ALL OPTICAL NETWORK-A NEW APPROACH FOR SECURITY

[1]K. Kajendran, [2]K.Balaji, [3] N. Siva kumar

[1]Associate Professor, Department of M.C.A, Panimalar Engineering College, Chennai

[2]PG Scholar, Department of M.C.A, Panimalar Engineering College, Chennai

[3]Asst Professor, Department of M.C.A, Panimalar Engineering College, Chennai

INTRODUCTION

The best way of accommodating the intensively growing network traffic and satisfying the ever tighter demands on throughput, delay and overall network performance is by using optical fiber technology. Optical fiber is characterized by huge bandwidth of up to 50 THz, low BER of 10 12 low loss of down to 0.2 dB/km and low noise and interference characteristics. The best way of exploiting this immense potential is by dividing it among independent sets of different wavelengths, which is the underlying principle of Wavelength Division Multiplexing (WDM). Each wavelength supports one communication channel, operating independently at an arbitrary speed. Independently modulated wavelengths are all multiplexed and carried simultaneously over the same physical fiber. Transparent Optical Networks (TON) enable all-optical channels, called light paths, to be established between any pair of nodes

ROUTING AND WAVELENGTH ASSIGNMENT

The Routing and Wavelength Assignment problem consists of two sub problems: finding the physical routes for the given lightpath demands in the Routing (R) part of the problem, and assigning a wavelength to each of them in the Wavelength Assignment (WA) subproblem. Most common objectives ofthe RWA process include minimizing the number of physical hops in the established light paths or light path congestion (R), or minimizing the number of wavelengths used (WA). The wavelength assignment problem is subject to two main constraints. The wavelength clash constraint prohibits assigning the same wavelength to light paths which traverse a common directed physical link while the wavelength continuity constraint ensures each light path is assigned the same wavelength along its entire physical path. This constraint is relaxed when wavelength converters are available, but they are not yet economically viable. There are three variations of the RWA problem. In the static case, all demands are known in advance and the virtual topology does not change over time.In scheduled RWA, their set up and holding times are known in advance, and in the dynamic case they arrive unexpectedly with random

holding times. For small-sized problems, exact solutions of the RWA problem can be found by, for example, formulating the problem as an integer linear program. Larger network instances, however,require heuristic approaches, such as those from [1], [2], [3] and [4]. The RWA problem has been shown to be NP-complete[5], so the Routing (R) and Wavelength Assignment (WA) subproblems are often solved subsequently.

ROUTING SUBPROBLEM

Given the physical network topology, i.e., set of nodes interconnected with physical links, and a set of lightpath demands, solving the Routing subproblem consists of finding a physical route for each of the lightpaths demands. Some of the commonly used approaches include [4]:

1) **FIXED ROUTING** - A lightpath demand between the same source node s and destination nodes d is always routed on the same, precalculated path, e.g. the shortest connecting path.

2**) FIXED ALTERNATE ROUTING** - The route of the lightpath is chosen among several possible routes to the destination, which are all kept in the source node's routing table. The default route is called 'primary', and it is usually the one corresponding to the shortest path. The term 'alternate route' may describe a route which is link-disjoint to the primary path, or it may be a general term for all available routes between the source and destination node.

3) **ADAPTIVE ROUTING** - The route between the source and destination is chosen dynamically, taking into consideration the changing network state. For example, the chosen route may be the shortest-cost path, i.e., the path which yields the lowest cost in a network with wavelength converters. Another example is the least-congested path routing, where the least congested route among the precalculated routes is chosen.

4) **FAULT-TOLERAT ROUTING** - In order to improve network robustness against link and node failures, we can ensure

backup capacity for the potentially affected traffic by reserving two link- and/or node-disjoint paths for a pair of end node

THE WAVELENGTH ASSIGNMENT SUBPROBLEM

After finding a physical route for each of the lightpath demands, the wavelength assignment subproblem consists of assigning a wavelength to each of them subject to the wavelength continuity and clash constraints. Wavelength Assignment has been shown to be equivalent to the NP complete graph coloring problem [6] and, as such, requires heuristic approaches.

1) **FIRST FIT**- Wavelengths are indexed in sequential order. Each lightpath is assigned the wavelength with the lowest index which is available on all of the physical links included in the lightpath's path. A lightpath is assigned a wavelength with an index higher than any other used wavelengths in case when none of the already used wavelengths can accomodate it.

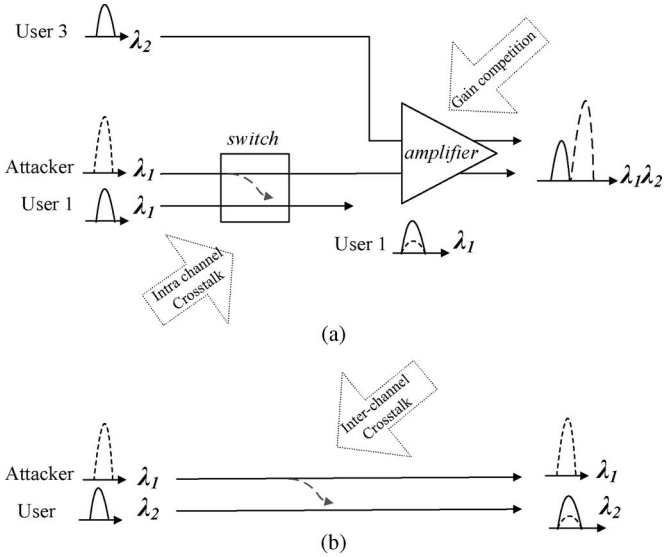
2) **Least-used/SPREA**D - In order to balance the load among wavelengths, each lightpath is assigned the wavelength which is the least used in the network. This method performs poorly in terms of blocking probability.

3) **Most-used/PACK** - Each lightpath is assigned the available wavelength which is the most used in the network.
This method tends to pack lightpaths into the smallest possible number of wavelengths, minimizing the wavelength usage for future network needs.

4) **RANDOM** - Each lightpath is assigned a random wavelength among those which can

accomodate the request.
In recent years, the research community has given much
attention to impairment-aware RWA approaches aimed at
minimizing the degradation of the quality of transmission
caused by physical-layer impairments. Namely, the intensity
and effects of many physical-layer impairments greatly depend
on the specific method of network planning [7], and their
impact can be diminished or compensated for through careful
network planning approaches.

Fig.. (a) Gain competition in amplifiers and intrachannel crosstalk in switches.
(b) Interchannel crosstalk in fibers.



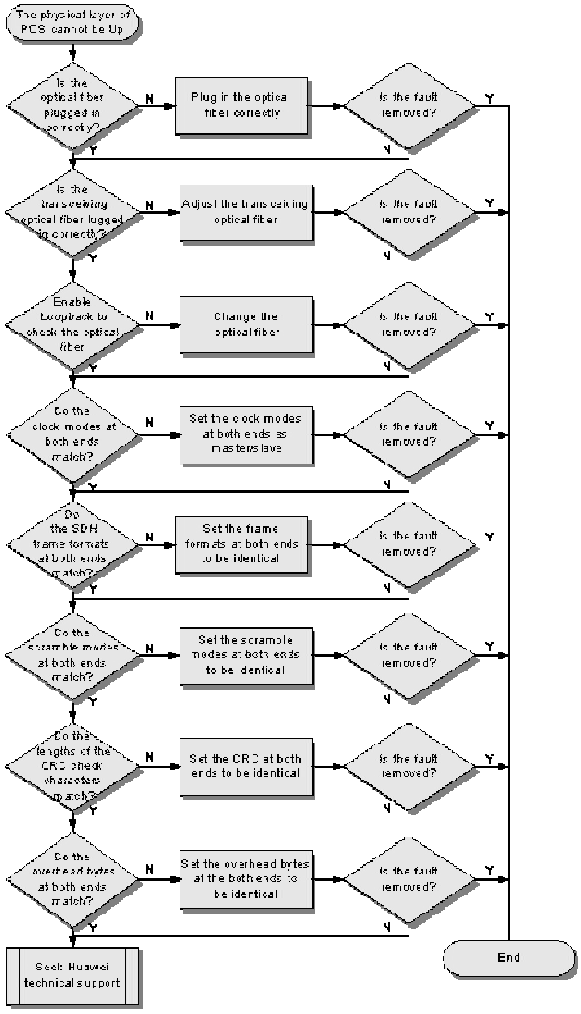


Fig: flowchart for physical layer attacks in optical fiber

ATTACK CLASSIFICATION

Distinguish two general types of security: physical and semantic. Physical security ensures that the data have a minimum privacy and quality of service (QoS), and that the users are informed when such conditions are violated. Semantic security protects the meaning of the data even if it has already been reached by an attacker, and it belongs to the domain of cryptography. As described in [10], [11], [12], depending on the goal of the attacker, network attacks can be broadly categorized into :

1) Service disruption, which prevents communication or degrades the quality of service (QoS), and

2) Tapping, which compromises privacy by providing unauthorized users access to data, which can then be used for eavesdropping or traffic analyses.

When it comes to physical-layer attacks, the authors in discern three categories:

> **Direct attacks**. Characteristics of certain physical link elements are more likely to be intruded and exploited as direct attack ports.
> Such attacks include:

Attacks aimed at network transmission: tapping, tapping and jamming following signal processing, jamming only. Attacks aimed at optical amplifiers: gain competition due to local or remote attacks, crosstalk.
Attacks aimed at optical transmission: fiber cut.

> **Indirect attacks**. Certain network elements are more likely to be attacked indirectly, because it is too complicated to attack them directly, or they are not easily accessible.

This type of attacks include:

Indirect crosstalk
Unauthorized access through add/drop ports
Intentional crosstalk propagation from preceeding blocks

3) Pseudo-attacks - anomalies which are not intrusions, but may be interpreted as such, due to significant changes in the signal quality depending on the physical
network design.

There are many other ways of classifying attacks. For example, each attack can be classified by its resources (passive or active), its means of attack (transmission/reception,protocol, control system), the target (specific users or network/subnetwork), the intended effect (service disruption or tapping), the location of the attack (terminal, node, link, multiple locations), and the attacker's willingness to be discovered in an economically more viable way.

ALGORITHM

TABU SEARCH:

Tabu search is an iterative meta-heuristic that guides simpler search procedures through various areas of the solution space preventing them from remaining in local optima. In each iteration, the search begins with a current solution, explores all its neighboring solutions, and chooses the best neighboring solution (which is not forbidden by the tabu list) to become the current solution in the next iteration. A tabu list is a memory structure specific to tabu search that "memorizes" a certain number of previously visited solutions to prevent the algorithm from cycling and getting stuck in local optima. Potential solutions are evaluated with respect to a certain fitness function. After a desired number of iterations, the algorithm terminates, and the bestfound solution is deemed the final result.

Tabu search was chosen since it was shown to give results for the RWA of scheduled lightpath demands in [3]. Wavelength assignment is solved subsequently using the graph coloring algorithm from

PROPOSED SYSTEM

To address the existing problem, we propose a novel approach to optical networks security that is aimed at minimizing the potential damage caused by physical-layer attacks. Our goal is to achieve significant prevention measures without the need for specialized equipment, i.e., at minimal extra cost, through careful network planning. Namely, we propose to consider the potential consequences of physical-layer attacks while solving the RWA problem.

The aim is to arrange the set of lightpaths in such a way as to minimize the possible disruption caused by various attack scenarios, i.e., minimize the maximum number of lightpaths that can be disrupted in such situations. Consequently, if fewer lightpaths are attacked, not only is network service disruption reduced, but failure detection and localization algorithms can be faster since they search for the source among fewer potential lightpaths. This extends our preliminary work, which introduced the problem and provided an initial version of the solution approach. To the best of our knowledge, attacks have not yet been considered in the literature in the context of routing and wavelength assignment.

MODULES USED

i. SOURCE MODULE
ii. LISTENER MODULE

LOGIN:

Authorized user only can allowed to access.
By the way of providing username and password

SOURCE MODULE:
This module contains a login page for authentication purpose. This module provides facilities to select the current workgroup of the source system. Once the workgroup is realized the workgroup collection is navigated to find the active nodes that can be reached from the source. After mentioning the nodes position in the network and a source node, the module works on the other nodes in the network to work out and reduce the maximum lightpath attack radius during transmission from the source to the destination. Then a data entered into an input field is transmitted from source to destination via the path with maxLAR reduction.

LISTNER MODULE:

The Listener module receives data from source module or another listener module. If the listener module is represents the destination node then it provides a mean to persist the data in the node and hence stops the data transmission process. Else, if the listener module represents an intermediate node then, it retransmits the data received to the next node in the transmission path.

PERFORMANCE ANLAYSIS

The reason behind using different traffic classes is due to the observation that subscribing content providers can be highly heterogeneous in terms of their traffic patterns and the type of content they handle. Hence, end-users request for content of varying sizes (ranging from small to large). The processing requirements also vary based on size of the content requested. The use of different traffic types allows us to reflect different user preferences and content request types.

After using available number of resources in the current site based on the additional demand given by the users. The user shares the media and the details are stored in database. We can generate the report and display from the database.

CONCLUSION:

The vulnerabilities of optical network fundamental physical components, as well as the attack techniques that exploit them combined with the transparency property of emerging all optical networks demand new, specific ways of attack detection, localization and network restoration. Besides upgrading existing ways of dealing with network failures and attacks and developing new ones, significant attention should be paid to prevention mechanisms, by taking physical layer impairments and attacks that exploit them into consideration already in the network planning phase. This approach, i.e., prevention oriented network planning is a new concept which may play a significant role in increasing the all-optical network security in an economically more viable way

REFERENCES:

1. H. Zang, J. P. Jue and B. Mukherjee, “A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks,” Optical Networks Magazine, vol. 1, pp. 47–60, January 2000.

2. I. Chlamtac, A. Ganz and G. Karmi, “Lightpath communications: an approach to high-bandwidth optical WANs,” IEEE Transactions on Communications, vol. 40, pp. 1171–1182, 1992.

3. R. Ramaswami and K. N. Sivarajan, “Optical Networks: A Practical Perspective,” 2nd edition, R. Adams, Ed., San Diego: Academic Press, 2002, pp. 437–488.

4. T. Song, H. Zhang, Y. Guo and X. Zheng, “Statistical Study of Crosstalk Accumulation in WDM Optical Network Using Different RWA,” Optics Communication 202, pp. 131–138, 2002.

5. S. Azodomolky, M. Klinkowski, E. Marin, D. Careglio, J. Sol´e Pareta and I. Tomkos, “A survey on physical layer impairments aware routing and wavelength assignemnt algorithms in optical networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 53, no. 7, p. 926–944, May 2009.

6. C. C. Saradhi and S. Subramaniam, “Physical Layer Impairment Aware Routing (PLIAR) in WDM Optical Networks: Issues and Challenges,” IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 109–130, 4th quarter 2009.

7.M. M´edard, D. Marquis, R. A. Barry and S. G. Finn, “Security Issues

in All-Optical Networks", IEEE Network Magazine, vol. 11, no. 3, pp. 42–48, May 1997.

8. T. Wu and A. K. Somani, "Cross-Talk Attack Monitoring and Localization in All-Optical Networks," IEEE/ACM Transactions on Networking 13, pp. 1390-1401 (2005).

9. M. M´edard, D. Marquis, S. R. Chinn, "Attack Detection Methods for All-Optical Networks", in in Proc. of Network and Distributed Systems Security Symposium, Session 3, paper 2, San Diego, California, 1998.

10. J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam and H.-A. Choi, "A Framework for Managing Faults and Attacks in WDM Optical Networks," Proc. of the DARPA Information Survivability Conference and Exposition, Anaheim, California 2001.

11. C. Mas, I. Tomkos and O. K. Tonguz, "Failure Location Algorithm for Transparent Optical Networks,", IEEE Journal on Selected Areas in Communication, vol. 23, no. 8, pp. 1508–1519, August 2005.

12. T. Deng and S. Subramaniam, "Covert low-power QoS attack in alloptical wavelength routed network," in Proc. of IEEE Global Telecommunications Conference (GLOBECOM)vol. 3, pp. 1948-1952, 200