IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 4, Issue 6 (Jan. - Feb. 2013), PP 01-08
www.iosrjournals.org

Surveillance on Manycasting Over Optical Burst Switching (OBS) Networks under Secure Sparse Regeneration

C.Veera lakshmi[1], V.Kavitha[2]
[1](*Second M.E.Communication Systems, M. Kumarasamy College of Engineering, Karur, India)*
[2](*Professor/HOD Dept of ECE, M. Kumarasamy College of Engineering, Karur, India)*

Abstract : *In wavelength-routed WDM optical networks requires regeneration for few light paths, when the strength of optical signal reduced and also security and privacy are essential before Optical Burst Switching (OBS) networks can become an everyday reality. Manycasting is a communication paradigm to implement the distributed applications. In manycasting, destinations can join or exit the group, depending on the service requirements imposed on them. This dynamic movement of the destinations in the group decreases blocking effect. Each application requires its own QoS threshold attributes like physical layer properties, delay as a result of transmission and reliability of the link. If the destinations satisfy the required QoS constraints set up by the application, then only they will qualify. There are two algorithms MCM-SPT and MCM-DM required for manycasting to resolve the multiconstraint QoS drawback. For continuous burst transmission lightpath should be regenerated before it loses the information due to lack of signal strength. To recover signal strength by sparse regeneration, where OOO switches are replaced by OEO swtches. There are three algorithms 1).NDF 2).CNF 3).SQP. Sometimes, there is an opportunity for the attacker to join the group. Service provided to the attacker is restricted by providing two levels of security. Using1).RSA algorithms, data level security is provided and using 2).certificate authentication, link level security is provided.*

Keywords: *Certificate generation, Manycasting, Optical Burst Switching Networks (OBS), Sparse regeneration, Quality of Service (QoS).*

I. Introduction

Information Security has become an important issue in data communication. Encryption plays a vital role in information authentication system. This authentication mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. Different types of algorithms are used to prevent malicious attack when the time of data transmission. Encryption algorithm can be divided into symmetric key (private) and asymmetric (public) key Encryption [1]. In Symmetric keys encryption or secret key encryption, the data is encrypted or decrypted using only one key. In Asymmetric keys, two keys such as private and public keys are used. Encryption is done by Public key and decryption is done by Private Key (example: RSA).

When the time of signal degradation due to long distance (>4000 km), attacker can easily hack the information. To avoid this dangerous situation at continuous wavelength routed WDM network, Sparse Regeneration is necessary. It is a technique where the light path is routed using Optical switches (OOO switches). The light path which carries the information loses its strength due to physical limitation of distance. Instead of OOO switches, OEO switches can be replaced in the network to regenerate the signal strength. The transparent optical network can be converted into opaque optical network which uses 3R (reamplification, reshaping, retiming) regeneration method at every intermediate node of a lightpath to regenerate the signal and improve transmission quality... In such a network, a lightpath can be successfully routed if and only if: 1) common wavelength should be there on each link and 2) before regeneration at an OEO switch,) the lightpath should not exceed the reach limit. Manycasting will be secured because of this protection along the information packaged at burst.

Manycast is also called *quorumcast* and was first proposed by [2] in which the groups of destinations that receive the message are to be selected instead of being given. In manycasting messages are sent to a subset of destinations (quorum pool), which are selected from set $D_{s,}$ such that $k \leq |D_s| = m$. Manycasting has caught the attention of several researchers during the recent past, due to the emergence of many distributed applications such as distributed interactive simulations (DIS), Video conference, storage area network (SAN) and grid computing.

Optical Burst Switching (OBS) [3–8] has emerged as a promising solution for satisfying the increased capacity demands of modern broadband networks. In OBS systems, the various types of data carried in the network (e.g., IP packets, ATM cells, frame relay frames, and so forth) are electronically buffered at the ingress node, aggregated into bursts, and then transmitted all-optically through the core network as a single burst. Upon arrival at the egress node, the burst is disassembled and the individual data packets are then forwarded to the appropriate destinations.

In this paper we propose two levels of security using RSA and Certificate Authentication for restricting burst to reach attacker and consider three algorithms for regenerating the signal strength. The rest of the paper is organized as follows: we first discuss about the existing system in Section II, proposed system in Section III, Section IV discusses performance evaluation of the proposed algorithms and explain the throughput and delay constraint of existing algorithms. Finally, conclusion is given by Section V in this paper.

1.1. Existing System

Existing work focuses on selecting the best possible destinations that can meet the service demand must effectively. Destinations chosen are able to provide quality of service attributes. If a destination satisfies the service requirements of the application, it will qualify as the member of quorum pool. Algorithms implemented in the centralized way, may fail due to a link failure and resulting in poor performance due to insufficient security and lack of information due to signal strength.

(s, D_s, k) is the manycast request where s is the source node, D_s is the destination set and k is the minimum number of destinations that are required to participate in the manycast session. Path information vector Ω is generated according to the service attributes such as Noise factor η_j, Reliability γ_j, Propagation delay $\tau_{j.}$ for link j,

$$\Omega_j = \begin{pmatrix} \eta_j \\ \gamma_j \\ \tau_j \end{pmatrix} \qquad (1)$$

For the successful establishment of QoS-based manycast session, the chosen destinations must satisfy the service requirements T ($^{\theta}{}_{P}$) that is given by,

$$\top^{(\theta_p)} = \begin{pmatrix} \eta_{\max}^{(\theta_p)} \\ \gamma_{\min}^{(\theta_p)} \\ \tau_{\max}^{(\theta_p)} \end{pmatrix} \qquad (2)$$

This system proposed two algorithms, MCM-shortest path tree (MCM-SPT) and MCM dynamic membership (MCM-DM) for evaluating the performance of manycasting with QoS constraints. Common steps involved in these algorithms,

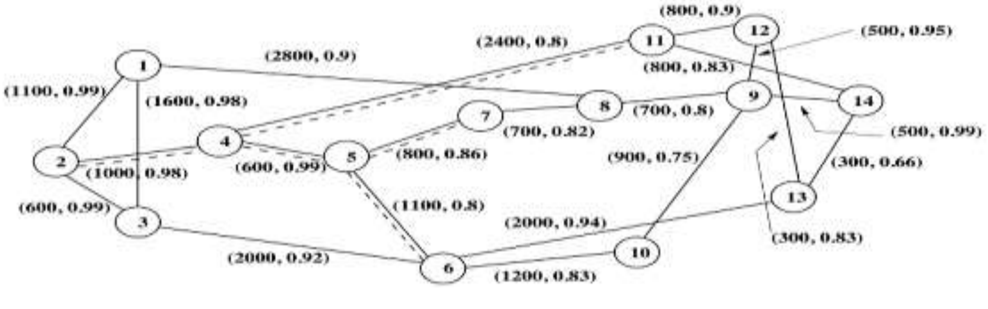

Fig.1: NSF topologies with 14 nodes. The weight represents distance (km) and corresponding reliability.

Step 1: Search the shortest path from source to all the destinations in D_S

Step 2: All the destinations in D_S are sorted in the non decreasing order according to the shortest distance from source to the destinations. Let D_S' be the new set.

Step 3: Choose the first K destinations from D_S'.

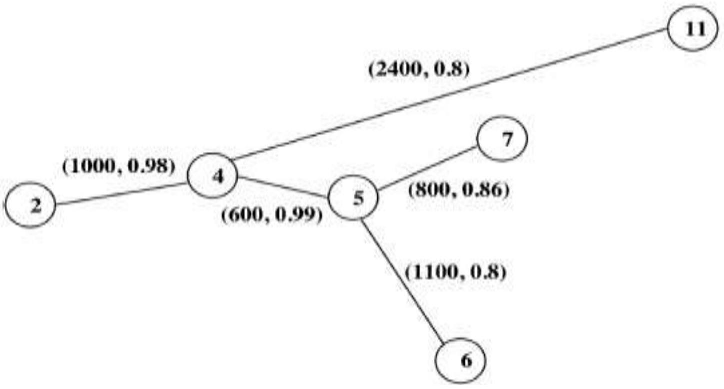

Fig.2: Illustrative example topology from Fig.1 which is represented as dotted line

In Fig.2.Consider a manycast request (s =2, D_s= {6, 7, 8}, k_0 = 2). Let the service threshold be T ($^{0}{}_{P}$) = [η_{th} = 6, γ_{th} = 0.6, τ_{th} = 20 ms].Then the above steps are followed. If the services are satisfied correct destinations will be found else QoS blocking will be occurred for MCM-SPT Algorithm. For MCM-DM Dynamically it calculates the destination as per the constraint they required. If it not possible QoS blocking will be occurred.

II. Proposed System

Proposed work focuses on regenerating the signal strength for lossless data communication and providing authentication for burst to reach the correct destination and protecting burst from attacker. Disadvantage of manycasting is the attacker can join into the group easily by act as a destination which satisfies the QoS service requirement and the signal degradation at long distances... To avoid this situation proposed work guaranteed two level of security such as Data level security using RSA algorithm and Link level security using Certificate authentication .Regenerating will be happened by choosing three algorithms such as 1).NDF (Nodal Degree First) 2).CNF (Centered Node First) 3).SQP (Signal Quality Prediction).

2.1. Data Level Security using RSA Algorithm

Data Security means protecting a database from destructive forces and the unwanted actions of unauthorized users. For this purpose we choose asymmetric key cryptography to provide efficient security. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) Supports Encryption and Digital Signatures. *Factorization* is a major problem when using RSA. The basis of security in RSA is difficulty of large number factorization Long numbers contains over the 1000 bits.

The RSA algorithm [11-13], [16] is based on the mathematical part that is easy to find two large prime numbers and multiple together, but factoring their product will be difficult. There are some important steps are involved in a RSA algorithm to solve a problem as given below:

Step 1: Assume two large prime numbers x & y.

Step 2: Compute: N = x*y Where N is the factor of two large prime number.

Step 3: Select an Encryption key (E) such that it is not a factor of (x-1)*(y-1) i.e. Ø (n) = (x-1)*(y-1) for calculating encryption exponents E, should be 1< E Ø (n) such that gcd (E, Ø (n) =1 The main purpose of calculating gcd is that E & Ø(n) should be relative prime Euler Totient Function is represented here is Ø (n) & E is the Encryption Key.

Step 4: Select the Decryption key (D), which satisfy the Equation D*E mod (p-1)*(q-1) = 1

Step 5: For Encryption:

Cipher Text= (Plain Text) E mod N (or)

CT=ME mod N

Step 6: For Decryption:

Plain Text= (Cipher Text) E mod N (or)

PT= (CT) E mod N

The main feature of RSA algorithm is the selection of large prime number (x, y) because any users or force attackers could not be able to find the capable numbers, timely to force attack is shortly non-feasible. Security will be provided by RSA depends on some parameters and its selection method.

1. Selection of large prime number(x, y):

Example: x = 5, y = 3 N= x*y = 5*3 = 15 = 1*15 = 15*1 = 3*5 = 5*

2. Selection of Encryption Key (E): During the selection Of Encryption key, selection of large prime fraction always creates impact. If the factor is high then the estimation of Encryption is infeasible.

Example: If x=7, y=17 must not be a factor of (x-1) *(y- 1) i.e. (7-1)*(17-1) = 6*16 = 96 = 2*2*2*2*2*3 So, E can be 5, 7, 11…

3. Selection of Decryption Key (D): Selection of large factors always create an effect on the Decryption key, there may be an inversely relation.

$$(E*D) \bmod (x-1)*(y-1) = 1$$

$$D \propto 1/ [(E)\ (x)\ (y)]$$

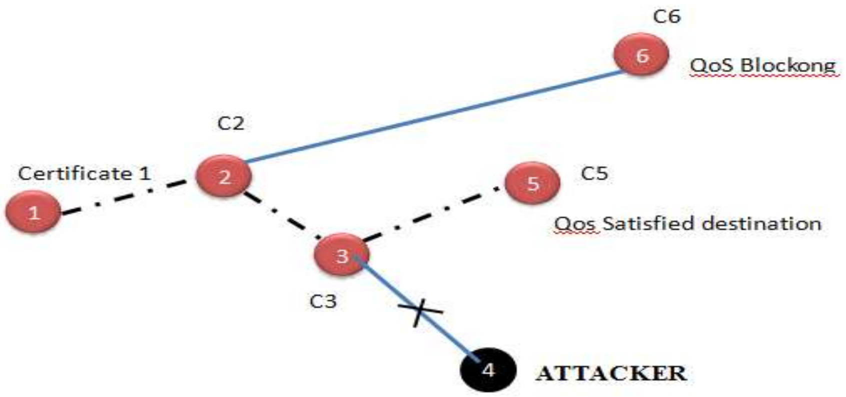

Fig.3: Restriction of attacker node by using combination of RSA and certificate authentication.

Some important points for reference are given below:

- Condition of Euler's Totient Function:
  1. Ø (1) = 0
  2. Ø (x) = x – 1 {if x is prime number}
  3. Ø (m*n) = Ø (m)* Ø (n) {if m and n is relative prime number
  4. Ø (Xe) = Xe – xe -1 {if x is a prime number}
- There is no necessity for a user to know his secret parameters x, y and Ø (n).
- The plain text or message (M) has the form of one or more positive integer M<N.
- Any user can use his private key to authenticate the communication.

RSA cryptosystem provides the facility of digital signature scheme. The message consists of letters, numbers and special characters (i.e. stop, colon, space etc.). Each character is represented by its own arrangement of Eight bits (o & 1). The most of the hardware & software products and standards that use public key technique for Encryption, Decryption etc. are based on RSA cryptosystem. There are some advantages of RSA Algorithm:

- Important benefits of Public key Cryptography is increased security and convinces.
- Second, it provides digital signature that can't be repudiated. For example, Kerberos secret-key authentication system involves central database that keeps copies of secret key.
- Public key authentication prevents the type of repudiation and each user has its own responsibility for protecting his own private key.
- We can select large prime numbers for enhancement of security of keys.
- Public key cryptography may be used with secret key cryptography.

2.2. Link Level Security using Certificate Authentication

Link encryption (sometimes called *link level* or *link layer encryption*) is the data security process of encrypting information at the data link level as it is transmitted between two points within a network. Link encryption takes place in the lowest protocol layers (layers 1 and 2 in the OSI model). because the process protects the message in transit. Link encryption is very useful in situations where the uncertainty of security. Dangerous issues can occur at a link when the message must be transmitted between hosts, the message is decrypted at each host in the transmission path, which are not known to be secure. Link encryption has been used successfully in military, where the assurance of security is provided for each link. It isn't work over the Internet, because intermediate links are neither accessible nor secure.

This can be done using certificate authentication. The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates [14]. A certificate is a digital document (DN) and an associated public key. The certificate is signed digitally by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate consumer. Each principal in the transaction presents a certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider .Commonly the certificate consists of source address, destination address, MAC address, public and private key.

Example: Certificate of Node 0

IP address	- 190.06.30.8
MAC address	- 25EFDHY5898
Public key	- 3
Private Key	- 3

2.3. Sparse Regeneration

Next generation optical networks are expected to be combination of all optical-Cross Connects (OXC) and OEO cross connects. In core network OEO cross connects are used for wavelength conversion and regeneration. Sometimes for long distance communication (>4000 km), light path needs to regenerate its strength for avoiding data loss. This problem is known as Sparse OEO Placement (SOEOP) problem [17].

A light path is a travelling path of light between two OXC's to carry the information. A typical light path is given by Fig.4. When the Optical Signal to Noise Ratio (OSNR) will be reduced, at that time regeneration will be needed. OEO OXC used for regenerating the signal strength.

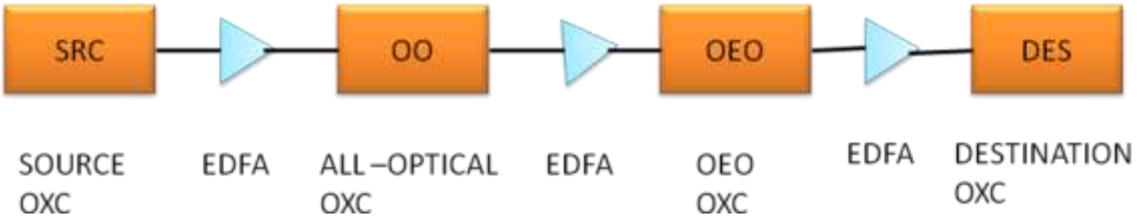

Fig.4: Light path from Transmission perspective

2.3.1. Sparse Regeneration Node Model

The 3R OEO regeneration can be performed by 3R OEO regenerator as shown in Fig.5.It consists of T-R pair with electronic processing to regenerate the optical signal through 3R processing [18]. The Sparse regeneration node model is given by Fig.6.

The wavelengths on incoming fiber links are demultiplexed at each node at OXC module. A node can add/drop the wavelength when it is needed. The regeneration capable node will be detected in the arrays of transmitter and receiver pair. At regeneration capable node, the regeneration demand is happened by the light path for say λ_1. It directs the light path for the available receiver in $R_{R.}$ Then it converts optical signal into electrical signal using O/E conversion .Electrical signal is processed by 3R regenerator. After regenerating, it is converted into optical signal through E/O converter at corresponding T_R as a wavelength λ_2.This regenerated optical signal is transmit through output fiber link.

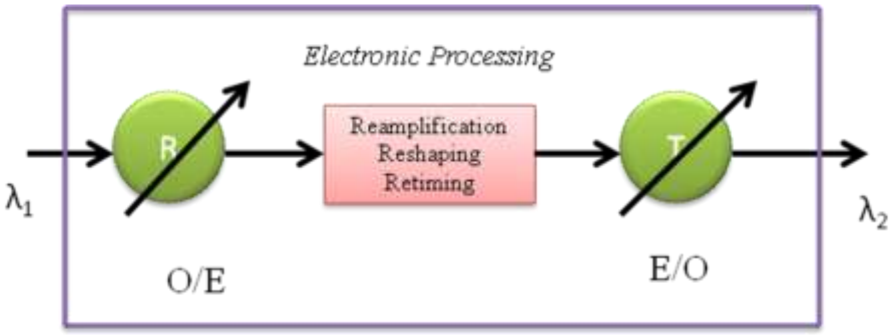

Fig.5:3R OEO Regenerator

There are three algorithms to regenerating the optical signal with high OSNR and high signal quality.

- **Nodal Degree First (NDF)**
- **Centered Node First (CNF)**
- **Signal Quality Prediction (SQP)**

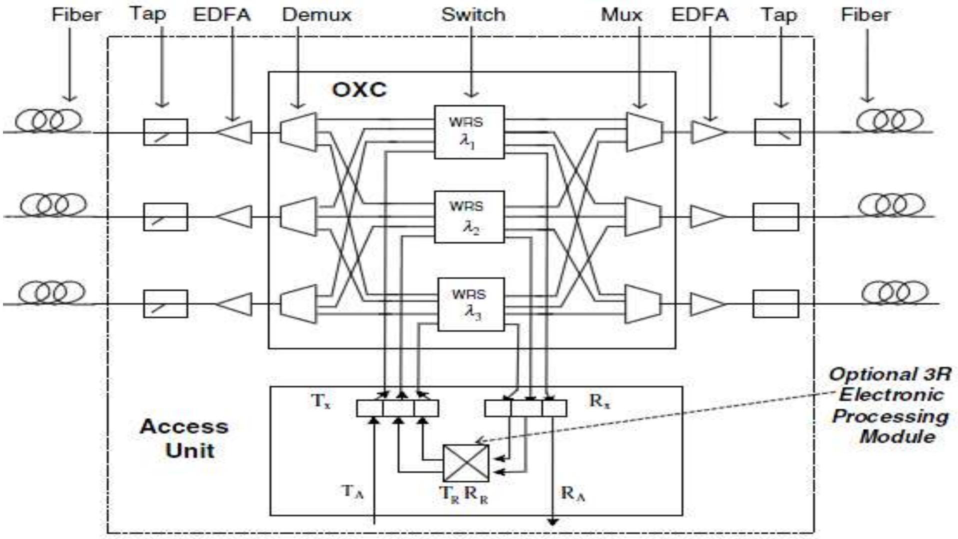

Fig.6: Sparse Regeneration Node

*3.3.2 **Explanation of Algorithms***

Algorithm 1. Nodal Degree First (NDF) regenerated placement.

Step 1: Specify each node by number equal to nodal degree.

Step 2: Choose a node with high regenerated capability. If more nodes exist choose randomly one node regenerator node and then reduce the degree by 1.

Step 3: Repeat the step until N groups of regenerators are placed.

Algorithm 2. Centered Node First (CNF) regenerator placement

Step 1: Specify large number for center node .The nodes equally centered are assigned number in random order.

Step 2: Choose N nodes as a regenerator nodes and place regenerators at each node.

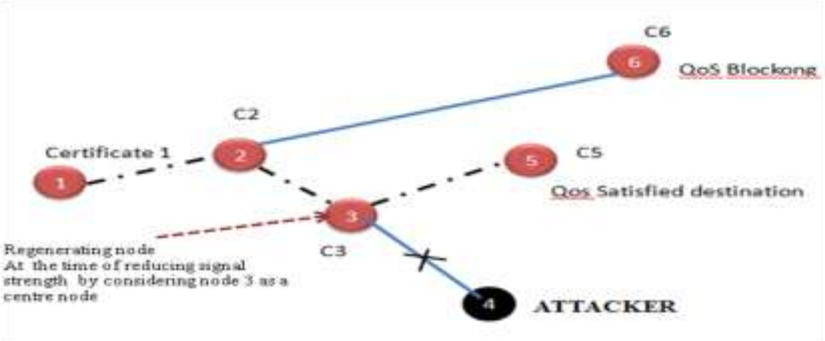
C6
6
QoS Blockong
C2
2
Certificate 1
1
5
C5
Qos Satisfied destination
3
C3
Regenerating node
At the time of reducing signal strength by considering node 3 as a centre node
4
ATTACKER

Fig.7: Using CNF regenerator placement (Node 3)

Algorithm 3. Signal Quality Prediction (SQP) based regenerator placement

Step 1: Specify each node j by number Cj, initialized to be zero.

Step 2: Workout a predefined wavelength routing algorithm on lightpaths demands which are randomly generated by following a predicted traffic pattern.

Step 3: Arrange all nodes in non-increasing order of Ci.

Step 4: Choose the first N nodes as regeneration capable nodes and place regenerators at each node.

Table 1: Comparison of Regeneration algorithms

Features	**NDF**	**CNF**	**SQP**
Blocking Probability	Moderate	High	Low
Loss of data	Moderate	High	No loss
Reachability of regenerated signal quality	Moderate	Very low	High

III. Performance Evaluation

These two authentication algorithms provides efficient security, when it finds the node is attacker at that time instantly it mark the node is attacker and the burst transmission for that node will be restricted. The certificate is not generated for that particular node. Fig.8. Describes which node is attacker and it is denoted as 0.Certificate generated nodes are denoted as 1. The comparison result of parameters such as throughput and delay also taken between MCM-SPT and MCM- DM as shown in Fig.9 and Fig.10. This simulation results show that MCM-shortest path tree (MCM-SPT) algorithm performs better than MCM-dynamic membership (MCM-DM) for delay constrained services and real time service, where as data services can be better provisioned using MCM-DM algorithm.

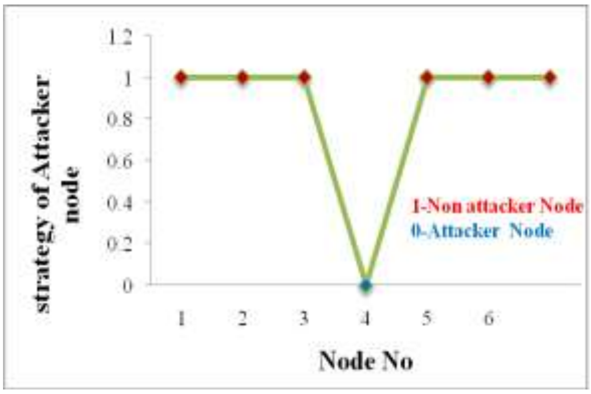

Fig.8: Certificate generation strategy of nodes

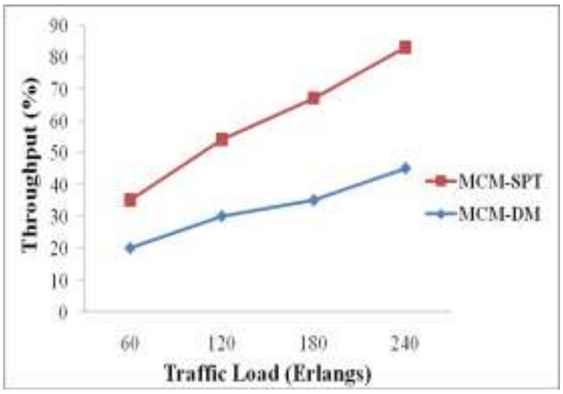

Fig.9: Traffic Load Vs Throughput

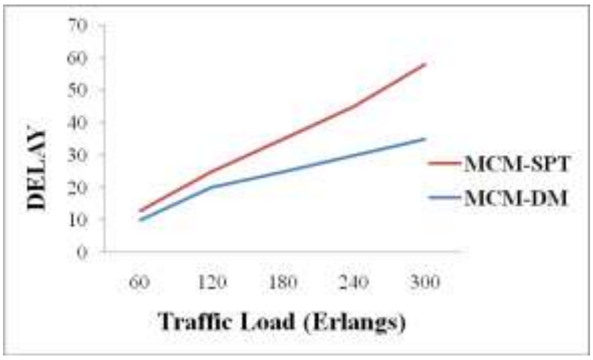

Fig.10: Traffic Load Vs Delay

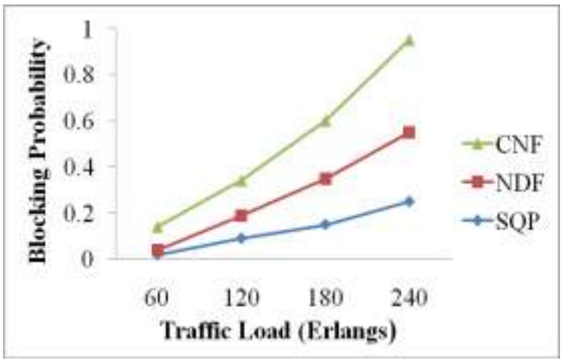

Fig.11: Traffic Load Vs Blocking Probability

One of the important features of the Sparse regeneration is the blocking probability as shown in Fig.11. it will be highest when using CNF algorithm because of choosing center node for placing regenerator. If the distance between center and Tr/Rr node is large, it will loss on the way, even it regenerate the signal. This difficulty is overcoming by NDF and SQP.

IV. Conclusion

In this paper, algorithms are proposed to support authentication and regeneration purpose in QoS constraint manycasting over Optical Burst Switching (OBS) networks. RSA and Certificate generation based cryptography supports source to fine the attacker by generating certificate with the help of public and private key, which are generated by RSA algorithm. Simulation results that multiconstrained manycast dynamic membership algorithm is suited for data service because it provides higher throughput and multiconstrained manycast shortest path tree algorithm for real-time service because it provides lower delay. NDF,CNF and SQP algorithms are used for regenerating the optical signal when the OSNR is decreased. The simulation result of Sparse regeneration said that blocking probability is higher than remaining both algorithms. We also evaluated the performance of our algorithms by strategies of attacker nodes, if it is attacker, the node doesn’t generate certificate (0).Our work can be further extended by considering the manycastiing over Optical Burst Chain Switching (OBCS) networks with sparse wavelength regeneration.

Acknowledgements

Our sincere thanks to Professor V. Kavitha M.E., (Ph.D)., Head of the Department of Electronics and Communication Engineering, M.kumarasamy College of Engineering, Karur, who have contributed towards development of work. Also the author would like to thank reviewers for their valuable comments to improve the quality of the paper.

REFERENCES

[1] Diaasalama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud , Evalution of the Performance of Symmetric Encryption Algorithms, *International journal of network security,vol. 10, No.3, pp, 216-222, May 201.*

[2] B. G. Balagangadhar, *QoS Aware Quorumcasting Over Optical Burst Switched Networks*, doctoral diss., Indian Institute of Science, Bangalore, India, Electrical and Communication Engineering July 2008.

[3] Chen.Y, Qiao. C, Yu and X, Optical burst switching a new area in optical networking research, *IEEE Netw.* 18, 16– 23, 2004.

[4] Qiao. C, Labeled optical burst switching for IP-over -WDM integration, *IEEE Commun. Mag.* 38(9), 104–114 (2000).

[5] Qiao, C, Yoo.M, Optical Burst Switching (OBS) — A new Paradigm for an optical internet, *J. High Speed Netw.* 8(1), 69–84, 1999.

[6] Turner.J, Terabit burst switching High Speed, *J. High Speed Netw* 8(1), 3–16, (1999).

[7] Yoo, M. Qiao, C, Dixit. S,Optical Burst switching for Service Differentiation in the next - generation optical internet, *IEEE Commun. Mag.* 39(2), 98–104, 2001.

[8] X. Huang, Q. She, V. M.Vokkarane and J. P. Jue, Manycasting over optical burst - switched (OBS) networks, *Proc. IEEE ICC, Glasgow,* Scotland, May 2007, pp. 2353–2358.

[9] A. Kaheel, T. Khattab A. Mohamed and H. Alnuweiri, Quality - of service Mechanismsin IP –over networks, *IEEE Commun. Mag. vol. 40, no. 12, pp. 38–43, Dec. 2002.*

[10] B. G. Bathula, V. M. Vokkarane and R. R. C. Bikram, Impairment aware manycasting over optical Burst - switched (OBS) networks, *Proc. IEEE ICC,* Bejing, China, May 2008, pp. 5234–5238.

[11] Anoop MS, Public key Cryptography (Applications Algorithm and Mathematical Explanations), Tata Elxsi Ltd, India.

[12] Andrea Pellegrini, Valeria Bertacco, Todd Austin, Fault-Based attack of RSA authentication, *University of Michigan.*

[13] Shashi Mehrotra Seth, Rajan Mishra, Comparative Analysis of Encryption Algorithms for Data Communication, *IJCST Vol. 2, Issue 2,* June 2011.

[14] Jim DeRoest, Certificate- Based Authentication, Published *on SunExpert Magazine,* June 1997.

[15] M.Catherine Jenifer, P.Jayachandar "Cryptanalysis on RSA algorithm" *Published on, International Journal of Communications and Engineering Volume 03– No.3, Issue 01* March2012.

[16] Prasant Singh Yadav, Pankaj Sharma ,Dr. K. P Yadav , Implementation of RSA algorithm using Elliptic curve algorithm for security and performance enhancement, *International Journal of Scientific & Technology Research Vol 1, Issue 4*, May 2012.

[17] Hui Zang, Renxiang Huang and James Pan, Methodologies on Designing a Hybrid Shared- Mesh Protected WDM Network with Sparse Wavelength Conversion and Regeneration, *Proceedings of SPIE Vol. 4910,*2002.

[18] Xi Yangz, Byrav Ramamurthy, Sparse Regeneration in Translucent Wavelength- Routed Optical Networks Architecture, Network Design and Wavelength Routing"*Journal of Photonic Network Communications 10:1, 39–53,* 2005.