# A Comparison of Path Protections with Availability Concern in WDM Core Network

M. A. Farabi
Photonic Technology Lab,
Universiti Teknologi Malaysia,
Malaysia

S. M. Idrus
Member, IEEE
Photonic Technology Lab,
Universiti Teknologi Malaysia,
Malaysia

S. N. Fariza
Photonic Technology Lab,
Universiti Teknologi Malaysia,
Malaysia

Nadiatulhuda Zulkifli
Member, IEEE Photonic Technology
Lab, Universiti Teknologi Malaysia,
Malaysia

M. A. Al-Shargabi
Faculty of Computer Science &
Information Systems, Universiti
Teknologi Malaysia, Malaysia

## ABSTRACT

The Internet is supported by long haul WDM core networks. Reliability is a huge concern in WDM core networks since service disruption would carry significant revenue, reputation and prospect loss. In ensuring reliability to network services, two means of protection scheme are usually used in WDM core networks; dedicated path protection and shared path protection. A comprehensive comparison of dedicated and shared path protection is discussed in this study. Availability concerned path protection implemented in the study will be based on random dynamic arrival traffic with adaptive routing method. The comparison will be based on several quality benchmarks such as availability satisfaction ratio, blocking probability, link utilization, provisioning complexity and network utilization.

## General Terms

Telecommunication Network Reliability

## Keywords

WDM Core Network, Mesh, Dedicated Path Protection, Shared Path Protection

## 1. INTRODUCTION

Modern telecommunication links in WDM core networks can provide a huge bandwidth at a very high transmission speed. Hence, even a few seconds of links failure can results in an intolerable data loss. There are plenty of reasons for connection failures in a WDM core networks. Shared Risk Group (SRG) may consist of all the optical lines within the same fiber, or within the same cable wrapper or those who traverse through the same conduit [1]. Failures of any SRG components such as amplifier or conduit may affect multiple connections. Hence, it is important that the primary and the backup path are SRG disjoint to ensure survivability of one path in case of failure. Port failures affect only corresponding channel. Node failure is usually overcome by the use of redundant node components while link failure is handled via redundant capacity sharing of unaffected links [2]. Fiber links failure can be regarded as the most common factor of failure, caused either by natural disaster or manmade construction. This study will focus on fiber links failure.

Fault management in WDM core networks can ensure robustness and reliability of telecommunication services. Higher layer protocols such as such as ATM, IP and MPLS are not sufficient to cope up with the sub milliseconds failure recovery requirement of WDM core networks. Recovery protocol imbedded within the optical layer will enable even network without upper layer fault compensation capability to ensure network reliability. Two methods of this are by implementing either the high availability dedicated path protection (DPP) or the low network resource usage shared path protection (SPP). Most publications such as in [3-7] tend to use Shared Path Protection (SPP) while others such as in [8] use Dedicated Path Protection (DPP).

In publication [9], the authors studied the availabilities for connections with different protection schemes via an integer linear program (ILP) approach. However, the ILP is limited to static connection arrival and within the scope of dedicated path protection. The authors do propose heuristics for dedicated path protection and compare it to the previous ILP results. However, this study also inculcates heuristics of dynamic connection arrival and shared path protection which are not covered by the said publications.

The study will revisit the comparison between these schemes, but with added Quality of Service (QoS) benchmark. QoS offered by a service provider is defined in the Service Level Agreement (SLA), the contract of guaranteed minimum service quality provided by the service provider to its clients. The contribution of this study is the comprehensive comparison of DPP and SPP performance via multiple QOS benchmarks such as availability satisfaction ratio ($ASR$), blocking probability ($P_B$), link utilization ($\min \lambda$), algorithm complexity ($t$), and network utilization ($\% \lambda$). This paper will continue as follows; Section II explains the groundwork for fault management implementation, Section III explains on the simulation methodology, Section IV discusses the simulation results and lastly, Section V concludes the study.

## 2. WDM CORE NETWORK FAULT MANAGEMENT

Modern WDM core networks consists of three planes; the management, control and transport plane. Management plane handles the operations, administrations, maintenance, provisioning and troubleshooting. Transport plane function as the data carrier via the network component. An optical control plane is introduced between the planes to shift some intelligence from the management plane closer to the transport plane but do not replace the original function from the management plane. In the IETF, the optical control plane is referred to as Generalized Multi-Protocol Label Switching (GMPLS) and within the ITU-T, as the Automatic Switched Optical Network (ASON). Some of the applications of control plane are network discovery, routing, path computation, signaling and many more.

Routing is done at the control plane within the optical layer without upper layer intervention via Optical Time Division Multiplexing (OTDM), Code Division Multiplexing (CDM) or Wavelength Division Multiplexing (WDM). WDM implementation is preferred due to synchronization ease and technological limitation of OTDM and CDM. WDM combines multiple transmissions into a single fiber; increasing data processing speed for several hundred times higher than conventional method. Different wavelength are multiplexed into the fiber and demultiplexed at end devices. Shortcoming of WDM implementation is non infinite fiber bandwidth resources and electronic bottleneck speed limitation if intermediate electronic wavelength conversion is applied.

Different wavelength may be transmitted by the access network into the WDM core networks via wavelength multiplexer. However, the wavelength continuity constraint stated that lightpath must occupy the same wavelength on fiber link through which it traversed for purpose of interference avoidance. A transparent WDM optical network can ignore the said constraint by utilizing Optical Cross Connect (OXC) capable of transferring ten terabits per seconds [1] at nodes for routing connections without any intermediate electronic conversion. Meanwhile, limited WDM core networks are only capable for limited wavelength conversion or when OXC is placed sparsely in network. Wavelength conversion is usually achieved by using semiconductor optical amplifier, cross gain modulation, four waves mixing, dispersion shifted fiber and other interferometric technique. This study will focus on transparent WDM optical networks.

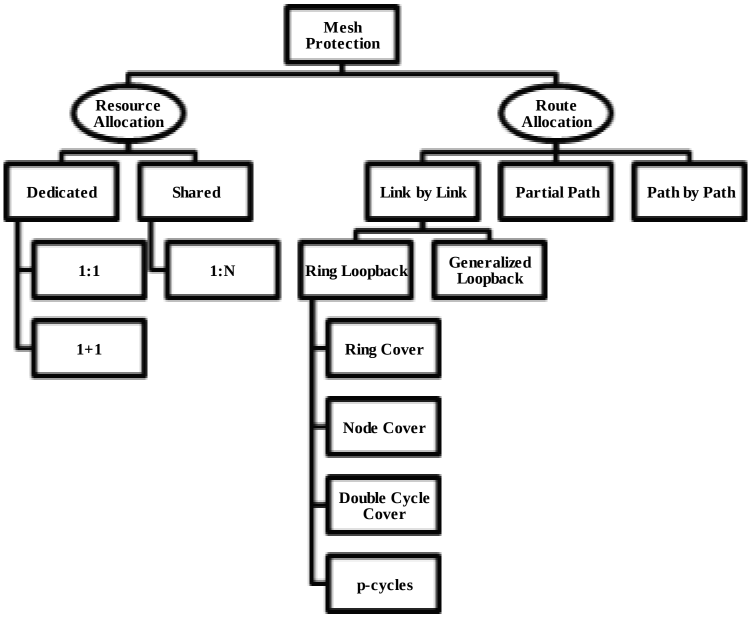

Fig. 1 Mesh Protection

WDM core networks recovery can be divided into two, via protection or restoration. Protection allows faster repair time than restoration [3] and guaranteed recovery from failure it is designed to protect [10]. Mesh protection as in Figure 1 is usually used in WDM core networks. Protection pre-computes and reserves backup resources in advanced during connection setup. Affected traffic will be rerouted to backup path during failure occurrence.

In terms of resource allocation paradigm, protection can be applied via dedicated or shared resource. Dedicated protection devotes backup resources for the primary connection, unavailable to any other entity [8]. Two common dedicated protection methods are; 1+1 method where data is transmitted simultaneously on primary and backup path and 1:1 method where data is transmitted in the primary path only, with idle or low traffic priority backup path. Shared protection, also known as 1:N protection shares backup resources among entities that their primary path is not traversing through a same link. Dedicated protection provides greater connection availability than shared protection which makes it preferred for stringent SLA needs application. Shared protection is more capacity efficient than dedicated protection but as the degree of sharing increases, the connection availability is reduced and longer recovery time than DPP since backup resources need to be configured after failure occurrence [2].

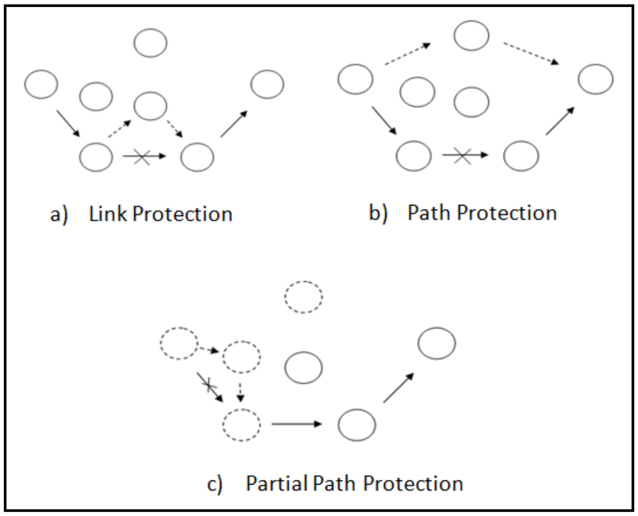

Fig.2 Route Allocation Paradigm

In terms of route allocation paradigm as in Figure 2, mesh protection is done via link by link protection (LP) basis, partial part protection (PPP) basis or path protection (PP) basis. LP reserves backup path for each primary path channel. PPP groups backup paths in a domain to collectively protect all channels on the primary path segment [8] that traverses within the same domain [10]. PPP can achieve a high scalability and faster recovery time compared to PP for a modest sacrifice in resource utilization, but still slower than LP [10]. For PP, two link disjoint routes will be allocated for a connection, the primary path and the backup path. PP utilizes backup resources best with a lower end to end propagation delay for the recovered route.

## 3. METHODOLOGY

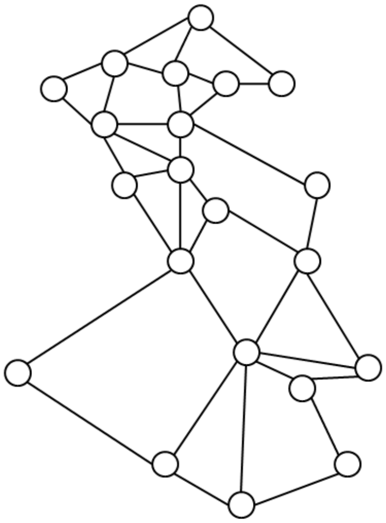

Fig. 3 Italian Network

21 nodes Italian WDM core network [11] with 36 bidirectional links is selected as the model network as in Figure 3. All nodes are assumed to have full wavelength conversion capability. The minimum nodal degree is two, maximum of six and average of 3.43. Each link has 16 wavelength channels with the ability to support bidirectional transmission. There are about 420 possible routes for the network. The maximum optical reach is 400km. Connection requests are randomly distributed among all possible source and destination nodes. Each connection uses entire wavelength channel. The connection will be blocked only if the primary path is unavailable. Although static lightpath establishment as used in publications [12-16] has the advantages of simplicity dynamic lightpath establishment as used in publications [3-7] is chosen for this study since it allocates and terminates connection periodically with higher bandwidth utilization and lower blocking probability than static case [17]. The randomness nature of the dynamic provisioning process can also serve as the average prediction of what the overall performance of the schemes might be. Incoming random connection requests are modeled by Poisson connection arrival rate with negative exponential service time and differ in holding time. Network loads are varied up to 150 Erlangs. Link loads are mutually independent so it is not affected by the number of connections carried by link. Only point to point traffic is considered. No queuing is available at nodes so if the connection cannot be serviced, it is blocked. A fully distributed control network is assumed so that the computation intelligence is distributed among nodes. All other network components availability is assumed to be unity. In all optical networks, most of wavelength assignment methods have the same performance [14] so first fit wavelength assignment that selects wavelengths according to a predefined order which leads to small computation overhead and low complexity with fair connection blocking will be implemented. Although fixed routing is simpler than adaptive routing, adaptive routing uses less resources with lower blocking probability. Adaptive routing which provision connections to current network state and terminates lightpath after a predefined lifetime is chosen for this study. It is inefficient to use fixed routing because if the fix allocated route for the source-destination pair is busy, the connection will immediately be blocked even before trying to allocate a different alternative path to it. Djisktra shortest path method is used to provision paths. Backup paths are only allocated for connection that their primary path has not fulfilled its availability requirement. In order to increase resource efficiency, connection availability can be varied according to the importance of the incoming data. Although it is known that in general, the availability request for telecommunication network is to be at 99.9%, in reality, this is often resulting in resource wastage since not all user connections carry the same importance i.e. 3-D online gaming, video conferencing and learning, video telephony and downloading, and high definition video on demand. Availability requirement should be varied according to the importance of multimedia content the connections is carrying. In this study, the availability requirements of the connection request are uniformly distributed among 98%, 99%, 99.5%, 99.7% or 99.9%.

Three mesh protection schemes are implemented; Adaptive Routing without protection (AR) in which connections are provisioned without any protection, Adaptive Routing with Dedicated Path Protection (ARDPP) in which connections are provisioned with 1:1 protection and Adaptive Routing with Shared Path Protection (ARSPP) in which connections are provisioned with 1:N protection. The proposed heuristics for this study is as follows:

```
Input: Network topology graph
Output: Lightpaths matrix with/without backup path

1. Create traffic request matrix of source and destination
   lightpath pairs with availability requirements, random
   traffic delay and random holding times among requests.
2. Start the timer.
3. Starting from the first request between node pairs
   perform the following steps in the graph:
      a. Delete those lightpaths with available
         capacities lower than requested pair
         requirements. It should be noted here that no
         wavelength channel is allowed to be shared
         in dedicated path protection case.
      b. Calculate the shortest path between the
         vertex-pair on the access layer. If path
         cannot be found, remove request from traffic
         list and add to blocked connections counter.
         Otherwise, use path to route request and
         compute the path availability. Mark the
         wavelength channel allocated.
      c. If either no protection is to be applied or the
         primary path availability already satisfies
         the required availability request, proceed to
         step h. Otherwise, continue to step d.
      d. Delete SRG links traversed by the primary
         path and lightpaths with available capacities
         lower than requested pair requirements. It
         should be noted here that no wavelength
         channel is allowed to be shared in dedicated
         path protection case.
      e. If dedicated path protection is applied,
         proceed to step g. Otherwise if shared path
         protection is applied, continue to step f.
      f. Delete all lightpaths that traverses through
         the same fiber as the primary path allocated
         before.
      g. Calculate the shortest path between the
         vertex-pair on the access layer. If path
         cannot be found, request is left in the traffic
         list with no protection.  Otherwise, reserve
         path as the backup route and compute the
         path availability. Mark the wavelength
         channel allocated.
      h. Update the timer and terminate connections
         that it's holding time has run out. Release all
         the resources used by that corresponding
         connections.
      i. Update the graph.
4. Repeat step 3 for all traffic requests in traffic list.
```

In order to accurately measure the performance of DPP and SPP, multiple QOS benchmarks such as availability satisfaction ratio ($ASR$), blocking probability ($P_B$), link utilization ($min\,\lambda$), algorithm complexity ($t$), and network utilization ($\%\,\lambda$) is taken into consideration.

Links availability ($a_l$) depends on Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) as in equations below where CC is the average length of cable that results in a single fiber cut per year. For terrestrial optical fiber, CC can be assumed to be 450km [18]. Duration of MTTR can be assumed as 24 hours long.

$$\text{MTBF}_{\text{fiber}}(\text{hours}) = \frac{\text{CC} \times 365 \times 24}{\text{length of fiber}}$$

$$a_l = 1 - \frac{\text{MTTR}_{\text{link}}}{\text{MTBF}_{\text{link}}}$$

The route availability ($A_p$) is defined by the following equations [9] where $a_p$ is the primary path availability, $a_b$ is the backup path availability, $\theta$ is the probability that connections sharing backup resources will not fail before the main connection fails. Since this study only focuses on single link failures scenario, $\theta$ can be assumed as unity.

$$A_p = 1 - \left(1 - a_p\right) \times (1 - \theta a_b) = a_p + a_b - a_p a_b$$

Which brings us to the equation of computing the availability satisfaction ratio ($ASR$). $A_r$ is the required path availability and p is the provision path.

$$ASR = \frac{\sum(A_p > A_r)}{\sum p}$$

Blocking probability ($P_B$) can be defined as the total percentage of connection that are unable to be provisioned by the network due to resource inefficiency.

$$P_B = \frac{\sum blocked\ connections}{\sum incoming\ traffic\ requests}$$

Link utilization ($min\,\lambda$) is defined as the minimum wavelength channel actually needed to fulfill the entire incoming traffic request at a given network traffic load.

$$min\,\lambda = \max(\lambda\ used\ at\ p)$$

Algorithm complexity ($t$) is defined as the time taken to provision the entire several thousand source-destination pair connection requests. The time is counted via a built in timer. Network utilization ($\%\,\lambda$) is defined as the percentage of network resources actually being used at a given traffic load. It should be noted here that the entire formula above are only for computing single parameter results while in the study, the results is averaged from several thousand run of heuristical study.

$$\%\lambda = \frac{\sum(\lambda\ used\ at\ each\ p)}{\sum(\lambda\ allocated\ at\ each\ p)}$$

## 4. RESULTS & DISCUSSIONS

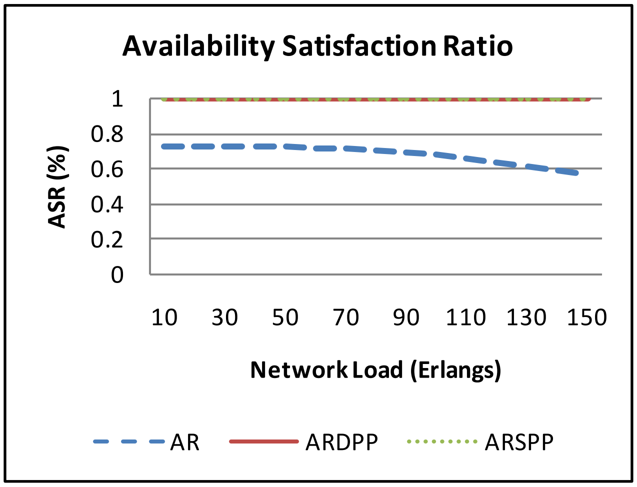

Fig.4 Availability Satisfaction Ratio vs. Network Load

From Figure 4, the benefit of implementing path protection in a WDM core networks is greatly shown. Both dedicated and shared path protection can offer perfect availability satisfaction ratio while an unprotected connection ASR will decrease as the network load increase. However, take note that the availability satisfaction ratio computation is only done on provisioned connection, thus making the next performance criterion equally important.

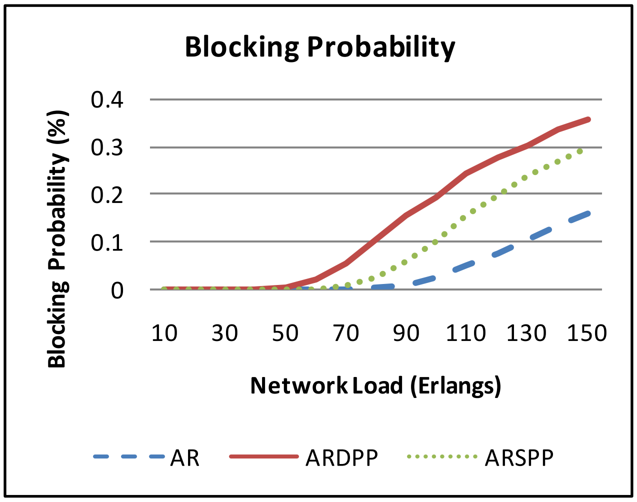

Fig.5 Blocking Probability vs. Network Load

The general trend that can be seen from Figure 5 is that increase of network load will increase the blocking probability. Although an unprotected connection performs best in terms of connection blocking probability, the earlier ASR computation shows that even though blocking occurrence is lesser, the ASR is not efficiently satisfied. Adding path protection will use up more network resources hence increasing the blocking probability but greatly improve availability satisfaction ratio. ASR represents the probability that a connection will remain active at a random time in the future. While both ARDPP and ARSPP perform similarly in ASR, ARDPP perform better in terms of resource blocking probability compared to ARSPP. It can be seen that network load contributes to no blocking for scheme ARDPP and ARSPP until about 50 Erlangs in which the rise is exponential while for scheme AR, blocking only starts to exist beyond 90 Erlangs. The increase of network load will reduce the time gap between connection arrivals making connection arriving more rapidly while the average holding time for in use connections remains the same. Hence, channel resources becomes limited due to slow release of connection that are unable to cope up with the increasing demand of rapidly incoming connections.

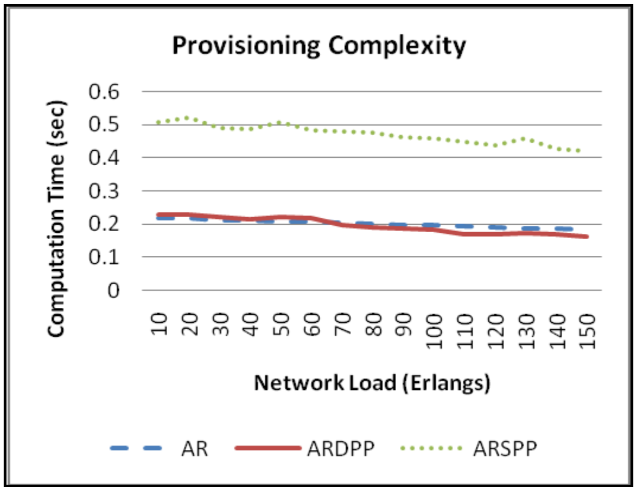

Fig.6 Provisioning Complexity vs. Network Load

Provisioning complexity is indicated by the computation time that depends greatly on processor speed and state. The processor used in this study is Intel Core i3-370M @ 2.4GHz with 4GB RAM. Scheme AR and ARDPP provision connections almost at equal cost of computation time. However, it may seems from Figure 6 that from 60 Erlangs of network load onwards, AR perform better in computation time than ARDPP but this is caused by the emerging effect of connection blocking in ARDPP which makes more connection blocking and thus reducing the number of connections that needs to be provisioned and reducing the average time needed to compute connection provisioning. Hence it can be concluded that adding dedicated path protection would not cost much in terms of computation time than utilizing no protection at all but with added benefit of ASR. ARSPP performs worst in terms of computational time required because the nodes needs to check the availability of wavelength channel that can be shared by protection since no primary path with same link traversed through can have any similar backup resources. The overall reducing trend of computation time required with increasing network load is caused by the increasing blocking probability with increasing network load.

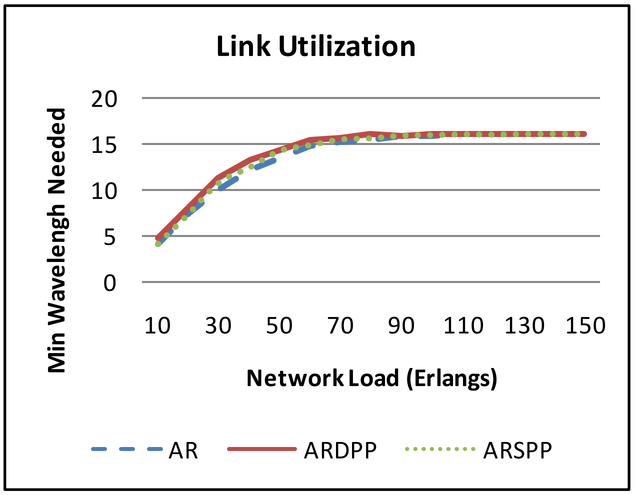

Fig.7 Link Utilization vs. Network Load

Although the amount of wavelength channel allocated per network link is fixed at 16, this study on wavelength channel used is done for the purpose of checking the wavelength utilization of each link. It seems from Figure 7 that the wavelength channels are underutilized for load under 60 Erlangs while at higher loads, all wavelength channel allocated at each fiber if fully used due to higher traffic rate. ARDPP utilizes wavelength channel per link best but, at higher load than 60 Erlangs as shown before, the limitation of 16 wavelength channels per links is not enough for all three schemes with ARDPP suffering from connection blocking the highest.

As the network load increase, the overall consumption of network resources increase too as shown in Figure 8. AR used the less resource since no protection is implemented but this proves to be costly in terms of ASR. ARSPP is shown to outcome ARDPP in terms of network resource usage at all loads but this comes with the trade off of higher connection provisioning computation time needed.

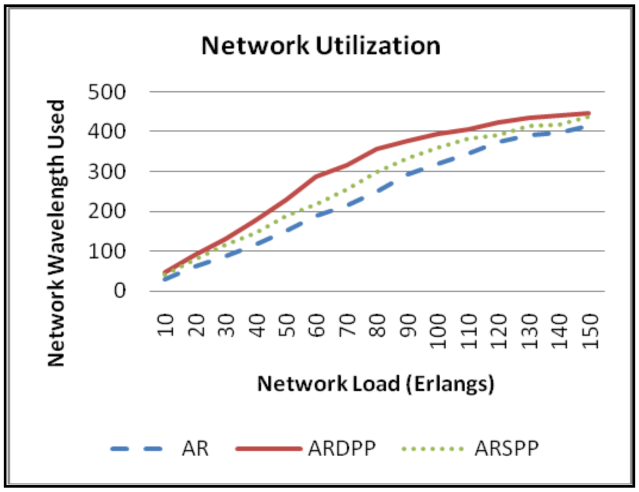

Fig.8 Network Utilization vs. Network Load

## 5. CONCLUSIONS

A comprehensive comparison of dedicated path protection and shared path protection is presented in this study. While both dedicated and shared path protection can offer perfect availability satisfaction ratio for WDM core networks services, this comes at the cost of increasing blocking probability and provisioning complexity with the increase of network load. Dedicated path protection has lower blocking probability and provisioning complexity compared to shared path protection. However, dedicated path protection has less resource usage efficiency than shared path protection as shown by the higher link and network utilization.

## 6. ACKNOWLEDGMENTS

The authors acknowledge the Ministry of Higher Education, Malaysia for the financial support through Fundamental Research Grant Scheme (FRGS) funding. The gratitude also goes to the administration of Universiti Teknologi Malaysia (UTM) especially for Research Management Centre (RMC) for the financial support through vote number 78540.

## 7. REFERENCES

[1] E. Bouillet and J. F. Labourdette, "Distributed computation of shared backup path in mesh optical networks using probabilistic methods," *IEEE/ACM Transactions on Networking*, vol. 12, pp. 920-930, 2004.

[2] H. Choi, *et al.*, "Loopback recovery from double-link failures in optical mesh networks," *IEEE/ACM Transactions on Networking*, vol. 12, pp. 1119-1130, 2004.

[3] R. He, *et al.*, "Dynamic service-level-agreement aware shared-path protection in WDM mesh networks," *Journal of Network and Computer Applications*, vol. 30, pp. 429-444, 2007.

[4] L. H. Liao, *et al.*, "Multicast protection scheme in survivable WDM optical networks," *Journal of Network and Computer Applications*, vol. 31, pp. 303-316, Aug 2008.

[5] L. Song, *et al.*, "Dynamic Provisioning with Availability Guarantee for Differentiated Services in Survivable Mesh Networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, April 2007.

[6] L. Song, *et al.*, "A Comprehensive Study on Backup-Bandwidth Reprovisioning After Network-State Updates in Survivable Telecom Mesh Networks," *Ieee-Acm Transactions on Networking*, vol. 16, pp. 1366-1377, Dec 2008.

[7] J. Zhang, *et al.*, "Backup Reprovisioning to Remedy the Effect of Multiple Link Failures in WDM Mesh Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, 2006.

[8] G. Xue, *et al.*, "Establishment of Survivable Connections in WDM Networks using Partial Path Protection," *Communications*, vol. 3, 2005.

[9] J. Zhang, *et al.*, "A new provisioning framework to provide availability-guaranteed service in WDM mesh networks," in *2003 International Conference on Communications (ICC 2003)*, Anchorage, AK, 2003, pp. 1484-1488.

[10]J. Zhang and B. Mukherjee, "A review of fault management in WDM mesh networks: Basic concepts and research challenges," *Ieee Network,* vol. 18, pp. 41-48, Mar-Apr 2004.

[11] M. Ali, "Shareability in Optical Networks: Beyond Bandwidth Optimization," *IEEE Communications Magazine,* vol. 42, 2004.

[12] A. Birman, "Computing approximate blocking probabilities for a class of all-optical networks," *IEEE Journal on Selected Areas in Communications,* vol. 14, pp. 852-857, 1996.

[13] S.-P. Chung, *et al.*, "Computing approximate blocking probabilities for large loss networks with state-dependent routing," *IEEE/ACM Transactions on Networking,* vol. 1, pp. 105-115, 1993.

[14] M. Kovačević and A. Acampora, "Benefits of wavelength translation in all-optical clear-channel networks," *IEEE Journal on Selected Areas in Communications,* vol. 14, pp. 868-880, 1996.

[15] C. Ou, *et al.*, "Subpath protection for scalability and fast recovery in optical WDM mesh networks," *IEEE Journal on Selected Areas in Communications,* vol. 22, pp. 1859-1875, 2004.

[16] A. Wason and R. S. Kaler, "Wavelength Assignment Problem in Optical WDM Networks," *IJCSNS International Journal of Computer Science and Network Security,* vol. 7, April 2007.

[17] D. Bisbal, *et al.*, "Dynamic routing and wavelength assignment in optical networks by means of genetic algorithms," *Photonic Network Communications,* vol. 7, pp. 43-58, 2004.

[18] S. Verbrugge, *et al.*, "General availability model for multilayer transport networks," Island of Ischia, Naples, 2005, pp. 85-92.