INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Strike Consciousness: An Intelligent Perspective To Optical Network Security

Sameena Sarwath[1], Raafiya Gulmeher[2]

[1]M.Tech Student,
Dept of Computer Science & Engg,
Khaja Banda Nawaz College of Engineering,
Gulbarga, Karnataka, India
sameenasarwath12@gmail.com

[2]Assistant Professor
Dept of Computer Science & Engg,
Khaja Banda Nawaz College of Engineering,
Gulbarga, Karnataka, India

Abstract**:** *In case of an attack most approaches are focused on developing fast detection and reaction mechanisms. In particular, considering Security issues and attack management in transparent wavelength division multiplexing (WDM) optical network where the high data rates are involved and also the vulnerabilities associated with its transparency such as deliberate physical-layer attacks by high-powered jamming, which can seriously degrade network performance and requires dealing with efficiently, we propose a novel approach to help deal with these issues in the network planning and provisioning process as a prevention mechanism rather than the general detection and reaction mechanism. Here we propose to route lightpaths in such a way as to minimize the potential damage caused by various physical-layer attacks. In the initial step of routing and wavelength assignment (RWA) problem, we make use of a criteria called the maximum Lightpath Attack Radius (maxLAR) and formulate the routing subproblem as an integer linear program (ILP). We tested it on small networks to get an insight into its complexity and comparing it to a formulation that minimizes congestion .Results indicate that our formulation achieves significantly better results for maxLAR obtaining near-optimal or optimal congestion in all cases. Coming to larger networks, we propose a tabu search algorithm for attack-aware lightpath routing, in combination with an existing graph-colouring algorithm for wavelength assignment. This approach thereby provides superiority with respect to maxLAR and average lightpath load, albeit at the expense of somewhat higher congestion. However, this is justified with the obtained improvement in network security.*

Keywords: *Integer linear programming (ILP), physical-layer attacks, routing and wavelength assignment (RWA), tabu search, transparent optical networks.*

1. INTRODUCTION

Transparent optical networks based on wavelength division multiplexing (WDM) can exploit the huge capacity of optical fibers by dividing it among different wavelengths. As such, they have been established as the enabling technology for today's high-speed backbone networks, meeting consumers' ever-increasing bandwidth demands. In wavelength-routed or transparent optical networks, all-optical connections, called lightpaths, are established between pairs of nodes. Transmission along a lightpath is entirely transparent, i.e., with no optoelectronic conversion at intermediate nodes. The set of established lightpaths is referred to as the virtual topology and is used to route the higher layer traffic.

1.1 The Routing and Wavelength Assignment (RWA) Problem

One of the most important challenges in transparent optical networks planning and provisioning is successfully solving the routing and wavelength assignment (RWA) problem. Given a physical topology and a set of lightpath demands, the RWA problem consists of finding a physical route for each lightpath demand and assigning to each route a wavelength, subject to the following constraints. If no wavelength converters are available, the same wavelength must be assigned along the entire lightpath (i.e., the wavelength continuity constraint). Furthermore, lightpaths that share a common physical link cannot be assigned the same wavelength (i.e., the wavelength clash constraint). Demands to set up lightpaths between certain nodes can be known a priori and set up semi permanently (static case), can be established according to a predefined schedule (scheduled case), or can arrive unexpectedly with random holding times (dynamic case). Several variations of the problem have been considered such as RWA with a limited or unlimited number of wavelengths in networks with wavelength converters at each node, at a subset of nodes, or in networks with no wavelength converters. Common objectives include minimizing the number of wavelengths used, maximizing the number of lightpaths successfully set up subject to a limited number of wavelengths, or minimizing the congestion (i.e., the maximum number of lightpaths routed over any one physical link in the network) for the static or scheduled cases. Minimizing the blocking probability is the most common objective for the dynamic case. The RWA problem has been shown to be NP-complete [1]. Thus, several heuristic approaches have been developed to help solve it sub optimally. Examples of heuristic

algorithms that efficiently solve the RWA problem for static, scheduled, and random dynamic lightpath demands can be found in [2]–[4], respectively, and references therein. Furthermore, some approaches consider physical impairments such as accumulated crosstalk and noise, which add new constraints and/or objectives to the problem, such as a limited bit error rate (BER) [5].

1.2 Security Issues and Motivation

The key advantage of transparent optical networks lies in their transparency, enabling high-speed connections with no optoelectronic conversion at intermediate nodes. However, transparency imposes several vulnerabilities to network security. The difficulty in detecting and locating failures (both component faults and deliberate attacks) is enhanced since monitoring must be performed in the optical domain. In general, fault and attack management consists of prevention, detection, and reaction mechanisms [6].

- Prevention mechanisms in transparent optical networks usually include hardware measures aimed at overcoming the physical vulnerabilities of optical components. Examples include alarming the fiber in case of tampering, or incorporating automatic gain control and power limiting amplifiers to thwart power-jamming attacks, which will be described in the next section. However, the efficiency of these approaches are a trade-off with the high price of such equipment.
- Detection techniques(eg: [7] & [8]) aim at detecting and localizing attacks based on information received from specialized optical monitoring equipment, which can be quite expensive. Thus, full monitoring capabilities cannot realistically be assumed at all nodes.
- Reaction mechanisms restore the proper functioning of the network by isolating the source of the failure and reconfiguring the connections. Such techniques can use preplanned backup paths or reactive rerouting schemes, creating a trade-off between speed and utilization of network resources.

In general the higher the reliability performance required the more spare resources are needed and, consequently, the higher the cost of the network equipment involved.

In this paper, 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 from [10] and [11], which introduced the problem and provided an initial versionof the solution approach.

2. RELATED WORK

Attacks in Transparent Optical Networks

Once a set of lightpaths is established via RWA, successfully maintaining it with efficient fault and attack management is critical to secure network operation. Attacks can be particularly malicious due to their ability to appear sporadically and propagate through the network as a result of lightpath transparency. Consequently, they can cause system-wide service disruption and are much harder to locate than component faults. Various physical- layer attacks can be performed, either by an internal attacker with access at a legitimate network node, or by an external one with physical access to a part of the fiber. In the latter case, an attack can be realized by bending the fiber slightly and radiating light into it, without otherwise disrupting the fiber, making it very hard to localize[6] .Here, we briefly review some typical attack scenarios in order to illustrate the vulnerabilities associated with transparent optical networks (TONs).

Erbium-doped fiber amplifiers (EDFAs), the most commonly used amplifiers in TONs, have a finite amount of gain available (a limited pool of upperstate photons), which is divided among the incoming signals. Thus, by injecting a high-power jamming signal within the amplifier passband, an attacker can exploit *amplifier gain competition* to both deprive other signals of power and increase its own power. An example of this is shown in Fig. 1(a). Some amplifiers may be equipped with automatic gain control functionality that can suppress gain dependence on input power, but such equipment can be expensive. However, most currently available amplifiers do have power monitoring functionality that can send an alarm in case abnormally high power is detected. Although this can trigger localization and reaction mechanisms, significant damage can already be done by the time these mechanisms react and restore proper functioning of the network. Furthermore, jamming signals can be injected sporadically, appearing for very brief intervals, making restoration even more difficult.

An attack scenario, referred to as a low-power quality-of-service (QoS) attack, which can cause damage even in networks equipped with automatic gain control amplifiers, is described in [13]. It is achieved by attaching a splitter at the head of a link to attenuate propagation power by a certain amount. Since the amplifiers are placed such that they compensate only for the losses on the previous fiber span, the induced attenuation can significantly degrade the performance metrics of attacked lightpaths. Furthermore, such an attack can propagate if there is optical cross connect (OXC) equalization at the network nodes. Namely, lightpaths sharing links with the attacked signal on links downstream of the attacking point are attenuated to ensure a flat power spectrum. In such a network, a high-powered jamming signal could not propagate, but a low-powered QoS attack could.

Another vulnerability of optical networks is significant crosstalk exhibited in optical switching nodes. In wave length-selective switches, channels on the *same* wavelength

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

can interfere with each other causing *intrachannel crosstalk* [Fig. 1(a)]. Furthermore, long distances and high-power signals can introduce nonlinearities in fiber causing *interchannel crosstalk* effects between signals on different wavelengths [Fig. 1(b)]. In this case, a high-power jamming signal injected on a link can interact with other channels via nonlinear effects (e.g., four-wave mixing, cross-phase modulation, Raman gain effects) and cause damage even if it is removed with a filter at the end of the fiber span.

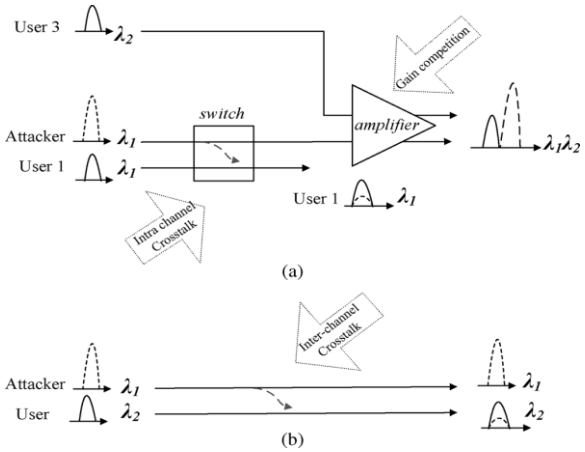

Figure 1: (a) Gain competition in amplifiers and intrachannel crosstalk in switches. (b) Interchannel crosstalk in fibers

An even more malicious attack can be achieved by slightly bending the fiber to tap part of a signal, and then inject noise at the tapping point to achieve both eavesdropping and degradation of the signal-to-noise ratio (SNR) on the attacked channel (*correlated jamming*). A simple overt attack causing outright service denial can also be realized by cutting the fiber.

3. PROBLEM DESCRIPTION

Given is a physical network and a virtual topology, i.e., a set of static lightpath demands. The physical optical network is modelled as a graph where edges are assumed to be bidirectional, each representing a pair of optical fibers (i.e., one fiber per direction). The RWA problem searches for a set of physical paths corresponding to the set of lightpath requests, subject to the wavelength clash and continuity constraints. We assume that there are enough wavelengths to satisfy these constraints for any routing scheme. We limit the maximum number of hops in a lightpath to prevent excessively long paths causing delay and, more importantly, unacceptable physical impairments.

3.1 A New Objective for the RWA Problem: maximum Lightpath Attack Radius(maxLAR)

Our main objective for the RWA problem is to minimize the maxLAR while successfully routing all lightpath requests. A secondary objective is to reduce lightpath congestion (i.e., the maximum number of lightpaths routed over any one physical link). Namely, the maxLAR of a routing scheme is also an upper bound on congestion, so by minimizing the maxLAR , we also minimize the worst case on congestion.

Note that one aspect of congestion is that it represents the maximum number of disrupted lightpaths in case of a fiber cut or other component malfunction along any link. Thus, minimizing congestion could potentially minimize the need for rerouting in case of such failures, which can be an additional benefit of our approach.

Furthermore, the maxLAR is also an upper bound on the number of wavelengths needed for successful wavelength assignment, both in networks equipped with wavelength converters and those without. In wavelength-convertible networks, the congestion is equivalent to the number of wavelengths required, making the maxLAR an upper bound on both. In networks with no wavelength conversion, congestion is only a lower bound on the number of wavelengths needed, while the maxLAR is still an upper bound. Namely, wavelength assignment can be modelled as the graph colouring problem on a graph where nodes represent lightpaths and two nodes are connected with a link if their corresponding lightpaths traverse a common physical link .We call such a graph the *conflict graph* of a particular routing solution The chromatic number of a graph is the minimum number of colours necessary to colour the. graph successfully. Although calculating the chromatic number is NP-complete, simple upper bounds have been defined. In [14] the upper bound was shown to be $\Delta(G)+1$, where ΔG is the maximum degree of the graph. According to our definition, the maxLAR is equal to the maximum degree of the conflict graph incremented by one, making it an upper bound on the chromatic number, i.e., an upper bound on the number of wavelengths needed.

An example of two different routing schemes for a set of five lightpath requests on a six-node network are shown in Fig. 2. Both routing solutions have a congestion of two, and both can be realized using two wavelengths.

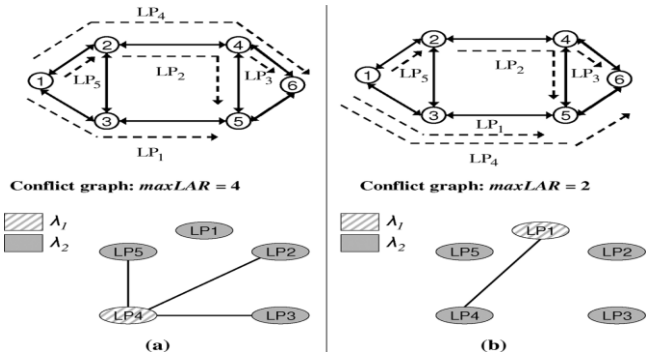

Figure 2: An example of two RWA schemes with the same number of wavelengths and the same congestion, but with different values for the maxLAR

However the maxLAR in the first routing scheme is 4 [Fig. 2(a)], while the second has a maxLAR of 2 [Fig. 2(b)]. Namely, a jamming attack injected at the beginning of lightpath 4 in the first routing scheme could potentially disrupt lightpaths 2–5. In the second routing scheme, a jamming signal injected on any legitimate lightpath could disrupt at most two lightpaths (including itself) . Even though these two routing schemes use the same number of

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

wavelengths, use equally long lightpaths, and have the same congestion, the second routing scheme could significantly reduce the damage caused by some physical-layer attacks at no extra cost.

4. INTEGER LINEAR PROGRAMMING FORMULATION

In this section, we formulate the routing sub-problem as an ILP with the objective to minimize the . The formulation could be extended to include wavelength assignment (WA) to ensure feasibility if there is a limited number of wavelengths given. However, this would increase complexity without necessarily favouring solutions using fewer wavelengths . Consequently, we solve wavelength assignment subsequently using an existing graph colouring heuristic algorithm from[15] which we refer to as the Greedy Graph Colouring algorithm that minimizes the number of colours used. The ILP formulation for the routing subproblem of RWA follows.

4.1 Notation

We use the following notation

i,j	The source and destination nodes of a lightpath, i.e., the end nodes of a virtual link in V, $i,j \in \{1,2,\ldots,N\}$
x,y	The source and destination nodes of a lightpath, i.e., the end nodes of a virtual link in V, $x,y \in \{1,2,\ldots,N\}$
m,n	The end nodes of a physical link in P, $s,d \in \{1,2,\ldots,N\}$
Parameters:	
N	The number of nodes in the network.
H	An upper bound on the number of physical hops of a lightpath.
$P_{m,n}$	The physical topology, where $P_{m,n} = 1$ of there exists a link between nodes m and n, and $P_{m,n} = 0$ otherwise.
$V_{i,j}$	The virtual topology, i.e., the set of lightpaths, where $V_{i,j} = 1$ of there is a lightpath request between nodes i and j, and $V_{i,j} = 0$ otherwise.
Variables:	
$p_{m,n}^{i,j}$	The physical route variables, where $p_{m,n}^{i,j} = 1$ if there is a lightpath between nodes i and j and it is routed on physical link $P_{m,n}$, and $p_{m,n}^{i,j} = 0$ otherwise.
$ls_{m,n}^{(i,j)(x,y)}$	The link-sharing variables where $ls_{m,n}^{(i,j)(x,y)} = 1$ if both lightpaths corresponding to virtual links $V_{i,j}$ and $V_{x,y}$ are routed via physical link $P_{m,n}$; $ls_{m,n}^{(i,j)(x,y)} = 0$, otherwise.
$ls^{(i,j)(x,y)}$	The link-sharing variables where $ls^{(i,j)(x,y)} = 1$ if the lightpaths corresponding to virtual links $V_{i,j}$ and $V_{x,y}$ share at least one common physical link; $ls^{(i,j)(x,y)} = 0$, otherwise.
$\mathrm{LAR}^{(i,j)}$	An integer representing the attack radius of lightpath $V_{i,j}$, i.e., how many other lightpaths it shares links with, including itself.
maxLAR	An integer representing the maximum attack radius of any lightpath in the network.

4.2. Objective

$$\text{Minimize} \quad \text{maxLAR}. \tag{1}$$

4.3. Constraints

1) Physical Routing Constraints:

$$p_{m,n}^{i,j} \le P_{m,n} \qquad \forall i,j,m,n \tag{2}$$
$$p_{m,n}^{i,j} \le V_{i,j} \qquad \forall i,j,m,n. \tag{3}$$

Remark: This ensures that only those lightpaths that are requested are routed [constraint (3)] and only on existing physical links [constraint(2)]

2) Flow Conservation Constraints:

$$\sum_m p_{k,m}^{i,j} - \sum_m p_{m,k}^{i,j} = \begin{cases} V_{i,j}, & i = k \\ -V_{i,j}, & j = k \\ 0, & k \neq i,j \end{cases} \qquad \forall i,j,k. \tag{4}$$
$$p_{m,j}^{i,j} \in \{0,1\}. \tag{5}$$

Remark: Constraints (4) and (5) ensure flow conservation of lightpaths over physical links.

3) Cycling Constraints:

$$\sum_m m p_{m,n}^{i,j} \le 1 \quad \forall i,j,n \tag{6}$$
$$\sum_n n p_{m,n}^{i,j} \le 1 \quad \forall i,j,m \tag{7}$$
$$p_{m,n}^{i,j} + p_{n,m}^{i,j} \le 1 \quad \forall i,j,m,n. \tag{8}$$

Remark: Constraints (6)–(8) help prevent cycles in lightpaths.

4) Link-Sharing Constraints:

$$ls_{m,n}^{(i,j)(x,y)} \ge p_{m,n}^{i,j} + p_{m,n}^{x,y} - 1, \quad \forall i,j,x,y,m,n \tag{9}$$
$$ls_{m,n}^{(i,j)(x,y)} \le p_{m,n}^{i,j}, \quad \forall i,j,x,y,m,n \tag{10}$$
$$ls_{m,n}^{(i,j)(x,y)} \le p_{m,n}^{x,y}, \quad \forall i,j,x,y,m,n \tag{11}$$
$$ls_{m,n}^{(i,j)(x,y)} \in \{0,1\}. \tag{12}$$

Remark: Constraints (9)–(12) ensure that if there are lightpaths between node pairs and that are both routed over link , that they are marked as link-sharing.

$$ls^{(i,j)(x,y)} \le \sum_{m,n} ls_{m,n}^{(i,j)(x,y)}, \quad \forall i,j,x,y \tag{13}$$
$$ls^{(i,j)(x,y)} \ge ls_{m,n}^{(i,j)(x,y)}, \quad \forall i,j,x,y,m,n \tag{14}$$
$$ls^{(i,j)(x,y)} \in \{0,1\}. \tag{15}$$

Remark: Constraints (13)–(15) ensure that is set to 1 if lightpaths and traverse at least one common physical link, and 0 otherwise.

5) Attack Radius Constraints:

$$\mathrm{LAR}^{(i,j)} = \sum_{x,y} ls^{(i,j)(x,y)}, \quad \forall i,j \tag{16}$$
$$\mathrm{LAR}^{(i,j)} \ge 0, \quad \mathrm{LAR}^{(i,j)} \text{integer} \tag{17}$$
$$\text{maxLAR} \ge \mathrm{LAR}^{(i,j)}, \quad \forall i,j. \tag{18}$$

Remark: Constraints (16) and (17) ensure that represents the attack radius of lightpath . Constraint (18) ensures that the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

lightpath attack radius of any lightpath is no greater than the, which is being minimized.

6) Hop Bound Constraints:lightpath is bounded by H

$$\sum_{m,n} p_{m,n}^{i,j} \leq H \quad \forall i,j. \tag{19}$$

5. A TABU SEARCH HEURISTIC

Herein, we propose a tabu search heuristic for the routing sub-problem, aimed to minimize the bigger problems. 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 [15].

5.1 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 best found solution is deemed the final result. A detailed review of the tabu search method can be found in [16].

5.2 The TS_LAR heuristic

TS_LAR Heuristic;

Input and initialization:

$G = (V, E)$; α;

$\tau = \{LP_1, \ldots, LP_M\}$, where $SLD_i = (s_i, d_i)$, $i = 1, \ldots, M$; *//the set of lightpaths*

K; *//the number of K-shortest paths*

$X_0 = (x_1^0, \ldots, x_M^0), x_i^0 := 1, i = 1 \ldots, M$; *//initial routing solution with all paths set to 1*

Find $\text{maxLAR}(X_0)$ and the corresponding lightpaths $L(X_0) = \{LP_{r_1}, \ldots, LP_{r_s}\}, r_i \in \{1, \ldots, M\}, i = 1, \ldots, s$;

$X := X_0$ such that $Degree(LP_{r_i}) \geq \alpha \cdot \text{maxLAR}(X_0)$; *//incumbent solution*

$\text{maxLAR} := LAR(X_0)$; *//fitness of incumbent solution*

$Tabulist := \{\}, i := 0, itWithoutImprov := 0$;

Begin:

//Tabu search iterations

while $i <$ desired number of iterations **do**

$X_{it} := \{\}, \text{maxLAR}(X_{it}) := \infty, L(X_{it}) := \{\}$;

for j in $1, \ldots, |L(X_i)|$ **do**

$x_{r_j}^{i\,\prime} =$ random number in $\{1, \ldots, K\} \backslash x_{r_j}^i$ except for that forbidden by tabu list;

$X_i' := (x_1^i, \ldots, x_{r_j-1}^i, x_{r_j}^{i\,\prime}, x_{r_j+1}^i, \ldots, x_M^i)$;

Find $\text{maxLAR}(X_i')$ and $L(X_i')$;

if $\text{maxLAR}(X_i') = \text{maxLAR}(X_{it})$ **then**

if $\Delta_2\{CG(X_i')\} < \Delta_2\{CG(X_{it})\}$ **then**

$X_{it} := X_i'$;

end if

if $\Delta_2\{CG(X_i')\} = \Delta_2\{CG(X_{it})\}$ **then**

Chose randomly between X_i' and the current X_{it} and set one of them as X_{it};

end if

end if

if $\text{maxLAR}(X_i') < \text{maxLAR}(X_{it})$ **then**

$X_{it} := X_i'$, $\text{maxLAR}(X_{it}) := \text{maxLAR}(X_i')$, $L(X_{it}) := L(X_i')$;

end if

end for

if $\text{maxLAR}(X_{it}) == \infty$ **then**

//all neighbors are on the tabu list

Find all nodes with Δ_2 in conflict graph of solution X_i (i.e., $\Delta_2\{(CG(X_i)\})$ and randomly reroute them. If this is on tabu list, choose a random number of lightpaths and randomly reroute them;

else

$X_i := X_{it}$, $\text{maxLAR}(X_i) := \text{maxLAR}(X_{it})$, $L(X_i) := L(X_{it})$;

end if

Update tabu list;

if $\text{maxLAR}(X_i) = \text{maxLAR}$ **then**

if $\Delta_2\{X_i\} < \Delta_2\{X\}$ **then**

$X := X_i$, $L(X) := L(X_i)$;

end if

if $\Delta_2\{CG(X_i)\} = \Delta_2\{CG(X)\}$ **then**

Chose randomly between X_i and the current X and set one of them as X

end if

end if

if $\text{maxLAR}(X_i) < \text{maxLAR}$ **then**

$X := X_i, \text{maxLAR} := \text{maxLAR}(X_i)$;

else

$itWithoutImprov := itWithoutImprov + 1$;

end if

if $itWithoutImprov \geq$ allowed no. of iterations without improvement **then**

Select a random number of lightpaths and randomly reroute them;

$itWithoutImprov = 0$;

end if

$i := i + 1$;

end while

End

6. CONCLUSION

In this paper, we consider the problem of routing and wavelength assignment in transparent optical networks. We present a novel objective criterion, called the maxLAR , which measures the largest number of lightpaths sharing a common link with any one lightpath. By minimizing the maxLAR we can limit the maximal disruption caused by various physical-layer attacks. As such, we can improve network security and robustness through careful network planning, at no extra cost for specialized equipment. We formulate the routing sub problem as an integer linear program and compare with a formulation with the objective to minimize congestion on a small network. The results show that our formulation obtains near-optimal results for congestion, while significantly reducing the maxLAR and the average number of lightpaths routed over all links (i.e., average load). For larger problems, solving the ILP is intractable and, thus, we propose a tabu search heuristic algorithm, run in combination with a graph colouring algorithm for wavelength assignment. Testing on a larger network and comparing with existing approaches from the literature indicates that the proposed algorithm obtains superior solutions with respect to the maxLAR and average load, but as a trade-off with an increase in congestion. This trade-off seems justified by the extremity of the vulnerabilities associated with optical networks security

REFERENCES

[1] **Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: An approach to high-bandwidth optical WANs," IEEE Trans. Commun., vol. 40, no. 7, pp. 1171–1182, Jul. 1992.**

[2] **T. F. Noronha, M. G. C. Resende, and C. C. Ribeiro, "A genetic algorithm with random keys for routing and wavelength assignment," Networks, submitted for publication.**

[3] **N. Skorin-Kapov, "Heuristic algorithms for the routing and wavelength assignment of scheduled lightpath demands in optical networks," IEEE J. Sel. Areas Commun., vol. 24, no. 8, pp. 2–15, Aug. 2006.**

[4] **X. Chu and B. Li, "Dynamic routing and wavelength assignment in the presence of wavelength conversion for all-optical networks," IEEE/ACM Trans. Netw., vol. 13, no. 3, pp. 704–715, Jun. 2005.**

[5] **B. Ramamurthy, D. Datta, H. Feng, J. P. Heritage, and B. Mukherjee, "Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks," J. Lightw. Technol., vol. 17, no. 10, pp. 1713–1723, Oct. 1999.**

[6] **M. Médard, D. Marquis, R. Barry, and S. Finn, "Security issues in alloptical networks," IEEE Network, vol. 11, no. 3, pp. 42–48, May/Jun. 1997.**

[7] **T. Wu and A. Somani, "Cross-talk attack monitoring and localization in all-optical networks," IEEE/ACM Trans. Netw., vol. 13, no. 6, pp. 1390–1401, Dec. 2005.**

[8] **C. Mas, I. Tomkos, and O. Tonguz, "Failure location algorithm for transparent optical networks," IEEE J. Sel. Areas Commun., vol. 23, no. 8, pp. 1508–151, Aug. 2005.**

[9] **M. Sivakumar, R. K. Shenai, and K. M. Sivalingam, "A survey of survivability techniques for optical WDM networks," in Emerging Optical Network Technologies: Architectures, Protocols and Performance, A. K. M. Sivalingam and S. Subramaniam, Eds. New York: Springer Science+Media, 2005, ch. 3, pp. 297–332.**

[10] **N. Skorin-Kapov, J. Chen, and L. Wosinska, "A tabu search algorithm for attack-aware lightpath routing," in Proc. ICTON, Athens, Greece, Jun. 2008, pp. 42–45.**

[11] **N. Skorin-Kapov, "A MILP formulation for routing lightpaths for attack protection in TONs," in Proc. NAEC, Riva del Garda, Italy, Sep. 2008, pp. 55–62.**

[12] **N. Skorin-Kapov, O. Tonguz, and N. Puech, "Self-organization in transparent optical networks: A new approach to security," in Proc. Contel, Zagreb, Croatia, 2007, pp. 311–318.**

[13] **T. Deng and S. Subramaniam, "Covert low-power QoS attack in alloptical wavelength routed networks," in Proc. IEEE Globecom, 2004, vol. 3, pp. 1948–1952.**

[14] **R. L. Brooks, "On coloring the nodes of a network," in Proc. Cambridge Phil. Soc., 1941, vol. 37, pp. 194–197.**

[15] **D. Kirovski and M. Potkonjak, "Efficient coloring of a large spectrum of graphs," in Proc. 35th Conf. Design Autom., San Francisco, CA, Jun. 1998, pp. 427–432.**

[16] **F. Glover and M. Laguna, Tabu Search. Boston, MA: Kluwer Academic, 1997.**