Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks

MOHAMMED AL-MOMIN, JOHN COSMAS, SAMAN AMIN
School of Engineering and Design
Brunel University
Uxbridge, Middlesex, UB8 3PH
United Kingdom

Mohammed.Al-Momin@brunel.ac.uk

Abstract: - Bandwidth, latency and data security are the three major factors that affect the Quality of Service (QoS) for any computer network. Different applications running on a network have different requirements of these three factors, and dealing with all applications types in a similar manner is an inefficient approach. This paper proposes a routing protocol that recognizes the type of traffic and routes it accordingly to provide the optimal QoS. Different data types are to be routed through different routes to satisfy the preferred QoS requirements of these data types. The weights of the network's links were partitioned in this paper into three layers to accommodate these three QoS requirements factors.

Key Words: - QoS, Adaptive Weighted Routing, Latency, Secure Transmission, Optical Network.

1 Introduction

A lot of works have been achieved to enhance the QoS of computer networks. The massive increase in the number of Internet users together with the rapid developments in the range of applications running over Internet has served as an incentive to encourage research towards finding an efficient routing technique. Data traffic on the Internet are not of the same types since they do not belong to a single application type. These different traffic types have different quality requirements and need to be dealt with differently. Some of the traffic over the Internet requires more bandwidth than others, whereas some other applications need less end-to-end delay (Latency). Furthermore, there are some other data that need to be dealt with most securely. For instance, phone-to-phone delay needs to be no more that 150 milliseconds to allow a comprehensible phone communications [1][2]. Non real time applications like web browsing and email are less delay sensitive, but loss sensitive instead, therefore the Internet operator should allocate a sufficient bandwidth for them, otherwise when there is network congestion they may be shed. When optical cable was first produced, it was considered to be immune against espionage. It has since been proven that it is not only possible to be insecure, but also, it could be simpler to tap than other predecessor technologies [3]. Some private information over the Internet such as VoIP and video telephony, in addition to their delay sensitivity, need to be transmitted securely without been revealed by eves droppers. The current Internet does not take into account the characteristics associated to each type of applications to assure an acceptable QoS [1][4]. This blind view to traffic leads to a uniform treatment of data traffic and consequently to a low quality of service. Metrics used in this paper to characterize applications' QoS requirements are the Available Bandwidth, Latency and Security.

This paper is organized as follows. Section 2 will describe the related works proposed to enhance the QoS in computer networks. In section 3, the three QoS requirement considered in this paper will be explained. In section 4, the proposed Three-Layer Weighted Link Routing Protocol (TLWLRP) will be explained. In section 5, an OMNeT++ model was created to simulate a sample optical network with the new routing protocol. Section 6 is concerned with the simulation results and their discussions. Finally, section 7 states some conclusions from this paper.

2 Related Works

Research in the last decades focused on two issues of computer networking, namely, the QoS and the security, dealing with them as two separate issues. Most of these works was achieved on Mobile Ad-hoc Networks (MANETs). In [5], three QoS requirements were considered to propose an enhanced QoS routing protocol for MANETs. These three requirements are bandwidth, latency and node lifetime. In addition to the fact that this protocol was proposed for MANETs whereas our proposal applies for optical networks, the last QoS requirement is more related to wireless Ad-hoc networks because they do not have a fixed infrastructure. In such networks, at any certain time, a node failure may occur since it is determined by the minimum battery lifetime of the node.

In [6], a system was presented to secure data over wireless Ad-hoc network as well. Elliptic curve cryptography was used to protect the privacy of information between the communicating nodes. It uses the idea of clustering to increase the system reliability. A limitation with [6] is that it considers only one QoS requirement, which is the security, ignoring other parameters.

Several research have been made on QoS routing for optical networks [7][8][9]. These researches have two drawbacks. First, they did not consider the security as a factor that affects the QoS, whereas in our paper we considered security as a third crucial parameter that evaluates the QoS in addition to bandwidth and delay. Secondly, they have treated each QoS requirement separately as an independent parameter, whereas some applications over the Internet need a mix of certain amounts of the different requirements. For instance, VoIP communications need both high levels of latency and security, and an acceptable amount of bandwidth. On demand media can accept a lower level of security but high levels of bandwidth and latency.

In most papers, security was dealt with separately, apart from being a QoS parameter, whereas other papers which are interested in security have no concern of the QoS and vice versa. An innovative way of protecting optical links from being tapped was proposed in [3]. Oyster optics' technologies attach a pair of secure oyster transceiver cards to every secure channel as shown in Fig.1 below.

This innovative idea for securing optical channels will be used in this paper to introduce the security as a new QoS parameter to our proposed QoS routing protocol.

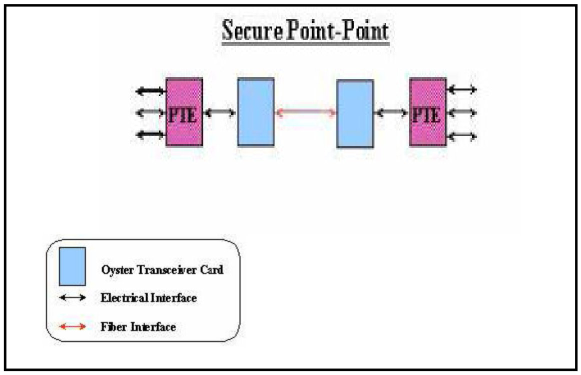


Fig.1: Using Oyster Transceivers for Securing Optical Channel

3. QoS Requirements

Internet nowadays offers a wide range of services, such as web browsing, email, on demand audios and videos and other services. The main motivation behind the next generation research is to control the quality of services being offered to the users, and the range of these services. The current Internet uses the best effort protocol in dealing with all information types transmitted on it. In best effort technique, only one route is allocated for each source-destination pair, where all the traffic directed to the same destination is sent through the same path regardless of the traffic type. Therefore, it provides the same level of quality to all application types transmitted on it.

Three QoS factors were considered in this paper

3.1 Bandwidth

In best effort protocol, there is just one path to follow for each destination [4]. In the case that a link is congested, the information will be dropped negatively affecting the QoS. The network in this protocol never guarantees that all the sent data will be received without loss as shown in Fig.2. In this paper, the required bandwidth for the data flow belonging to a particular application is estimated first, the available bandwidth of the paths leading to the destination is checked, and then the data will be transmitted across that path in which this data fit.

Applications differ in terms of the bandwidth they require. For instance, P2P file sharing is the most bandwidth consuming application, therefore, any shortfall in the channel's bandwidth will lead to a data loss. If the congestions of links are not taken into account, much of information will be lost. Note that the available bandwidth of a link is changing with the link's load. Therefore, our routing protocol checks the statistics of the links every time traffic is to be sent, and it chooses the available least congested path to transmit those applications with high bandwidth sensitivity to avoid data losses. This selection of the least congested routes will contribute to balance the load over the different networks' links. Packets lost en-route will either be retransmitted as it is the case in the TCP applications, or ignored possibly resulting in an impaired quality of the application output as in the case of UDP applications. In the first case retransmitting the lost data will increase congestion in the network and cost more delay for the application, and in the second case, the data will be lost at the application, therefore in both cases this will result in a lower QoS.

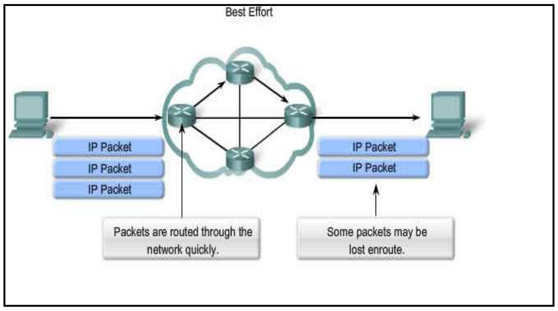

Best Effort
IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
Packets are routed through the network quickly.
Some packets may be lost enroute.

Fig.2: A Network with Best Effort Protocol

3.2 Delay

The end-to-end delay is another crucial requirement that affects the QoS [10]. In general, real time applications usually need a special care in that requirement, because some applications cannot tolerate long delays and need to be dealt with as a delay sensitive application. The end-to-end delay between any two communicating parties is composed of four sub-delays: queuing delay, processing delay, transmission delay and propagation delay. In the optical networks which is the case considered in our paper, the speed of data transmission and propagation is so high that these delays can be neglected.

Queuing delay is the time required for a packet to be processed (processing time) in the node's buffer and sent when the transmission channel is ready. It is directly proportional to buffer size. When the packet arrival rate at a particular optical router exceeds the buffer's packet transmission rate, the packets will be accumulated in the buffer, and when the buffer fills, the surplus packets will be dropped.

If the packet arrival rate of a particular queue is more than its packet departure rate, the packet loss rate will be unpredictable and will sharply increase. Consequently, a feedback could be sent to the sending entity to regulate its transmission rate. However, a queuing delay and a processing delay are also required at each hop, therefore, reducing the number of hops will reduce the total time consumed due to traffic queuing and processing.

In optical networks, it is currently technologically infeasible to have an optical cache that keeps a store of the high bandwidth traffic transmitted on the optical cables. To solve this problem, the optical data should be first converted to electronic form, queued in an electronic buffer, processed electronically in that queue, and then converted back to its optical form. This can be performed by Optical-Electronic-Optical converters.

3.3 Security

Data security is one of the most significant QoS factors. Although the Internet represents a completely insecure media for exchanging information, some private information needs to be transmitted on the Internet. This information needs to be transmitted securely without being revealed or attacked by intruders. Using cryptography is one of the methods used to protect the privacy of information, where data is converted into an unconceivable form. The original data is called plain text, and the encrypted data is called cipher text. Only the authorised user at the destination will be able to decrypt the message. Cryptography is an efficient way of protecting data from unauthorized access to these data, but it still has its own drawbacks. One drawback is that its protocols run in the presentation layer of OSI model, or below the high level application protocols and above the TCP/IP layer in TCP/IP model. That means that it will leave all the underlying layers insecure. So it does not work to protect data in the physical layer, where intruders still have the opportunity to extract data by tapping the cable connecting the communicating entities.

Another problem with cryptography is that it is depending on a mathematically solvable algorithm, with one secret key. There is no real existence of what is so called unbreakable cryptographic scheme, since by using the new technologies, fast processors and brute force algorithms, the secret key can be derived [11]. However, cryptography has a small usability rate due to the difficulties in implementation and maintaining and the high cost associated with using it [12].

In optical networks there are a lot of techniques used by intruders to tap the optical cable. All of these tapping techniques fall into one of these optical tapping categories:

A- Splicing: This tapping method is done by splicing the optical cable between the two communicating parties, and inserting an sensor between the two splices, this sensor allows the two communicating parties to exchange information, but sends this information to a third party (intruder) as well.

B- Splitter and Coupler: In this method no splicing is necessary. The cable is either bent to allow a small amount of the light to escape from the optical cable to be captured by photo-detector equipment as shown in Fig.3-a, or a clamp with an optical detectors is placed somewhere on the cable to detect the information as in Fig3-b. Receiving just 1% from the light of signal in the cable will be enough to detect the information transmitted on that link.

C- Non-touching tapping: In this method no interference with the optical cable is required, because this method depends on capturing the small amount of light naturally radiated from the cable.

Since cryptography does not work in the physical layer as mentioned before, it is infeasible to use it in protecting the optical cables tapping. As an alternative, Oyster Optics technology can be used to supply some of the network's links with a high level of security at the physical layer.

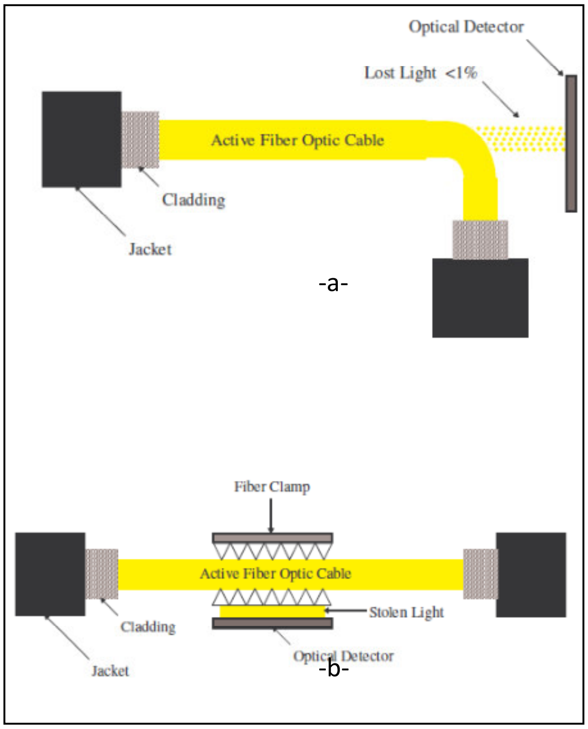


Fig.3: Optical Tapping Using Splitter and Coupler Method

Oyster Optics technology uses a patented method of secure phase modulation to securing data over the optical link. This security technique is fully explained in [3].

Two application types, namely, VoIP and video communications, were assigned high security sensitivity in this paper, and ten links in our optical network were secured using Oyster Optics technology to supply the network with secure routes for the transmission of these private data.

4 Three-Layer Weighted Link Routing Protocol (TLWLRP)

This paper suggests breaking the link weight into three sub weights (layers), namely, the available bandwidth, the latency, and the security. Each packet over the network has TOS (Type Of Service) bits in its header to define the class of traffic. Each application has three coefficients (k1, k2, k3), one to reflect the importance of each of the QoS requirements to this application type. The sum of these coefficients equals 1. For instance, interactive gaming traffic is a very small bandwidth consuming application; therefore, the bandwidth is not of real importance since just a little amount of it will be sufficient, so k1 is set to the value of 30%. On the other hand, this application type is very delay sensitive, therefore, traffic due to this type need to be routed as fast as possible [9], k2=70%. Security is not of real importance for this class of traffic, k3=0%. The resultant link weight, which will be used to choose the optimal path to the destination according to these QoS requirements, will be calculated using equation (1) below.

$$\begin{aligned}\text{Total Load} = &(k1 \times \text{Available Bandwidth})\\ &+ (k2 \times \text{End-to-End Delay})\\ &+ (k3 \times \text{Security}) \qquad (1)\end{aligned}$$

The weighted Djikstra routing algorithm, with some changes to accommodate these three-layer sub weights, was used in this paper in an OMNeT++ simulation platform to select the desired routes to the different destinations.

Note that the available bandwidth is calculated using equation (2) below [13].

$$B_A = \frac{(100-Load)*channel\_bandwidth}{100} \qquad (2)$$

Where B_A is the available bandwidth of the optical link. As the name of our proposed protocol implies, the available bandwidth is to be adapted and updated with time to give the protocol a clear image of how the link is utilized.

The network layer is responsible of the routing protocols; therefore, our TLWLRP function should be placed at that layer as shown in Fig.4 below. A signaling system is used supply TLWLRP with QoS requirements of the different applications from the application layer, and link utilization information from the physical layer.

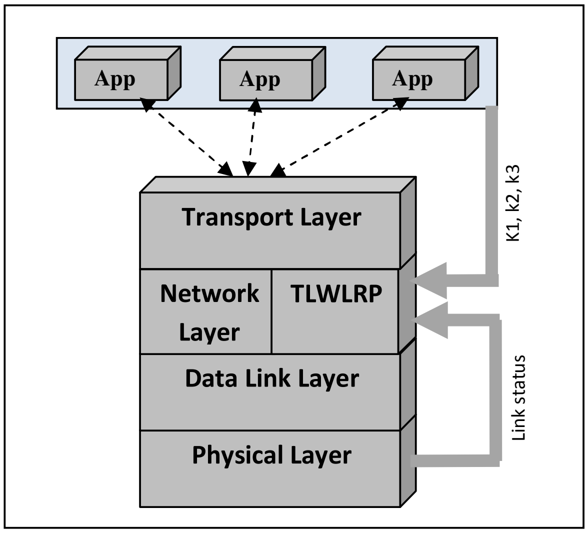


Fig.4: Internet Layered System with TLWLRP

Using TLWLRP means that applications between the same source and destination nodes may take different routes according to the QoS requirements of the application and the route characteristics. The proposed routing protocol offers high reliability in cases of nodes or cable failure. This is because the protocol will automatically choose the alternative second optimal route to deliver the traffic.

4.1 Applications and QoS Requirements

Different applications have dissimilar QoS requirements. Nine application types were considered in this paper. These application types cover all types of possible applications used on the Internet nowadays [14][15]. These applications are: web browsing, streaming audio, streaming video, IPTV, VoIP, video communication, interactive gaming, P2P file sharing and miscellaneous uploads and download.

However, the applications on the current Internet are categorized into two main categories:

A- Asymmetric Applications:
Those applications, which do not request equal resource consumptions on the both end-point hosts, are termed as asymmetric applications.

B- Symmetric Applications:
The applications under this category request the same amount of resource consumptions on the both end point hosts.

According to this classification, each of our applications used in this paper falls into one of the following classes: Non Real Time and Asymmetric, Real Time and Asymmetric, Real Time and Synchronous.

4.1.1 Non Real Time and Asymmetric

This class includes those applications, which do not have any demanding delay and loss QoS requirements. The best way to deal with these applications is by using the first-come, first-served technique, or what is well known as best effort protocol. Examples of these applications are:

- Web browsing
- Miscellaneous uploads and downloads.
- Streaming Audio and video applications.
-P2P file Sharing.

Notice that all the non real time applications are asymmetric. This is because in the non real time applications, a client requests services from a server.

4.1.2 Real Time and Asymmetric

Those applications with real time requirements need an acceptable latency since they use real time protocols e.g. UDP and do not have time to invoke an Automatic Repeat Request (ARQ) protocol. Security is not an important QoS requirement for these applications because the nature of the traffic being communicated is not private. Interactive gaming falls in this class.

4.1.3 Real Time and Synchronous

Some applications request stringent QoS requirements. Applications in this class are considered bandwidth insensitive since they require very little amount bandwidth, latency sensitive and security sensitive. Examples of the application in this class are:

-VoIP.

- Video Communications.

The values of factors K1, K2 and K3 in Table 1 were derived from the QoS requirements statistics for the different applications in [1] and [14].

Table 1: QoS Requirements Weightings for the Different Applications

Application	K1	K2	K3
Web Browsing	0.75	0.25	0
Streaming Audio	0.40	0.60	0
Streaming Video	0.50	0.50	0
IPTV	0.30	0.70	0
VoIP	0.10	0.45	0.45
Video Communications	0.05	0.47	0.48
Interactive Gaming	0.10	0.90	0
P2P File Sharing	0.90	0.10	0
Misc. Up/Download	0.50	0.50	0

4.2 Securing Channels on Optical Networks

Oyster Optics, Inc. has patented a way for securing data over optical networks in an encryption-free manner [3]. Since this security operation takes place in the physical layer, all the upper layers will be protected as well. One of the major benefits of this security technique is its possibility to be applied to the already existing infrastructure. It is infeasible to change the entire optical communication infrastructure in order to get all the data transmitted over the network secured, this will be a costly process. In addition, some applications do not need their traffics to be secured. The best solution is to replace the transceivers of some optical links by secure Oyster transceiver cards in order to create some secure paths across the already existing optical network as shown in Fig.1. Our proposed routing protocol was employed to route the security-sensitive data through these secure paths. Oyster Optics security technology is thoroughly explained in [3].

5 System Simulation

The optical network shown in Fig.5 was simulated using OMNeT++ simulator to investigate the QoS improvements gained using our proposed routing protocol. Nineteen nodes were interconnected through both secure and unsecure optical links. Each node represents a Regional Area Network (RAN) with 10000 users. Ten links were secured using the Oyster Optics technology mentioned in section 4.2.

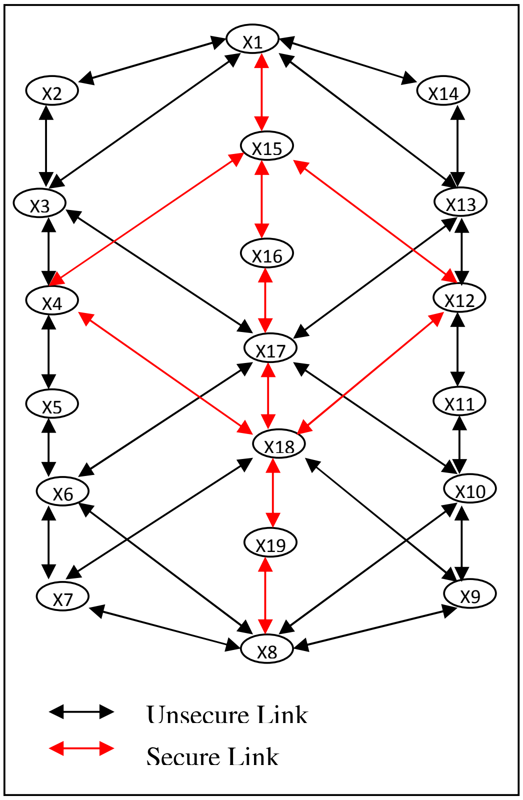


Fig.5: Optical Network with Secure and Unsecure Links

The nine application types in Table 1 were applied to the network. In order to easily investigate the feasibility of our proposed routing protocol, and to clarify the behaviour of the proposed routing technique against different QoS requirements, the traffic over the network links due to three application types were focused on and analysed. These three applications are: P2P file sharing, interactive gaming and video communication. These three applications were chosen because P2P has (0.9, 0.1, 0) QoS requirements as shown in Table 1, therefore, it is extremely bandwidth sensitive. Consequently, it can be analysed to prove the efficiency of bandwidth selectivity in our proposed scheme. Interactive gaming (0.1, 0.9, 0) on the other hand is a very delay sensitive application, and was analysed to show the delay latency selectivity. Finally, video communication (0.05, 0.47, 0.48) was used to test the security selectivity of TLWLRP. Traffics between any source-destination pair at busy time is computed using equation (3).

$$TF_{A\rightarrow B} = B_{App} * NOU_A * ({}^{NOU_B}/_{NOU_T}) \qquad (3)$$

Where:

$TF_{A\rightarrow B}$: Traffic flow directed from A to B.

B_{App}: Bandwidth required for an application type. (Per User Busy Hour Rate).

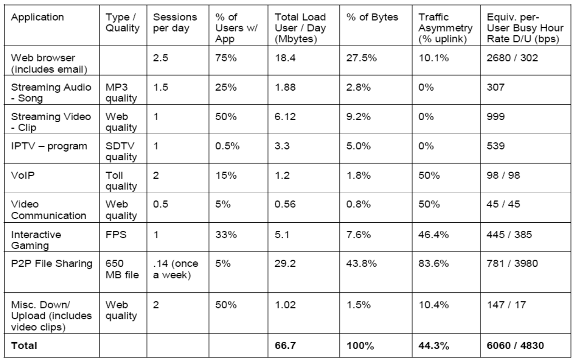
NOU_A: Number of users of node A.

NOU_B: Number of users of node B.

NOU_T: Total number of network's users.

The required bandwidth for each application type is taken from [14] as shown in Table [2].

Table 2. User Behavior Statistics



Application	Type / Quality	Sessions per day	% of Users w/ App	Total Load User / Day (Mbytes)	% of Bytes	Traffic Asymmetry (% uplink)	Equiv. per-User Busy Hour Rate D/U (bps)
Web browser (includes email)		2.5	75%	18.4	27.5%	10.1%	2680 / 302
Streaming Audio - Song	MP3 quality	1.5	25%	1.88	2.8%	0%	307
Streaming Video - Clip	Web quality	1	50%	6.12	9.2%	0%	999
IPTV – program	SDTV quality	1	0.5%	3.3	5.0%	0%	539
VoIP	Toll quality	2	15%	1.2	1.8%	50%	98 / 98
Video Communication	Web quality	0.5	5%	0.56	0.8%	50%	45 / 45
Interactive Gaming	FPS	1	33%	5.1	7.6%	46.4%	445 / 385
P2P File Sharing	650 MB file	.14 (once a week)	5%	29.2	43.8%	83.6%	781 / 3980
Misc. Down/ Upload (includes video clips)	Web quality	2	50%	1.02	1.5%	10.4%	147 / 17
Total				**66.7**	**100%**	**44.3%**	**6060 / 4830**

6 Results

To investigate the feasibility of our new routing protocol clearly, three application types, namely, P2P file sharing, interactive gaming and video communications, were put under the focus, and the traffics due to them were calculated on the different networks' links. The QoS requirements patterns for these application types are (0.9, 0.1, 0), (0.1, 0.9, 0) and (0.05, 0.47, 0.48). Mainly, four benefits were gained from our proposed routing protocol: releasing more bandwidth from the congested links to avoid data loss when the amount of traffic exceeds the channel capacity, reducing the end to end delay for the delay sensitive applications, securing the private data over the network and links' load balancing.

6.1 Bandwidth Gain

Fig.6 shows that the rate of increase in the used bandwidth of the link (link utilization) due to P2P file sharing decreases with the increase of the total network load rate corresponding to that application type to allow spreading load over the other links leading to an improved links' utilisations. The available bandwidth is a vital factor in choosing the optimal route for this application type. This enhances the links' utilisations because the traffics select the route with the most available bandwidth and avoid the congested ones.

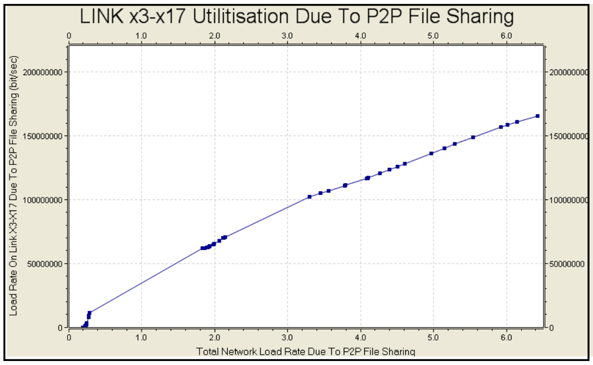


Fig.6: Link x3-x17 Utilisation Due To P2P File Sharing

6.2 Delay Gain

The traffics over the various network's links due to interactive gaming (0.1, 0.9, 0) are shown in Fig.7. This type of traffic prefers those routes with the minimum end to end delay. Since our network is optical, the link speed is very high and we assume that the propagation time is negligible. The Optical-Electronic-Optical (O-E-O) conversions are the most time consuming operations. Since one O-E-O conversion is required for each hop, the optimal route to be chosen is that of the minimum number of hops. Most of the high bars in Fig.7 represent the load over the sloping (diagonal) links in Fig.5 because these links serve to decrease the number of the required hops to their destinations. Therefore, these routes will be loaded more than the others with this QoS requirements pattern.

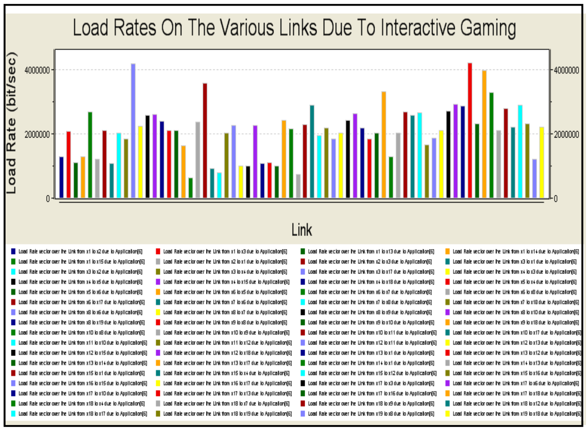


Fig.7: Load Rates Over The Various Links Due To Interactive Gaming

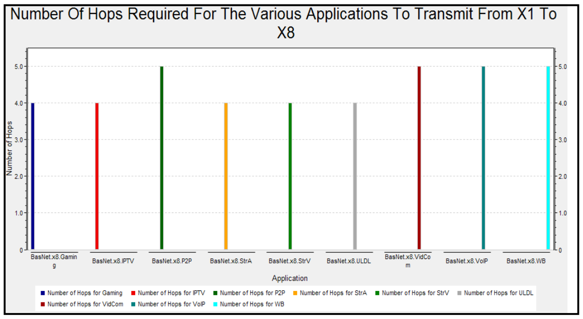


Fig.8: Number of Hops Required For The Various Applications To Transmit From X1 to X8

Fig.8 shows the number of hops required for the different applications in our application mix to transmit from X1 to X8. The diagonal routes (x1-x3-x17-x6-x8) and (x1-x13-x17-x10-x8) represent the available minimum number of hops routes from X1 to X8 with four hops. Therefore, interactive gaming, IPTV, streaming audio, streaming video and miscellaneous up/downloads follow these routs since they all have relatively high delay sensitivity. On the other hand, P2P file sharing and web browsing are bandwidth sensitive applications, thus they select those routes of the highest available bandwidth, i.e., they avoid the congested links which were allocated for the five delay sensitive applications even if they are the shortest path routes. The two remaining application types, VoIP and video communications are security and delay sensitive applications. Consequently they look for minimum delay and maximum security available routes to send their traffics through. Even though these applications tolerate one more hop than the minimum number of hops but that would be at the expense of increasing the path's security as shown in Fig.10.

6.3 Security Gain

Fig.9 below shows the traffics over the links due to VoIP. From this figure, it is clear that the secure links (red links in Fig.5) are the most congested links because the traffics due to this type of application is security sensitive, thus it prefers transmitting data over the secure links.

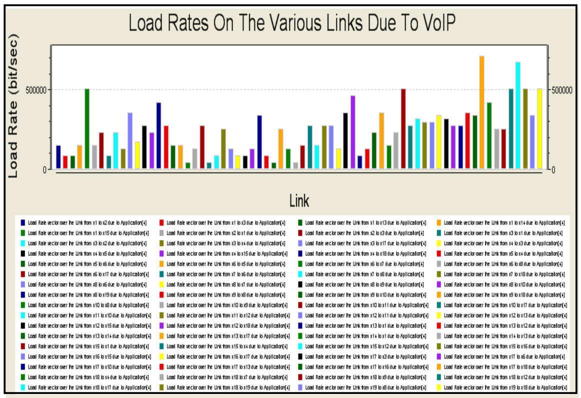


Fig.9: Load Rates over the Various Links due to VoIP

From Fig.10 note that VoIP and video communication were completely secured to a percentage of 100% by transmitting through the routs (X1-X15-X4-X18-X19-X8) and (X1-X15-X12-X18-X19-X8), whereas web browsing and P2P file sharing were partially secured to 60% that is not because we need them to be secured, but because their routes are through some secure links to avoid the congestion of the other links since they have a relatively high bandwidth sensitivity.

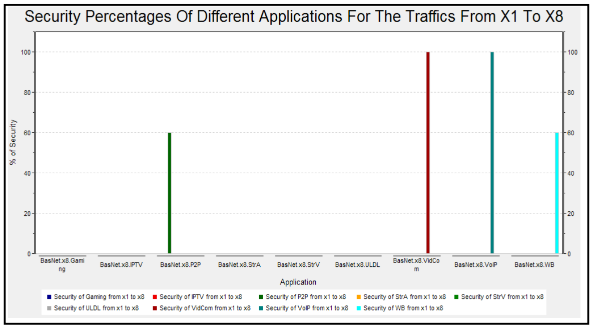


Fig.10: Security Percentages of Different Applications for the Traffics from X1 To X8

6.4 Load Balancing

Bandwidth sensitive applications will also contribute to improve the link utilization efficiency as a consequence of balancing load rates over the different links. Fig.11 clarifies how the P2P File Sharing load rate is balanced over the various links.

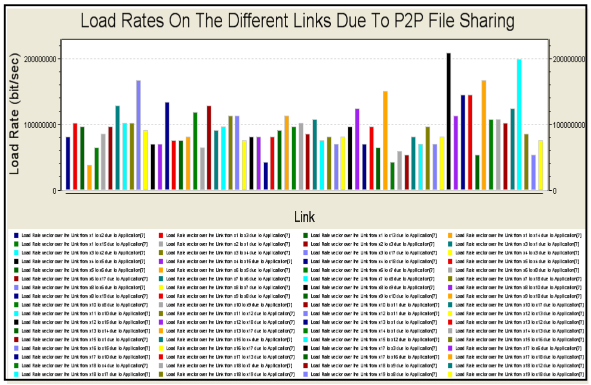


Fig.11: Load Rates over the Various Links due to P2P File Sharing

6.5 Comparison with Other Routing Protocols

Two conventional routing protocols were selected here to compare our proposed routing with them. These protocols are: Latency-Aware Routing Protocol and Congestion Aware Routing Protocol.

6.5.1 Latency-Aware Routing Protocol

In latency-aware routing, the end to end delays for all traffics types are minimised, where it is clear from Fig.12 that the number of hops from X1 to X8 was minimised to only four hops regardless how sensitive this information is to delay, but on the other hand, it does not differentiate among the different traffic types. This creates congestions over the fast delivery routes (diagonal links) as is shown in Fig.13 below, where it is clear that the load is not fairly distributed over the networks links and the network's links are inefficiently utilised. This routing technique conventionally offers no bandwidth QoS, and no 0% security for all information since no links were secured in this conventional type of this routing technique.

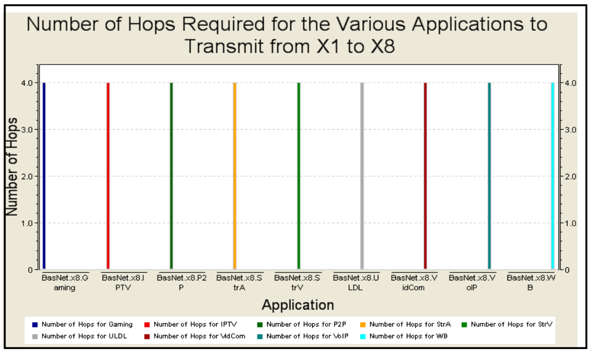


Fig.12: Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Latency-Aware Routing

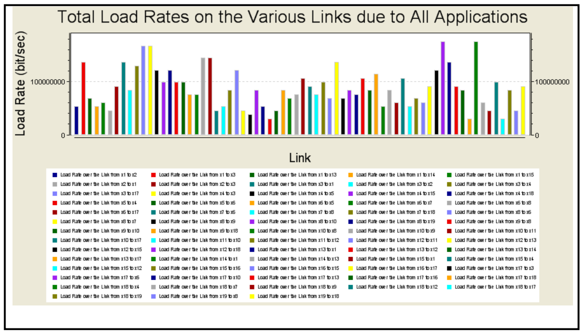


Fig.13: Total Load Rates on the Various Links in Latency-Aware Routing

6.5.2 Congestion-Aware Routing Protocol

This routing technique enhances the links' efficiencies by balancing the load over them as shown in Fig.14, but it still does not differentiate among the traffic types, and does not offer any QoS other than the congestion avoidance. The achieved load balance will be on expense of extra end to end delays for the information as shown in Fig.15. Again, conventional congestion-aware types offer 0% security level since oyster optics secured links has not been used with this routing technique.

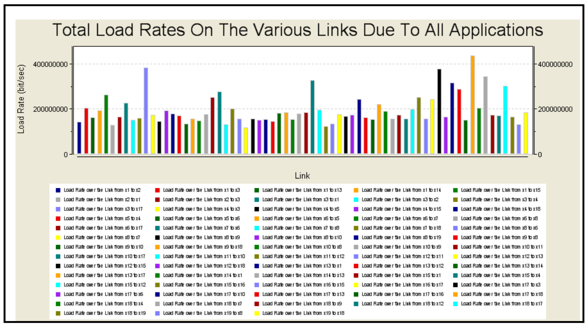


Fig.14: Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Congestion-Aware Routing

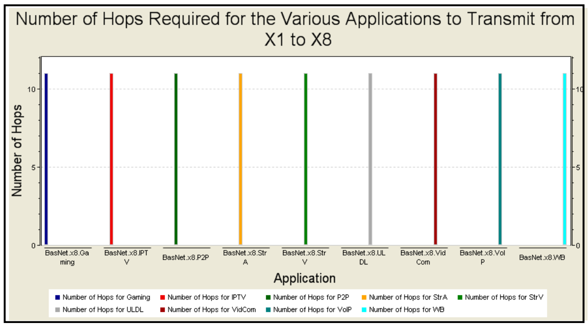


Fig.15: Number of Hops Required for the Various Applications to Transmit from X1 to X8 in Congestion-Aware Routing

These results show that our proposed routing technique outperforms other routing protocols since it differentiates among the different traffic types, utilizes all the bandwidth, whilst meeting the desired latency and security QoS requirements by making suitable routing decisions.

7 Conclusion

This paper proposes a novel routing protocol for improving the QoS in optical computer networks. Three QoS issues have been addressed here, namely: bandwidth, delay and security. Oyster Optics security technology was used by inserting some transceiver cards on some optical links in order to get them secured.

A mix of nine application types was applied to a sample optical network with some secure links. Each of these applications was assigned three factors k1, k2, and k3 to reflect the significance of available bandwidth, end-to-end delay, and security issues to that application. The optical link weight was divided into three layers to accommodate these three QoS significance factors.

By keeping a track of the load rate changes on the different network's links, this routing protocol is able to be adaptive, since it would continuously read and update links' statuses by using physical layer sensors to inform TLWLRP in the network layer of the new links' statuses. This information together with the information of QoS requirements from the application layer is used by TLWLRP to select the optimal route for each type of traffics.

The results of our simulations shows that the benefits of this routing technique is that, compared to more conventional techniques, it releases more links' bandwidths, provides more efficient links utilisation, decreases the end-to-end delay for the delay sensitive applications, provides secure transmission for private data, and balances load rates on the different network's links. Overall, it clearly improves the QoS offered by the network.

References:

[1] Y. Chen, T. Farley, N. Ye, QoS Requirements of Network Applications on the Internet, *Information-Knowledge-Systems Management*, Vol. 4 Issue 1, 2004, pp. 55-76.

[2] Cisco, 2008, Understanding Delay in Packet Voice Networks. [online] available at: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml#standarfordelaylimits [Accessed: 14 February 2012]

[3] U S Patents, *Securing Fiber Optic Communications against Optical Tapping Methods*, Oyster Optics, Inc. 2003. Available: www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf [Accessed: 14 February 2012]

[4] B R. Smith , J.J. Garcia-Luna-Aceves, Best Effort Quality-of-Service, *Proceedings of 17th International Conference on Computer Communications and Networks*, US Virgin Islands, 2008, pp. 1-6.

[5] A. N. Al-Khwildi, S. Khan, K. K. Loo, H. S. Al-Raweshidy, Adaptive link-weight routing protocol using cross-layer communication for MANET, *WSEAS Transactions on Communications,* Vol. 6, Issue 11, 2007.

[6] V. Vijayalakshmi, T.G. Palanivelu, Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography, *Journal of Computer Science*, Vol. 3, Issue 12, pp. 939-943, 2007.

[7] W. Zhang, J. Tang, C. Wang, S. d. Soysa, Reliable Adaptive Multipath Provisioning with Bandwidth and Differential Delay Constraints, *INFOCOM'10 Proceedings of the 29th conference on Information communications,* IEEE Press Piscataway, pp. 2178-2186, , USA, 2010.

[8] T. Deng, S. Subramaniam, Adaptive QoS routing in dynamic wavelength-routed optical networks, *2nd International Conference on Broadband Networks*, BroadNets 2005. Vol. 1, pp. 184-193, 2005.

[9] V. N. Raghavan, M. Venkatesh, T. Labbai, P. D. Prabhu, Evaluating Performance of Quality-of-Service Routing in Large Networks, *World Academy of Science, Engineering and Technology, 2007.* Available: www.waset.org/journals/waset/v26/v26-48.pdf [Accessed: 14 February 2012]

[10] Y. Ito, S. Tasaka and Y. Fukut, Psychometric analysis of the effect of end-to-end delay on user-level QoS in live audio-video transmission, *IEEE International Conference on Communications,* Vol. 4, 2004, pp. 2214 – 2220

[11] T. Eisenbart, S. Kuma, A Survey of Lightweight Cryptography Implementations, *IEEE Design & Test of Computers*, Vol. 24, Issue 6, 2007, pp. 522 – 533.

[12] N. R. Potlapall, S. Ravi, A. Raghunatha, Niraj K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, *IEEE Transactions on Mobile Computing*, Vol. 5, Issue 2, 2006, pp. 128 – 143.

[13] C.R. Lin, J.-S. Liu, QoS routing in ad hoc wireless networks, *IEEE Journal Selected Areas in Communications*, Vol.17, No.8, 1999, pp. 1426-1438.

[14] M. Needham, J. Harris, Traffic and Network Modeling for Next Generation Applications, *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, Las Vegas, Nevada USA, April, 2008, pp. 1-18.

[15] J. Cosmas, J. Loo, A. Aggoun, E. Tsekleves, Matlab traffic and network flow model for planning impact of 3D applications on networks, *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, Shanghai, China, 2008, pp. 1-7.

Mohammed M. Saeed Abdullah Al-Momin was born on October 17, 1980, in Basrah, Iraq. He was educated in Iraq and received B.Sc. degree in computer engineering in 2002 from University of Basrah, Iraq. He received the M.Sc.

degree in computer engineering in 2005 from University of Basrah, Iraq. He worked as an assistant lecturer at the technical college of Basrah. He is currently a Ph.D. student at Brunel University, London, UK. His research area is concerned with computer networks and QoS routing.

John Cosmas is a Professor of Multimedia Systems in the School of Engineering and Design at Brunel University in West London. He co-leads the Wireless Networks and Communications Research Centre, (http://www.brunel.ac.uk/sed/ece/research/wncc), is the course director of MSc Advanced Multimedia Design and 3D Technologies (http://www.brunel.ac.uk/sed/ece/courses/postgraduate/advanced-multimedia-design-and-3d-technologies-msc) and is an associate editor of IEEE Transactions on Broadcasting.

His research interests are concerned with the development of Multimedia Systems applied to Future of Broadcasting, the Future of Internet and 3D multimedia video/graphics design and the synergies between these technologies. He has participated in eleven EU-IST and two EPSRC funded research projects since 1986 and he has led three of these (CISMUNDUS, PLUTO, 3D MURALE).

Saman Hameed Amin received the B.S. in Control and System Engineering and the M.S. in Computer Engineering from University of Technology, Iraq. He is currently PhD student in School of Electric and Computer Engineering, Brunel University, UK. His research areas include wireless communication, network security and cognitive network.