International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 2, February 2014

Survey of Burst Integrity Protocols for Optical Burst Switched Networks

A.M.BALAMURUGAN [1], V. CHANDANA [2], A.SIVASUBRAMANIAN [3]
Research scholar & Associate Professor[1], PG Scholar[2], Professor[3]
Department of Electronics and Communication Engineering
St.Joseph's College of Engineering, Chennai, Tamilnadu
INDIA

***Abstract*— Optical burst switching is one of the most promising technologies in the optical domain. In OBS network, bursts of data consisting of multiple packets are switched through the network all optically. A burst header packet is transmitted ahead of the burst in order to configure the switches along the burst's route. The burst header and the bursts are separated at the source, as well as subsequent intermediate nodes, by an offset time. Even though OBS has a greater advantage with high speed data transfer but if suffers from security vulnerabilities. Once the burst header is redirected by the malicious node, the burst may redirect to fake destination. In this paper, we discuss the various burst integrity algorithms for optical burst switched networks. Moreover we conclude that Secure Hash Algorithm finds to be an optimal solution for burst integrity.**

***Keywords* — Optical Burst switching, Attacks, Burst integrity, Secure hash algorithms.**

I. INTRODUCTION

Optical networks are high capacity telecommunication networks based on optical technologies that provide routing, grooming and restoration at the wavelength as well as wavelength based services. These optical networks use virtual fibres to transmit the data in a single link with different frequencies. Restoration made in any optical network has proved to be faster and efficient. Though these are the certain distinguishing features about optical networks, the most remarkable and accountable advantage is the cost reduction. The optical signals can be transferred over a long distance, thereby eliminating the use of amplifiers and converters. The optical networks have the possibility of reselling the bandwidth rather than the fibres.

This ease of access in optical networks has carved the concept of optical burst switching. OBS architecture consist of two nodes namely, the edge node and the core node which is shown in figure 1. The node which performs the assembly and the disassembly process in node architecture is the edge node. That is, the node which assembles the data packets from various sources into a burst is called as ingress node. The process of combining packets from various sources at the ingress node is called as burst assembly. Similarly, the node which disassembles the burst into packets again is done by the egress node. The burst disassembly process is performed at the egress node. The nodes excluding the ingress and the egress nodes are called the core nodes. Core nodes are also called as intermediate nodes. In the OBS concept the control packet consist of data burst and a header. The control packet contains the information which is required to route the data burst from source to destination. They also contain the information regarding the data burst length and the offset time. Offset time is defined as the time between the data burst and the header to compensate the configuring delay. At the intermediate OBS node the control packet undergoes O/E/O conversion. OBS is a two way reservation scheme. In this reservatin scheme header is sent prior to the packet to reserve the resoureces.After a certain offset time the data burst is sent. Resources are allocated without explicit two-way end to- end signalling, instead so-called one-pass reservation is applied. Bursts may have variable sizes. Buffering is not required in Burst switching. Burst assembly function can be used to reduce the self-similarity traffic. Good quality is guaranteed if the burst network relies on limited congestion and small buffers.

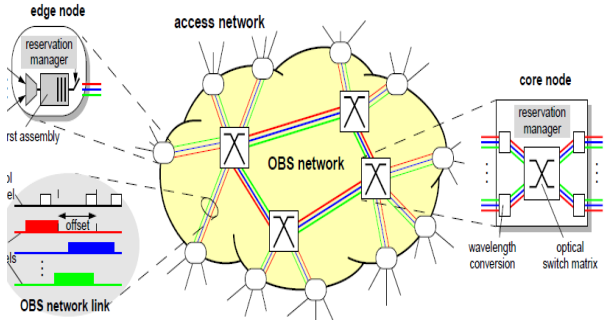

Figure 1: Node and network architecture for optical burst switching

II. BURST INTERGRITY

Burst integrity is referred as validation of the burst. The information transferred from the ingress node must reach the egress node without any modification or change in the burst content. This is a challenging problem in optical domain. OBS networks show great promise in providing cost effective interconnection solutions to the ever growing Internet. However, OBS network is not free of security concerns.

ISSN: 2278 – 909X

III. SECURITY VULNERABILITIES IN OBS NETWORKS

The need to bring security measures to OBS networks is considered to be very important. The different types of attacks and security vulnerabilities are addressed here:

A. Orphan Bursts

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 set up for the arriving burst. Since the burst has been launched, it is going to arrive at the input of the core router in any case. At this point, the burst is no longer connected with its header and becomes an orphan burst. As a result, orphan data bursts can be tapped off by some undesirable party, compromising its security.

B. Redirection of Data Bursts

The one-to-one correspondence between the burst header and its associated burst is implied by the offset time carried in the burst header. Such one-to-one correspondence can be violated by injecting a malicious header corresponding to the same burst. As a result, the route and the destination for the burst can be altered by the malicious header, even though a legitimate path has been set up by the authentic header.

C. BCH flooding attack

If any optical node is compromised by intruders and using that node, creates multiple copies of the same burst header and advances it to the next node and thereby flooding the next intermediate node with the duplicate copies of the original burst control header. So the next intermediate node tries to make reservations for these fake burst control headers. Hence overflow of buffers will happen at the intermediate core node or if the wavelength conversion is implemented then this bogus burst control header reserves different wavelength for its respective data burst. Thus the uncompromised nodes will not able to reserve the resource if it receives a valid burst header. This attack is called as Burst header flooding attack.

D. Replay

Replay attack can be launched by capturing a legitimate but expired burst and transmitting at a later time, or by injecting a expired burst header to cause the optical burst to circulate in the OBS network, delaying its delivery to the final destination.

E. Land Attack

A virtual source code is those that redirect the incoming burst and multiples their destination to any wavelength. Thus under this attack the malicious header modifies the intended address and redirects them to the source node resulting in the data burst making a round trip and reach both the intended delivery address as well the source node wasting the resources of the network.

F. Malicious burst header injection

The data burst simply follows the optical path and does not possess any idea on routing the information to their intended destination in the OBS network. Hence as the burst header is set on a schedule and enters the network is lost to the unauthorized or illegitimate address. This is mainly due to the lack of absence of authenticating authority in the network. This type of attack is called as malicious burst header injection.

G. Circulating Burst Header Attack

This is a type of attack where in two or more compromised nodes are pulled together to form an attack on the OBS network. They flow in an already circuited path slowing down the delivery of the Data burst to its destination. Under this one comprised node acts like a master controlling the rest in the predetermined circuit and forwards the burst control header to the intended recipient. This results in wastage of resources and also in blockage and unnecessary delay on data burst.

H. Denial of Service

More input generations than the node can process. This attack is described in the next chapter. A DDoS flooding attack is an attack that attempts to make a failure in a network by giving more inputs than the network nodes can process properly.

IV. BURST INTERGRITY ALGORITHM

The cryptography system provides secrecy, or confidentiality, but not integrity. However, there are occasions where we may not even need secrecy but instead must have integrity. One way to preserve the integrity of a document is through the use of fingerprint. To ensure that the original content is not changed, fingerprints can be used at the bottom of the document. For this purpose hashing technique can be introduced. A hash function maps the bit strings of arbitrary length to bit strings of fixed length. The desirable properties of hash techniques are easy to calculate, seemingly random output and the irreversibility.

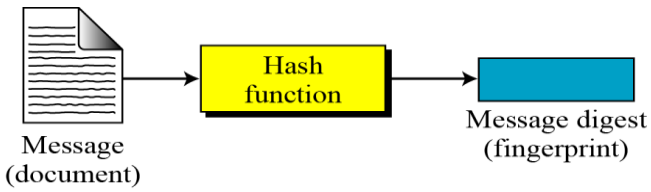

Figure 2: Message and digest

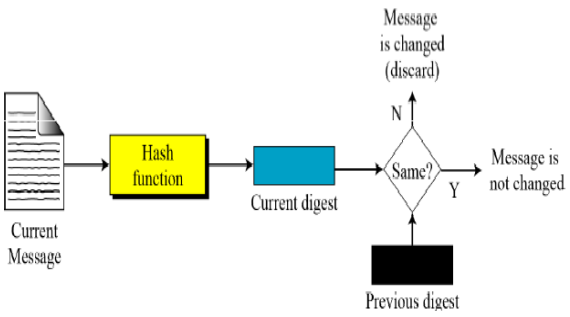

Figure 3: Checking integrity

In order to perform this hashing technique, the electronic equivalent of the document and the fingerprint are taken. The electronic equivalent of the document and the message are

ISSN: 2278 – 909X

referred to as message and message digest respectively which is shown in figure 2. This pair can therefore be termed as message digest pair. Though the two pairs found to be similar they are distinguished by certain features. The integrity of the document can be checked by combining the current document with the hash functions. The current document along with the hash functions produces the current digest. This current digest is then compared with the previous digest which is shown in figure 3.If the message is not changed after comparison then it can be concluded that integrity is maintained.

In general the cryptographic hash function must satisfy three essential criteria's:

1. Preimage Resistance.
2. Second preimage resistance.
3. Collision resistance.

1. *Preimage Resistance*

In the Preimage resistance for a given the message digest y, the problem of preimage compression is the computation of x such that y= h(x). A function for which the preimage problem cannot be efficiently solved is called as one way function or preimage resistance function which is shown in figure 4.

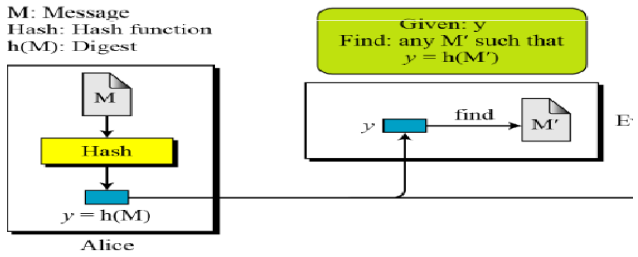

Figure 4:Preimage resistance

2. *Second Preimage Resistance*

Second preimage resistance for the given message x, the problem of second preimage compression is the computation of x' such that h(x') = h(x). A hash function for which the second preimage compression cannot be efficiently done is called as second preimage resistance which is shown in figure 5.

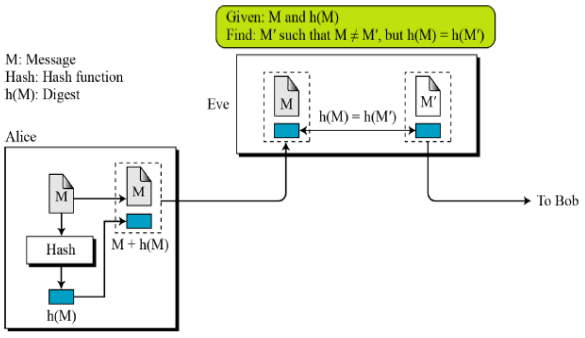

Figure 5:Second preimage technique

3. *Collision Resistance*

The problem of collision is the computation of a pair of x and x', which are equal such that h(x')= h(x). If such a valued pair is found collision is detected. A hash function for which the collision problem cannot be efficiently solved is called collision resistance which is shown in figure 6.

The hashing cryptographic function can provide only integrity but not availability or confidentiality. Since this paper is mainly dealt about the integrity the remaining concepts are not considered. The message digest does not authenticate the sender of the burst. To provide message/burst authentication one has to prove one's identity which is practically impossible. The two groups of hash functions created by compression functions are Message Detection Code (MDC) and secure hash Algorithm (SHA).The digest created by the cryptographic hash function is called Message Detection Code (MDC).MDC is a message digest which can prove the integrity of a message. If a burst has to be sent from the ingress node to egress node, the respective burst should not be changed during transmission. For this the ingress node must create a message digest and message detection code(MDC).Now the egress node has to create a new MDC from the message and compare the received MDC and new MDC.If they are same then the message has not be changed. The versions of message digest algorithm are MD2, MD4and MD5.

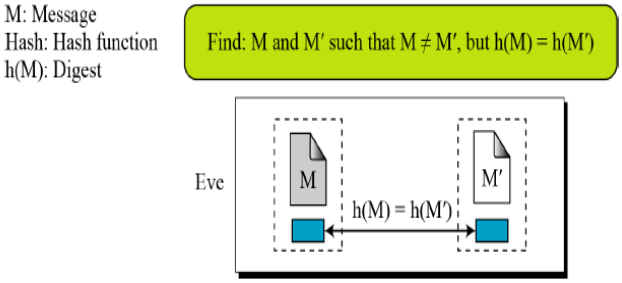

Figure 6: Collision resistance

MD2 is a message-digest algorithm. They are meant for digital signature applications. Here a large message has to be compressed in a very secure manner before they are being processed with the private key. The input is any burst of arbitrary length and the output will be a 128bit message digest. Thought these algorithmic structures are found to be similar, the design analysis of MD2 is different from that of MD4 and MD5.MD2 is very much optimal for 8-bit machines, but MD4 and MD5 algorithms are optimized for 32-bit machines. MD4 is a hash algorithm (the four in series). The hash has a length of 128 bits. Similarly MD5 is also a message-digest algorithm that takes the input burst of any arbitrary length and produces burst of fixed length. The MD5 algorithm is very much applicable and defined for digital signature applications. Here also a very large content has to be compressed in a secure way before they are used for further processing. Comparing to other digest algorithms, MD5 is simple to implement, and provides an output burst of any arbitrary length. It performs very fast on 32-bit machine.MD5 is considered one of the most efficient algorithms currently available.

Similarly the versions of secure hash algorithm are SHA-1, SHA-2.The performance of SHA is more secured

ISSN: 2278 – 909X

when compared with SHA. Though **SHA-1** is analysed and carved only after MD4, it creates a hash which has a length of 160 bits instead of 128 bits.**SHA-2**is classified into four different types, known as SHA-224, SHA-256, SHA-384, and SHA-512 which is shown in Table 1.

When SHA-512 is compared with other types of SHA algorithm it proves to be better in certain aspects.SHA-512 algorithm has a maximum message size of2^{218}-1.Thought SHA-384 exhibits the same maximum message size the message digest size is highly varied in SHA-512.This makes SHA-512 more better and suitable for comparison. The block size of SHA-512 is 1024 and found to have a higher rate when compared to other versions. From this table the different versions of SHA is compared and found that SHA-512 is advantageous in all aspects.

Table1: Comparison of Different SHA algorithm

Characteristics	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Maximum Message Size	2^{64}-1	2^{64}-1	2^{64}-1	2^{128}-1	2^{128}-1
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80

V. CONCLUSION

From the above table and from the analysis of different algorithm types it clearly depicts that SHA-512 algorithm produces better results for burst integrity, when compared with other algorithms. Since this paper mainly concentrates only on burst integrity SHA-512 algorithm advantages is mainly taken into account.

VI.ACKNOWLEDGEMENT

Our sincere thanks to Mr. Jerome Melkisidak, Managing director of Stigmata Techno Solutions to complete this paper.

REFERENCES

[1] Chlamtac. I, Ganz. A, Karmi. G, , Lightpath communications: An approach to high bandwidth optical WAN's, Communications,IEEE Transactions on July 1992, pp.1171 - 1182

[2] Qiao, C. Yoo, M.: Optical burst switching (OBS) – A new paradigm for an optical internet. Journal of High Speed Networks, No. 8, January 1999, pp. 69-84.

[3] A.M.Balamurugan, Dr.A.Sivasubramanian, Optical burst switching issues and its features, International journal of Emerging Trends & Technology in computer science, Volume 2, Issue 3, May-June 2013, pp-306-315.

[4] Christoph Gauger, Klaus Dolzer, Jan Späth, Stefan Bodamer, Service Differentiation in Optical Burst Switching Networks**,** *Photonic Networks*, March 12-13, 2001

[5] Yuhua Chen, Pramode K. Verma and Subhash Kak, Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks, Security and Communication Networks. 2009

[6] Sreenath. N, Muthuraj. K, Vinoth. G, Threats and Vulnerabilities on TCP/OBS networks, Computer Communication and Informatics (ICCCI), 2012 International Conference on January 2012, pp 1 – 5.

[7] A.M. Balamurugan and A. Sivasubramanian, "Quantum Key Based Burst Confidentiality in Optical Burst Switched Networks," The Scientific World Journal, vol. 2014, Article ID 786493, 7 pages, 2014. doi:10.1155/2014/786493

[8] Ragab.A.H.M, Ismail.N.A, "An efficient message digest algorithm (MD) for data security", in TENCON 2001. *Proceedings of IEEE* International Conference on Electrical and Electronic Technology (Volume:1),pp191 - 197vol.1.

[9] Karimi, R., Qazvin, Iran ; Kalantari, M.,:Enhancing "Security and confidentiality in location-based data encryption algorithms",,*IEEE Transactions* on August 2011.pp.30-38.

[10] Zhiliang Zhu ; Ke Zhai ; Beilei Wang ; Hongjuan Liu, Research on "Chaos-Based Message Digest Method for Medical Image and Signal Processing",in *IEEE transaction* 2009. CISP '09. 2nd International Congress,pp1-5.

[11] Chu-Hsing Lin,Chen-Yu Lee ; Yi-Shiung Yeh ; Hung-Sheng C, 'Generalized secure hash algorithm: SHA-X", in *EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE*,pp1-4.

[12] Kitsos, P.Sklavos, N., "On the hardware implementation efficiency of SHA-3 candidates", in Electronics, Circuits, and Systems (ICECS), 2010 17th *IEEEInternational Conference*,pp-1440-1443.

AUTHOR

A.M.Balamurugan is a Research Scholar and pursuing a Doctoral Degree in Information & Communication Engineering at the Department of Electronics and Communication Engineering at Anna University, Chennai – 600025, India. He received his B.E in Electronics and Communication Engineering (2002) from Madurai Kamaraj University, Madurai, Tamilnadu, India. He received his M.E in Digital Communication and Network Engineering (2005) from Anna University, Chennai, Tamilnadu. He has 10 years of experience in teaching and guiding projects for undergraduate and postgraduate students. His research areas are Optical networks and Optical Communication.

V.Chandana PG Research Scholar, pursuing her master's Degree in applied electronic in the department of Electronic & Communication engineering at St. Joseph's college of

ISSN: 2278 – 909X

engineering, Chennai, India. Received her B.E in ECE engineering (2012) from SMK Forma institute of technology, Chennai, Tamilnadu, India. Her research areas are Optical Network and Optical Communication.

Dr.A.Sivasubramanian has received B.E. degree in ECE from University of Madras in 1990, and M.E. in Applied Electronics from Bharathiar University in 1995 and Ph.D. degree in Optical Comm. from Anna University Chennai in 2008. Currently he is working as a Prof & Head, in the department of Electronics and communication engineering at St.Joseph's College of Engineering, Chennai, India. He has 20 years of experience in teaching and guiding projects for undergraduate and postgraduate students. He has added ten international and national publications to his credit. He is a recognized supervisor for the doctoral degree programme at Anna University Chennai and Sathyabama University, Chennai. His areas of interests include optical communication, optical networks, Bio-optical Engineering, Wireless sensor and computer networks. He is a member of ISTE, IETE, IEEE, and OSA.

ISSN: 2278 – 909X