Security in All-Optical Networks: Failure and Attack Avoidance Using Self-Organization

Gerardo Castañón, *IEEE* Senior *Member,* Ivan Razo-Zapata, Carlos Mex
Raúl Ramirez-Velarde, and Ozan Tonguz*
Center of Electronics and Telecommunications, Tecnológico de Monterrey, Monterrey N.L., 64849, México
**Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213, USA*
Tel: (52)(81)8158-2293, e-mail: gerardo.castanon@itesm.mx

ABSTRACT
While transparent optical networks become more and more popular as the basis of the Next Generation Internet (NGI) infrastructure, such networks raise many security issues, which do not exist in traditional optoelectronic networks. The existing protection schemes which rely heavily on fault detection due to the use of network monitoring performed by the use of optoelectronic conversion at the switching nodes, is not sufficient to provide security assurance for all optical networks which lack the massive use of optoelectronic monitoring and require timely protection from malicious sabotage as well as inadvertent faults. In order to increase the security of future networks, them will need to use reactive mechanisms and self-organize through multipath routing (MPR) to protect themselves from potential failures caused by malicious new attacks and ordinary reliability problems. If we make the analogy to the human immunization system's primary defense mechanism, MPR will act as the primary defense mechanism reacting timely to network problems and evolving based on network information. In this paper we are proposing the use MPR as an instinct immediate network reaction to failures and attacks in transparent networks; after the nodes transmit the data and causes of failure are classified, better self organized decisions can be used based on changing routing output priorities to reach destination.

1. INTRODUCTION

Transparent all-optical networks (AON) are becoming more and more attractive due to their ability to reduce power consumption and cost based on the less use of transponders in the network, they can also avoid the bottleneck of optoelectronic conversion and switching at each node. However, transparency raises many security vulnerabilities as well as reliability issues which do not exist in traditional optoelectronic networks [1]. In WDM systems, multiple optical signals co-propagate in fiber and optical components, possibly affecting each other directly or indirectly. Then, the quality of a signal is sometimes dependent on or degraded by other signals. Moreover, in a transparent network, it is desired that signals are not regenerated between source and destination unless it is absolutely necessary [2]. It has been discussed in [3] how signals can be maliciously designed to pass through transparent components, causing undesirable effects at remote components and degrading other signals passing through the components. While there are many reliability studies to defeat physical layer impairment problems in AONs, these measures require human intervention to adapt the network to failures that are most likely to happen. Apart from component failures and accidental fiber cuts, networks are vulnerable to attackers capable of disrupting a network from the physical level up to the transport level. Usually, attackers are more interested in failures that can be repeated and controlled, especially if those created failures are rare. In addition, attackers may use automated software to repeatedly cause a fault far more often than it would occur otherwise. Attackers who artfully exploit well-known or newly discovered or unexpected vulnerabilities may circumvent the existing countermeasures. In order to increase the security of future networks we will need to imbed intelligence into the network such that they can continuously learn from the experience and self-organize to protect themselves from potential failures caused by malicious new attacks and ordinary reliability problems.

As the resource provisioning paradigm moves toward more dynamic regimes, the IP layer, which may be currently accessed by users or attackers, is directly placed on top of the WDM layer, and new emerging technologies comes into play, failure management has become a very important issue to offer a secure and resilient network. Meanwhile, many traditional protection strategies for optical networks would become insufficient with these trends, which rely on post-mortem detection and reaction against pre-informed vulnerabilities after the damage caused by failures. A complementary strategy is to handle unexpected failures and avoid potentially malicious or dangerous attempts before they are casted into attacks and begin causing damages. In particular, considering the high data rate on optical channels, a service disruption even for a short period of time would be disastrous. Thus, our strategy is based on two approaches: we are proposing the use of MPR as an instinct immediate network reaction to failures and attacks in transparent networks and after the nodes transmit the data and causes of failure are classified, better self organized autonomous decisions can be made based on changing routing output priorities to reach destination. In this paper, we present results which show how self-organization can help to achieve these goals.

978-1-4244-3485-5/08/$25.00 ©2008 IEEE

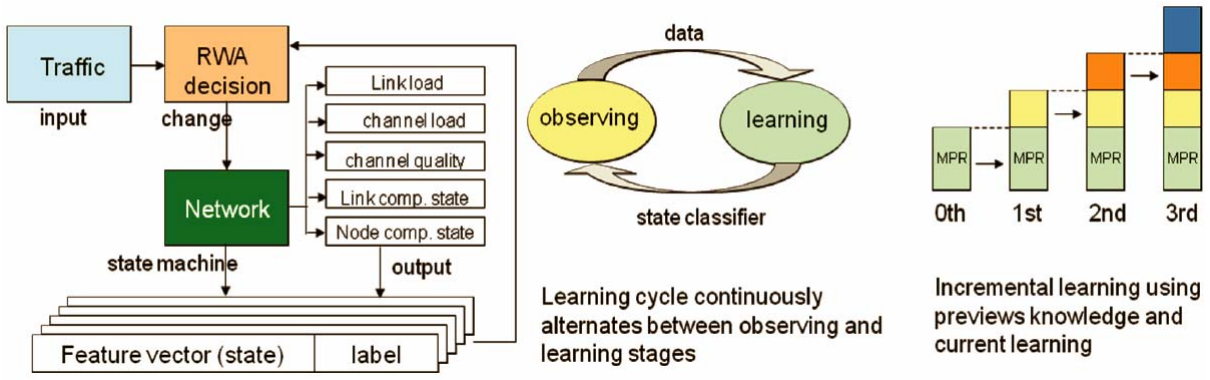
Authorized licensed use limited to: Tec de Monterrey. Downloaded on February 5, 2009 at 13:01 from IEEE Xplore. Restrictions apply.

The rest of the paper is organized as follows. In Section 2, we briefly identify the threats of concern in AONs, and discuss existing countermeasures. In Section 3, we describe how a network can learn to self-organize to reduce potential failures in the future. In Section 4, we demonstrate how a wavelength failure or attack can be avoided with self-organization via simulation experiments.

2. THREATS AND RELATED WORK

In this paper, we focus in such cases where the goal of attacks is disruption or degradation of service by exploiting physical layer impairments. An attacker may directly inject malicious signals from compromised optical components or manipulate components, which may affect information-bearing signals. Such an attack requires full access to the components (including physical access and the control software of the components). However, optical components such as cross-connects are typically locked in a secure facility with restricted access. Therefore, one might consider such a direct attack unlikely, but insiders have all the capability. Past experiences show that the computer related crimes by insiders (i.e., employees of a company as well as ex-employees and partners) are as significant as those coming from outsiders [4].

Furthermore, as the IP-over-WDM vision comes true, the control of IP and WDM layers are being merged. In supporting the merged control efficiently, IP and WDM components may become integrated as well. In such a case, it is also likely that the management of IP and WDM layers becomes merged. The more tightly merged they are, the more risk is shared between IP and WDM layer. As the network size grows and equipments become sophisticated, many device vendors also provide management systems that can be remotely operated by automated management software. However, such software is often found vulnerable and can be exploited for attacks on network infrastructures [1].



(a) (b)

Figure 1. (a) Self-organizing mechanism: The network is modeled as a state machine. The approximate functional relationship between states and outputs of the state machine is learned, and then used to make routing decisions. (b) Learning cycle continuously alternates between observing and learning stages and incremental learning using current and previous data observing and learning stages.

Network security countermeasures are categorized into three types of practices: *prevention, detection and reaction*. Since attacks are achieved via physical layer impairments, limiting the physical layer vulnerabilities is of common interest in both reliability and security researches. In transparent optical networks, prevention schemes that aim to reduce vulnerabilities include network design, component design, provisioning, and operational regulations, etc. In general, two approaches exist to assure reliable optical channels in the presence of physical layer impairments: the routing constrained by estimated physical layer impairments and the network architecture design to guarantee the service quality in every possible case in the given network and traffic demand [5]. While these measures are more adequate to guarantee the strict sense of reliability under a given condition, they lack the capability of adaptation to network expansion, component upgrade or aging, and creative attacks. In addition, they tends to prepare for the worst case when various effects are involved while limiting the utilization, or focus on a limited set of impairment effects which are most likely to happen spontaneously while being unprepared for the unexpected. On the other hand, the agile adaptation to network faults, network changes, and creative attacks is crucial for perpetual availability, which is not provided in many cases when human intervention is required. Our goal is to address this problem with autonomous adaptation against new vulnerabilities and the effective recognition of risk. Monitoring and detection methods in AONs are discussed in [6]. Failure location algorithms which provide a framework to locate faults and attacks in AONs also exist [7,8].

Authorized licensed use limited to: Tec de Monterrey. Downloaded on February 5, 2009 at 13:01 from IEEE Xplore. Restrictions apply.

3. DESIGN AND IMPLEMENTATION

The purpose of self-organization is that if a network experiences significant physical layer impairment problems in certain network conditions, it learns them, and then tries to keep away from any of such conditions or unforeseen but similar conditions which are expected to produce similar or worse performance. For example, instead of blindly using the first-fit route we propose to use a flexible multi-path routing (MPR) scheme, which chooses the safest path, satisfying the packet or the burst of packets. It is well known that multi-path routing has many benefits, such as decreasing the number of components in an all-optical network, decreasing the use of optical memory (fiber delay lines) at the routers, decreasing the use of wavelength converters, provides a quick way to solve contention of packets, faults, and attacks using an alternate routing [9,10]. Multi-path routing uses a packet forwarding output link table with several output link options ordered by priority. Initially this forwarding table may be created using the k-shortest paths based on the minimum hop routing. For example in case of a packet conflict, one of the packets will be forwarded through the output link with the best priority and the second packet can be forwarded through the output link with second priority in case the node does not count with other contention resolution mechanism as optical memory and wavelength conversion. The node's forwarding routing tables can be continuously self-organizing based on the conditions of the network of the state machine and using routing algorithms that update the forwarding tables based on the different faults or attacks the network may suffer. The key difference from the previous works is that such intelligence is obtained nether with human intervention nor with instantaneous detailed knowledge of the network component subsystem, besides is able to self-organize autonomously as the network changes. We use supervised machine learning approach for pattern classification to support this. If we make the analogy to the human immunization system's primary defense mechanism, Multi-path routing will act as the primary defense mechanism reacting timely to network problems and evolving based on the network information. Basically we are proposing the use of MPR as an instinct immediate network reaction to failures and attacks in transparent networks and after the nodes transmit the data and causes of failure are classified, better routing decision can be used based on changing routing output priorities to reach destination. In this case routes will be continually updated based on the state of the network. Here, we define a network as a ***state machine***, where the current ***state*** of a network is defined as the current set of wavelength usage status on each link in the network and supplemental important information as the state of node and link components. Since intelligence is distributed, every node has to send information to all other nodes of the network about the state of the wavelengths, state of the fibers, and state of the links components and state of the nodes components. It is important to mention that we assume a link comprises several transmission fibers and in the same way a fiber comprises several wavelengths.

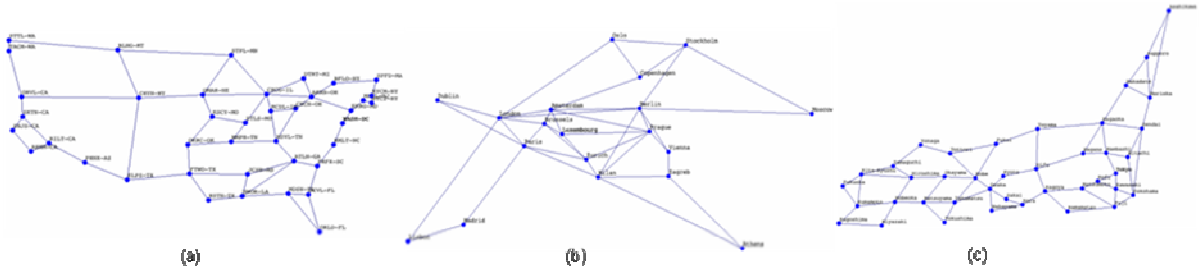


Figure 2. Topologies used in the analysis, a) USA topology, b) European topology and c) Japanese topology.

We assume that complete bit error rate (BER) statistics are available for every incoming wavelength at a node. In practice all-optical networks will require BER monitoring at every node. This BER monitoring can be performed by the receivers that read the header of the incoming packets in case the packet information travels in band before the packet's payload [11]. If header information is transmitted out of band in order to avoid the header reader detectors, BER monitoring can be performed splitting the signal power by a coupler and at one of the coupler output a tunable optical filter before the BER monitoring receiver. Using this last scheme, the BER monitoring can be done sequentially tuning the filter to every incoming wavelength of the fiber.

Fig. 3 shows results of the average packet lost against simulation time. Figures 3(a) and 3(b) are results for the USA topology using shortest path routing and MPR. Figures 3(c) and 3(d) are results for the European topology using shortest path routing and MPR. Figures 3(e) and 3(f) are results for the Japanese topology using shortest path routing and MPR. Solid lines are results when there is no wavelength failure, dashed lines are results when one wavelength in a fiber is failing, dashed doted lines are results when two wavelengths in a fiber are failing, doted lines are results when three wavelengths in a fiber are failing and crosses are results when all wavelengths in a fiber are failing.

To compute the statistics presented in Fig. 3 we collected data for 5000 clock cycles during the steady-state period. To be sure that the simulation was in steady state at the time we started the computation, we compared the mean number of packets injected into the network per time slot (injection throughput) with the mean number

Authorized licensed use limited to: Tec de Monterrey. Downloaded on February 5, 2009 at 13:01 from IEEE Xplore. Restrictions apply.

of packets going out of the network per time slot (absorption throughput) plus the mean number of packets lost in the network per time slot (lost throughput) after the transient period. For every probability of packet injection, we obtained a small difference of the order of 10^{-2} between the injection throughput and the sum of absorption throughput and lost throughput.

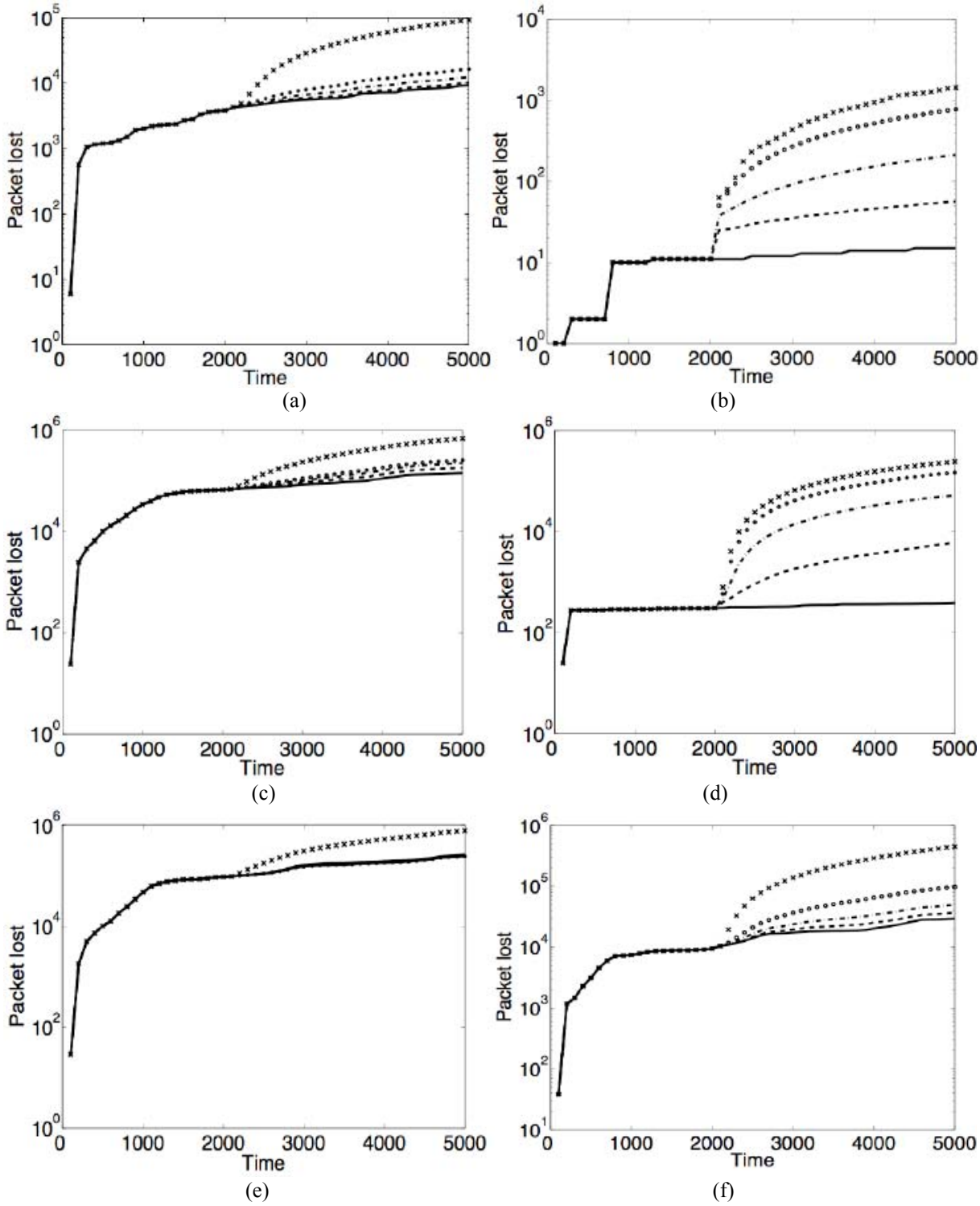


Figure 3. Results of the average packet lost against simulation time. (a) and (b) are results for the USA topology using shortest path routing and MPR. (c) and (d) are results for the European topology using shortest path routing and MPR. (e) and (f) are results for the Japanese topology using shortest path routing and MPR. Solid lines are results when there is no wavelength failure, dashed lines are results when one wavelength in a fiber is failing, dashed doted lines are results when two wavelengths in a fiber are failing, dots are results when three wavelengths in a fiber are failing and crosses are results when all wavelengths in a fiber are failing.

Authorized licensed use limited to: Tec de Monterrey. Downloaded on February 5, 2009 at 13:01 from IEEE Xplore. Restrictions apply.

The network resources dimensioning was limited in order to allow some loss of packets and observe the advantages of using MPR as the routing platform. However, the same network resources were used when shortest path (SP) routing and MPR were applied. Note that when MPR is used the number of packet lost is lower compared to SP. Also note that when wavelength failure is produced at time 2000 MPR produces much less losses of packets compared to SP. Note in Fig. 3*a* and 3*b* that when four wavelengths fail the maximum packet lost in MPR is in the order of about 1000 and for the case of SP the packet lost is in the order of 10^5-10^4 approximately 90000 packet lost.

As depicted in Fig. 3*c*-*d*, benefits from the use of MPR still can be observed for simulations where packet lost is higher than those presented in Figure 3*a* and 3*b*. In the event of no failure, MPR offers a reduction of packet lost in the order of 10^2 compared to SP using same network resources, as shown in Fig. 3*c* and 3*d*. When wavelength failures are produced, use of MPR again gives advantages over SP delivering an instinct way to self-organize to overcome the failures.

Finally, in Fig. 3*e-f* similar results as those presented in previous figures can be observed. Despite of a slight increase of packet lost for steady state for both, SP and MPR, the results still show that MPR performs better than SP. Note in Fig. 3*c* that for SP the difference of packet lost when the number of wavelengths that fail in a fiber ranges from 1 to 3 is negligible. Besides, the gain for MPR over SP is not as high as seen in Fig. 3*a*-*b* when all wavelengths in a given fiber fail, these results can be explained pointing out the difficulty of routing packets when the network resources are more limited if compared with the simulations reported in Fig. 3a-*b*. Therefore network resources dimensioning is an issue when self-organizing is carried out.

4. CONCLUSIONS

In this paper, we have shown that MPR working as an instinct immediate network reaction to failures and attacks in transparent networks is a very promising direction for providing security protection in future transparent optical networks. Most of the current reliability approaches are not effective enough to keep up with newly emerging vulnerabilities and continuously evolving attacks. On the other hand, the self-organizing network autonomously and persistently adapts to network changes by learning newly exposed vulnerability patterns and obviates the exploitation of the vulnerabilities that are discovered so far as well as the ones that are not encountered yet but similar. Our preliminary results show that a self-organizing network can provide powerful defense mechanisms by limiting the attack capability of hostile parties. We are currently investigating how self-organization can count in the packet blocking issue. The self-organization capability is provided via machine learning techniques. In this paper, we present results with simple vulnerability and attack scenarios in order to demonstrate how the self-organization helps to adapt against new vulnerabilities and avoid attacks. Our future work will also include further improving the self-organization intelligence by using more efficient learning techniques and also network dimensioning to improve performance.

REFERENCES

[1] J-S. Yeom, O. Tonguz, and G. Castañón: Security in All-Optical Networks: Self Organization and Attack Avoidance, in *Proc. ICC 2007*, pp. 1329-1335, June 2007.

[2] G. Castañón: Performance requirements for all-optical networks, in *Proceedings SPIE, Conference on Optical Transmission Systems and Equipment for WDM networking III*, vol. 5596-18, pp. 127-134, Philadelphia, USA, October 2004.

[3] M. Medard, D. Marquis, and S. R. Chinn: Attack detection methods for all-optical networks, in *Network and Distributed System Security Symposium*, 1998.

[4] CSI/FBI, computer crime and security survey 2000-2004. [Online]. Available at: http://www.gocsi.com.

[5] I. Tomkos, et al.: Performance engineering of metropolitan area optical networks through impairment constraint routing, *IEEE Communications Magazine*, vol. 42, no. 8, pp. S40–S47, Aug. 2004.

[6] D. C. Kilper, et al.: Optical performance monitoring, *IEEE/OSA Journal of Lightwave Technology*, vol. 22, no. 1, pp. 294-304, Jan. 2004.

[7] C. Mas, I. Tomkos, and O.K. Tonguz: Failure location algorithm for transparent optical networks, *IEEE Journal on Selected Areas of Communications, Special Series on Optical Communications and Networking*, vol. 23, no. 8, pp. 1508-1519, Aug. 2005.

[8] R. Bergman, M. Medard, and S. Chan: Distributed algorithms for attack localization in all-optical networks, *Network and Distributed System Security Symposium*, session 3, paper 2, 1998.

[9] G. A. Castañón, L. Tancevski and L. Tamil: Optical packet switching with multiple path routing, *Journal of Computer Networks and ISDN Systems, Special Issue on Optical Networks for New Generation Internet and Data Communication Systems*, vol. 32, pp. 653-662, 15 May 2000.

[10] F. Callegati, W. Cerroni, C. Raffaelli: Routing techniques in optical packet switched networks, in *Proc. ICTON 2005*, Tu. A1.1.

[11] G. A. Castañón, US6,810,211, B1. Preferred WDM packet switched router architecture and method for generating the same, October 2004.

Authorized licensed use limited to: Tec de Monterrey. Downloaded on February 5, 2009 at 13:01 from IEEE Xplore. Restrictions apply.