [16]

$$
\begin{aligned}
a_i &= \Sigma_0(a_{i-1}) + f_{MAJ}(a_{i-1}, b_{i-1}, c_{i-1}) \\
&\quad + \Sigma_1(e_{i-1}) + f_{IF}(e_{i-1}, f_{i-1}, g_{i-1}) + h_{i-1} + K_i + w_i \\
b_i &= a_{i-1} \\
c_i &= b_{i-1} \\
d_i &= c_{i-1} \\
e_i &= d_{i-1} + \Sigma_1(e_{i-1}) + f_{IF}(e_{i-1}, f_{i-1}, g_{i-1}) + h_{i-1} + K_i + w_i \\
f_i &= e_{i-1} \\
g_i &= f_{i-1} \\
h_i &= g_{i-1}
\end{aligned}
$$

$$\Sigma_0(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x)$$

$$\Sigma_1(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x)$$

$$f_{IF}(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$f_{MAJ}(x, y, z) = (x \wedge y) \oplus (x \wedge y) \oplus (z \wedge x)$$

$$W_i = \begin{cases} m_i & for\ 0 \le i \le 15 \\ \sigma_1(W_{i-2}) + W_{i-2} + \sigma_0(W_{i-15}) + W_{i-16} & for\ 16 \le i \le 63 (or\ 80) \end{cases}$$

$$\sigma_0(x) = ROTR^{1}(x) \oplus ROTR^{8}(x) \oplus SHR^{7}(x)$$

$$\sigma_1(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^{6}(x)$$

There are 8 registers used in conventional SHA 512 algorithm. They are designated from a to h. Here only the registers a and e are nonlinearly updated. Whereas the other register values are just copied. The round function of SHA 512 algorithm uses $\sum_0$ and $\sum_1$. Consider the equations $\sum_0(x) = X$ and $\sum_1(x) = X$, when these equations find any solutions a "fixed point" for transformations for $\sum_0$ and $\sum_1$ transformations are obtained. Here XORs are only used by both the transformations and the equations $(\sum_0 \oplus I_{64})(x) = 0$ and $(\sum_1 \oplus I_{64})(x) = 0$ for SHA 512 are equivalently looked at. From the fixed points obtained from $\sum_0$ and $\sum_1$ of SHA 2 algorithm, an analysis has been made and found that they have common fixed points. These common fixed points are of simpler and easy

structures. When they are expressed in 64 bit quantities the bits can either be 0 or 1 [15, 16]. The numeral value for these common fixed points are 0 and −1. This is one of the strategies which make nonlinear local collisions of higher probability.

Somitra Kumar et al. [17] suggested some improvements in conventional SHA 512 algorithm (SShash): The affine functions Γ_0 and Γ_1 replaces the linear function $\sum_0$ and $\sum_1$ respectively. The first point for SHA 512 algorithm is considered as $\Gamma_i(x) = \times$ where some $\times$ implies $(\sum_i \oplus I_{64})$ $x = b_i$ and $\Gamma_i(x) = x'$ for Some $\times$ implies $\Gamma_i(x) = (\sum_i \oplus I_{64})$ $x = b_i$; where $i = 0.1$. The first point holds good; if both b_i and b_i' are not in column space of $(\sum_i \oplus I_{64})$. Similarly the second point is applicable only if $b_0 \oplus b_1$ and $b_0 \oplus b_1$ are not in the column space of $(\sum_0 \oplus \sum_1)$.The design process of SHA 512 algorithm round function uses XOR operation. Here the XOR operation is used lesser number of times when compared to the modular addition. The mixing of $+$ and $\oplus$ operations provide a better result. This is because the XOR differentials are difficult to analyse the values of a and e registers. The proposed algorithm also uses these suggestions to overcome all the pitfalls and produce a better digest value for the secured burst transmission. Moreover the proposed algorithm uses QKD-based Initial Vector selection.

5 Proposed QKD-based SHA-512 (QKBSHA-512) algorithm for burst integrity

The proposed QKBSHA-512 algorithm suggests some modifications to improve the avalanche effect of the conventional SHA-512 algorithm. Avalanche effect is considered to be desirable property to investigate any encryption algorithm. Avalanche effect is defined as the ratio of total number of flipped bits to total number of bits. It is evident that when the avalanche effect is high the security to the burst is also very high.

The Enhanced Round Function Includes:

- The Initial vector value for the first round function will be taken from the permuted combination of shared QKD keys which is stored in RAM.
- The e register value computation uses XOR differentials instead of modular addition. Because it is more difficult to analyse and lesser time when compared to the modular addition.
- The new affine functions Γ_0 and Γ_1 replaces the $\sum_0$ and $\sum_1$ because it is highly resilient to the nonlinear attacks.
- It has already been proven that the QKD-based shared keys are theoretically unbreakable. So its gives stronger support to the proposed algorithm.
- The d and h registers updation uses modified a and e register values.

The proposed QKBSHA-512 algorithm is as follows:

$$
\begin{aligned}
a_i &= h_{i-1} + \Gamma_0(a_{i-1}) + f_{MAJ}(a_{i-1}, b_{i-1}, c_{i-1}) + \Gamma_1(e_{i-1}) \\
&\quad + f_{IF}(e_{i-1}, f_{i-1}, g_{i-1}) + K_i + W_i \\
b_i &= a_{i-1} \\
c_i &= b_{i-1} \\
d_i &= c_{i-1} + a_{i-1} \\
e_i &= (d_{i-1} + \Gamma_1(e_{i-1}) + f_{IF}(e_{i-1}, f_{i-1}, g_{i-1}) + h_{i-1} + K_i) \oplus w_i \\
f_i &= e_{i-1} \\
g_i &= f_{i-1} \\
h_i &= g_{i-1} + e_{i-1}
\end{aligned}
$$

$$
\begin{aligned}
f_{IF}(x, y, z) &= (x \wedge y) \oplus (\neg x \wedge z) \\
f_{MAJ}(x, y, z) &= (x \wedge y) \oplus (x \wedge y) \oplus (z \wedge x)
\end{aligned}
$$

$$
\begin{aligned}
\Sigma_0(x) &= ROTR^{18}(x) \oplus ROTR^{44}(x) \oplus ROTR^{29}(x) \\
\Sigma_1(x) &= ROTR^{44}(x) \oplus ROTR^{8}(x) \oplus ROTR^{21}(x)
\end{aligned}
$$

$$
\begin{aligned}
\Gamma_0(x) &= \Sigma_0(x) \oplus b_0 \\
\Gamma_1(x) &= \Sigma_1(x) \oplus b_1
\end{aligned}
$$

$$
\begin{aligned}
b_0 &= \Sigma_0(x).x \\
b_1 &= \Sigma_1(x).x
\end{aligned}
$$

$$
W_i = \begin{cases} m_i & for\ 0 \le i \le 15 \\ \sigma_1(W_{i-2}) + W_{i-2} + \sigma_0(W_{i-15}) + W_{i-16} & for\ 16 \le i \le 63 (or\ 80) \end{cases}
$$

$$
\begin{aligned}
\sigma_0(x) &= ROTR^{7}(x) \oplus ROTR^{38}(x) \oplus SHR^{34}(x) \\
\sigma_1(x) &= ROTR^{15}(x) \oplus ROTR^{61}(x) \oplus SHR^{26}(x)
\end{aligned}
$$

6 Results and discussions

With the above said modifications incorporated into the conventional algorithm, the proposed QKBSHA-512 algorithm was successfully executed in the Xilinx ISE platform. The HDL used is verilog. The simulation criteria are shown in Table 1. The proposed QKBSHA-512 algorithm contains 80 rounds with the input size of 2048 bits.

The performance was evaluated and compared with the conventional algorithm and SShash algorithm. The

Table 1: Simulation criteria.

Simulation Criteria	
Integrity algorithm	QKBSHA-512
Number of rounds	80
Digest size	512
Burst size	2048 bits
Number of IP source	2
Packet Size	1024 bits
Number of rounds	80
HDL	Verilog
Version	Xilinx ISE 14.1

Table 2: Avalanche effect comparison of proposed QKBSHA-512 with conventional algorithms.

Burst Integrity Algorithm	Avalanche Effect Comparison		
	Digest size (Bits)	Average number of flipped bits	Avalanche effect (%)
Conventional SHA 512 Algorithm	512	264	51.5
SShash Algorithm	512	270	52.7
Proposed QKBSHA-512 Algorithm	512	**282**	**55.0**

Table 3: Time complexity analysis of proposed QKBSHA-512 algorithm with conventional algorithms.

Burst Integrity Algorithm	Time Complexity (Device: VIRTEX7)				
	Total Time in ns	Logic	Logic (%)	Route	Route (%)
Conventional SHA512 Algorithm	569.8ns	333.3ns	58.5	236.2ns	41.5
SShash Algorithm	578.8ns	263.8ns	45.6	314.9ns	54.4
Proposed QKBSHA-512 Algorithm	719.7ns	351.4ns	48.8	368.2ns	51.2

observations made are shown in Tables 2 and 3. Table 2 summarizes the avalanche effect comparison.

From Table 2, it can be concluded that the avalanche effect of the proposed QKBSHA-512 algorithm is better than the conventional algorithm. The evaluation is performed for different types of input combinations. If one byte is changed in the input, there are a drastic number of changes in the output 512 digest value. This is because the new compression function is suggested in the proposed QKBSHA-512 model. Moreover, the proposed QKBSHA-512 algorithm is highly resilient to the nonlinear attacks.

The proposed QKBSHA-512 burst integrity algorithm is synthesized on commercial off the shelf FPGA system to test the physical building feasibility in silicon. The FPGA used for this purpose is VIRTEX 7. For comparison the conventional and SShash algorithm are also synthesized on the same FPGA. The propagation delay comparison of the three algorithms is presented in Table 3. The delay is the time taken for the generation of the digest after the inputs are applied. The delay is split as the delay consumed in the logic and the delay for the routing between the blocks of the system. The delay is less for the conventional when compared with SShash and proposed QKBSHA-512 algorithm. The delay is maximum for the proposed work as the system scales up in complexity. The increase in complexity is due to the increase in avalanche effect in the enhanced compression technique used for the proposed algorithm. When observed the increasing delay is contributed mainly due to the scale up in delay involved in routing. This may further be reduced by back annotation of the system and synthesising the system for speed optimization. At the cost of the extended propagation delay the integrity of the digest is improved under external attacks.

7 Conclusion

It can be concluded that the proposed QKBSHA-512 algorithm gives better avalanche effect than the conventional algorithms. The enhanced compression function design uses logic utilization which is almost equal to the conventional algorithm. The time complexity of the proposed algorithm is slightly higher than the conventional algorithms. But this delay variation is mainly due to the routing, and also it can be reduced in future. Moreover, this proposed work is resilient to the attacks in optical burst switched networks. This QKBSHA-512 with enhanced round function can be the best choice for real-time secure integrity applications of optical burst switched networks.

References

1. Qiao C, Yoo M. Optical burst switching (OBS) – A new paradigm for an optical internet. J High Speed Networks 1999;8:69–84.
2. Manoj Ramesh Rao R, Johny Richards R, Joel Manohar BA, Sivasubramanian A. Erbium doped fiber amplifiers: state of art. Int J Sci Technol Res 2013;2:316–19.
3. Balamurugan AM, Sivasubramanian A. Optical burst switching issues and its features. Int J Emerg Trends Technol Comput Sci 2013;2:306–15.

4. Gauger C, Dolzer K, Spath J, Bodamer S. Service differentiation in optical burst switching networks. Photonic Networks 2001;2001:124–32.
5. Haselton F. A PCM frame switching concept leading to burst switching network architecture. IEEE Commun Mag 1983;21:13–19.
6. Fok MP, Wang ZX, Deng YH, Prucnal PR. Optical layer security in fiber-optic networks. IEEE Trans Inf Forensics Secur 2011;6:725–36.
7. Chen YH, Verma PK, Kak S. Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks. Secur Commun Networks 2009;2:546–54.
8. Sreenath N, Muthuraj K, Vinoth G. Threats and vulnerabilities on TCP/OBS networks. International Conference on Computer Communication and Informatics (ICCCI), January 2012, pp. 1–5.
9. Balamurugan AM, Sivasubramanian A. Modeling the performance of DDoS attack in optical burst switched networks Aust J Basic Appl Sci (AENSI Journals) 2014;8:479–82.
10. Balamurugan AM, Sivasubramanian A. Quantum key based burst confidentiality in optical burst switched networks. Sci World J 2014;2014:Article ID 786493, 7 pages. doi:10.1155/2014/786493.
11. Bennet CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984, pp. 175–9.
12. Townsend PD, Phoenix SJD, Blow KJ, Barnett SM. Design of quantum cryptography systems for passive optical networks. Electron Lett 1994;30:1875–7.
13. Balamurugan AM, Sivasubramanian A. A novel QKD based secure edge router architecture design for burst confidentiality in optical burst switched networks. J Opt Commun 2014;35:109–16. ISSN (Online) 2191–6322, ISSN (Print) 0173–4911. doi:10.1515/joc-2014-0003.
14. Balamurugan AM, Chandana V, Sivasubramanian A. Survey of burst integrity protocols for optical burst switched networks. Int J Adv Res Electron Commun Eng (IJARECE) 2014;3:235–9.
15. Sanadhya SK, Sarkar P. Non-linear reduced round attacks against SHA-2 Hash family. In: Mu Y, and Susilo W, editors. Information security and privacy – ACISP 2008, The 13th Australasian Conference, Wollongong, Australia, 7–9 July 2008, Proceedings, volume 5107 of Lecture Notes in Computer Science. Springer.
16. Stallings W. Cryptography and network security: principles and practice. 5th ed. Prentice Hall, 2011.
17. Kumar S, Sarkar P. Attacking reduced round SHA-256. In Bellovin S, and Gennaro R, editors. Applied cryptography and network security – ACNS 2008, 6th International Conference, New York, NY, June 03–06, 2008, Proceedings, volume 5037 of Lecture Notes in Computer Science. Springer.