Research Article

Optimal attack-aware RWA for scheduled lightpath demands

Saja Al Mamoori[1] · Meenakshi Nizampatnam[1] · Arunita Jaekel[1]

Abstract
In Transparent optical networks (TONs), the data signals remain in the optical domain for the entire transmission path, creating a virtual topology over the physical connections of optical fibers. Due to the increasingly high data rates and the vulnerabilities related to the transparency of optical networks, TONs are susceptible to different physical layer attacks, including high-power jamming attacks. Developing strategies to handle such attacks and mitigating their impact on network performance is becoming an important design problem for TONs. Some approaches for handling physical layer attacks for static and dynamic traffic in TONs have been presented in recent years. In this work, we propose an integer linear program (ILP) formulation to control the propagation of such attacks in TONs for *scheduled lightpath demands*, which need periodic bandwidth usage at certain predefined times. We consider both the fixed window model, where the start and end timings of the demand are known in advance, and the sliding window model, where exact start and end times are unknown but fall within a larger window. We consider a number of potential objectives for attack-aware RWA and show how the flexibility to schedule demands in time can impact these objectives, compared to both attack-unaware and fixed window models.

Keywords Transparent optical networks (TONs) · High-power jamming attacks · Scheduled lightpath demands (SLDs) · Integer linear program (ILP) · Routing and wavelength · Assignment (RWA)

1 Introduction

Transparent optical networks allow high-speed end-to-end connections in the optical domain, without undergoing optical to electronical to optical (OEO) conversion at intermediate nodes. However, such transparency can lead to increased vulnerabilities to physical-layer attacks caused by high-powered jamming signal and can seriously degrade network performance [1]. Transparency also enhances the difficulties in detecting and localizing attacks, because monitoring must be performed in the optical domain [2–4]. In addition, techniques to detect and localize attacks need information from specialized optical monitoring equipment and can be quite expensive. In general, the more reliable performance of the network required, the more resources are needed and thus the cost of the security equipment is higher [5]. Along with the development and wide application of transparent wavelength division multiplexing (WDM) optical networks, security issues and physical-layer attack management have become increasingly important to the network manager [6]. Existing approaches to optical networks security are generally aimed at minimizing the potential damage caused by several major physical-layer attacks including gain competition, inter-channel crosstalk attack and in-band crosstalk attack [7].

A number of different attack-aware RWA algorithms have been proposed in the literature, for static [1, 5, 8, 9] and dynamic [10–12] lightpath allocation. Attack-aware RWA approaches typically try to reduce the *attack-radius* (AR) [11, 13, 14] for a given set of lightpaths, by suitably choosing the route and/or wavelength for each lightpath. The AR of a compromised lightpath p can be loosely defined as the number of lightpaths (including itself) that

✉ Saja Al Mamoori, almamo@uwindsor.ca | [1]School of Computer Science, University of Windsor, Windsor, Canada.

SN Applied Sciences (2019) 1:1421 | https://doi.org/10.1007/s42452-019-1418-z

Received: 9 May 2019 / Accepted: 9 October 2019 / Published online: 16 October 2019

can be adversely affected by an attacking signal on p. This typically occurs when p shares at least one link or at least one node and a common channel [1, 15] with the other lightpath. The attack-radius of a lightpath p, is a widely used metric to measure the impact of introducing an attack signal on p and we have also used this metric in this paper.

In this paper, we propose 2 novel *integer linear program* (ILP) formulations to address the attack-aware *routing and wavelength assignment* (RWA) problem in transparent WDM optical networks for *scheduled lightpath demands* (SLDs) [13, 15]. First, we present a new ILP that minimizes the AR of a set of SLDs, by taking into account the start and end times of the demands under a fixed- window scheduled traffic model. Next, we show how this ILP can be extended to further reduce the AR, by intelligently selecting the demand start times, for the sliding window model. To the best of our knowledge, our work is the first that addresses attack-aware RWA for *scheduled* lightpaths. We have conducted extensive simulations to compare the performance of the proposed approaches to traditional attack-unaware RWA. Some preliminary results from these simulations are reported in [13] and [15] for the fixed-window and sliding-window scheduled traffic model, respectively. The major contributions of this paper are:

- A novel ILP formulation (*ILP_fixed*) that can handle both *in-band* and *out-of-band* attacks for fixed- window scheduled traffic.
- A second extended ILP (*ILP_sliding*) that can intelligently schedule demands in time, in addition to performing attack-aware RWA, for sliding-window scheduled traffic.

2 Related work

2.1 Scheduled traffic model

The models of traffic demand typically considered in the literature for the design of WDM network include *static* and *dynamic* traffic. For static demands, the set of traffic demands is known beforehand and does not change for relatively long periods. In *dynamic* traffic, the arrival time and duration of individual requests are not known ahead of time and lightpaths are established as needed, assuming sufficient resources are available. The RWA problem, under both the static and dynamic traffic models, has been widely investigated and a number of ILP formulations as well as heuristics are available to solve this problem [16].

In recent years there has been an increasing number of applications that require periodic use of lightpaths (e.g. once per day, or once per week) at predefined times. For example, an online "class" with one two hour lecture per week on a specified day and at a specified time, or a bank transferring its data to a central location every night between 2 and 4 am. A new model, called the *scheduled traffic model* (*STM*), has been proposed in the literature [17] to handle such demands. This model is appropriate for applications that require *periodic* use of lightpaths and exploits the fact that the setup and teardown times of the demands are known in advance, so that the RWA algorithm can optimize resource allocation in both space and time. An excellent survey of RWA for this model is available in [18].

One class of STM is the fixed-window model [13], where the start and end time for each SLD is fixed and known beforehand. A lightpath p in this model can be represented by a tuple $p = (s_p, d_p, st_p, \tau_p)$, where s_p (d_p) is the source (destination) node of the demand, st_p is the start time and τ_p is the duration. The second class of STM is the sliding-window model [15], where a demand has a specified duration τ_p, and can be scheduled any time within a larger window (a_p, ω_p), such that the demand can only start after a_p, and must be completed before ω_p. For the sliding window model, a demand is represented by a tuple $p = (s_p, d_p, a_p, \omega_p, \tau_p)$, since the actual start time for the demand is not known ahead of time.

2.2 Handling attacks in all-optical networks

2.2.1 Attack types in TONs

Attacks on networks can be of forms, such as traffic analysis, eavesdropping, data delay, service denial, Quality of Service (QoS) degradation and spoofing [19]. Because many of these attacks have similar characteristics, they are often grouped into two main categories—(1) service disruption and (2) eavesdropping. All-Optical Networks provide transparency capabilities, allowing routing and switching of traffic without any modification or examination of signals in the network [20]. Transparency offers many advantages in supporting high data rate communications, but also brings new challenges that do not exist in traditional networks. Three main categories of physical layer attacks that have been identified for optical networks are [21]:

- Signal insertion attacks,
- Signal splitting attacks, and
- Physical infrastructure attacks

Handling physical infrastructure attacks, which damage or tamper with network equipment are out of the scope of this paper. Our proposed approach deals with some common types of signal insertion and signal splitting

attacks that can be used to compromise legitimate lightpaths established over the network. An overview of physical-layer attacks, which are addressed by the proposed ILP is discussed in this section.

A common type of signal insertion attack is the high power jamming attack, where an optical signal with high power (5–10 dB above normal) is introduced on a legitimate channel. When the attacker introduces a high-powered signal into the optical fiber, it can interfere with the signals on other wavelengths because of the optical fiber non linearities. The inter channel crosstalk between signals on different wavelengths transmitted over the same optical fiber can be exploited to mount out-of-band jamming attacks [1, 22]. The Raman gain effect and cross-phase modulation are some of the causes that create non linearities in optical fibers [22]. A high power signal can also cause gain competition attack [6] in optical amplifiers, as the attack signal acquires more energy at the expense of legitimate signals. Older networks, that are not equipped with variable optical amplifiers (VOAs) to regulate output power of signals, are typically the most susceptible to high power jamming attacks. However, even when the jamming signal is attenuated at the first downstream node in steady-state, short-lived oscillations, called transients, can cause error-bursts and may even propagate through multiple links [21]. Repeated, intermittent injection of high-power signals on a malicious lightpath can cause transients. The harmful effects of such transients may be multiplied, if they cause multiple 'restorations', which lead to even more transients as legitimate lightpaths are disrupted and reestablished.

In addition to affecting co-propagating channels on the same link, a high-power signal also introduces intra-channel (or in-band) crosstalk between the signals on the same wavelength inside an optical switch [10]. When a high-powered attacking signal is injected on a wavelength, all the signals using that wavelength and sharing a common switch gets attacked. This can be more harmful than the out-of-band high-power jamming attacks, as the signals are on the same wavelength as that of the attacker signal [23].

Another attack, called low-power QoS attack [21]—a type of signal splitting attack, can also be used to affect lightpaths on multiple links. In this type of attack, the attacker deliberately attenuates a channel, e.g. by attaching a splitter. This not only degrades the performance of the attacked channel, but the attack can propagate if nodes are equipped with fixed attenuation based power equalization. Such equipment is helpful for limiting propagation of high power jamming attacks but a low power attack can still propagate as legitimate signals on the link will be attenuated to ensure a flat power spectrum.

Another attack scenario outlined in [1] involves the attacker requesting a legitimate channel but not transmitting any data on it. In this case, the channel will carry only leakage signals picked up through crosstalk. The weak leakage signal can then be amplified along its path and delivered to the attacker at the destination node.

2.2.2 Attack-aware RWA

The attack-aware routing and wavelength assignment (RWA) is aimed at minimizing the potential damage caused by physical-layer attacks, without the requirement of specific network monitoring components. One of the most widely used metrics for measuring the potential negative impact of a malicious lightpath is the size of its *attack group*, i.e. the set of lightpaths that may be affected by it [1, 24]. In this paper, we will use the following terminology available in the literature.

- The *lightpath attack group* (LAG_p) for a lightpath p consists of the set of lightpaths (including p itself) that shares at least one common link with p. The lightpath attack radius (LAR_p) is a commonly used metric for measuring the impact of an out-of-band attack carried out on a lightpath p and is defined as the number of lightpaths in LAG_p i.e., $LAR_p = |LAG_p|$.
- The *in-band attack group* (IAG_p) is defined as the set of lightpaths (including p itself) that use the same wavelength and share at least one common node with p. The corresponding value of in-band attack radius (IAR_p) is defined as the number of lightpaths in IAG_p i.e., $IAR_p = |IAG_p|$.

In [1], an ILP is proposed to handle the *out-of-band* and gain competition attacks for static traffic. The main objective of this ILP is to minimize the Maximum link-share attack radius (maxLAR), which can be calculated as the maximum number of lightpaths that are link sharing with a single lightpath demand in the network. The secondary objective of this formulation is to reduce the average load on the network.

In [25], the authors propose ILP formulations to handle *in-band* attack propagation in all optical WDM networks for offline planning problem. Both the direct and indirect in-band crosstalk propagations are examined and are minimized to control the propagation. The main objectives of these two ILPs are minimizing the maximum primary attack radius (PAR) and the maximum secondary attack radius (SAR) values respectively. The ILP-PAR simply checks for the lightpaths that are sharing the same switch and are using the same wavelength and calculates the PAR value. ILP-SAR takes the constraints of ILP-PAR and calculates the secondary attack radius (SAR) value, by checking the

spread of in-band crosstalk over the network indirectly, by already attacked signals. The wavelength assignment (WA) problem for in-band attacks are also considered in [5, 26, 27]. The concept of propagating crosstalk attack radius (P-CAR) is proposed in [5] and an attack-aware wavelength assignment that minimizes the worst-case potential propagation of in-band crosstalk jamming attacks is presented. In [26], the authors select a wavelength based on estimated BER to improve BER and blocking probability for dynamic lightpath allocation. In [27], the authors propose both ILP and heuristic formulations and define new objective criteria for wavelength assignment.

In [12], an ILP is proposed to handle the propagation of both in-band and out-of-band jamming attacks for the static lightpath allocation problem. Interactions among the lightpaths, which are sharing a common link are calculated and are added to the objective to cover the inter channel crosstalk susceptibility. In the first phase of programming, a set of K candidate paths is obtained using Dijkstra's algorithm [4]. The acquired routes for all the source and destination pairs are given as an input to the ILP, with the objective of controlling the spread of both inter and intra channel crosstalk attacks.

A number of papers have also considered attack-aware RWA for survivable optical networks. In [28] the authors propose a two-step ILP for RWA of working and backup lightpaths using dedicated path protection and a heuristic for larger problems. Heuristic approaches that ensure attack groups of primary and backup paths are disjoint and use the minimum number of wavelengths are presented in [24] and [29]. Finally, in [30], the authors formulate and ILP for jamming-aware shared path protection (JA-SPP) in WDM networks.

3 Attack-aware integer linear program (ILP) formulations

In this section, we introduce our proposed approaches for solving the attack-aware RWA of for both fixed-window and sliding-window STM. The objectives of the proposed ILP formulations is to minimize the maximum combined attack radius (maxAR) for the set of lightpaths. We are given a physical network $G(N, E)$, where N is the set of nodes and E is the set of fiber links in the network, and each link has a set of W available channels for establishing lightpaths. We are also given a set P of scheduled lightpath demands, where each $p \in P$ can be specified as a tuple $p = (s_p, d_p, st_p, \tau_p)$ ($p = (s_p, d_p, \alpha_p, \omega_p, \tau_p)$) for fixed-window (sliding-window) STM.

The entire time period is divided into M non-overlapping intervals, numbered 1, 2, …, M. The proposed ILPs are independent of the duration of each interval and the number of such intervals. The duration of each interval can vary from a few seconds to several minutes or even hours, depending on the application, and is set by the user. In the proposed ILPs, the start and end times of a demand (or corresponding window for sliding window model) are specified in terms of the interval in which the demand (or window) starts and/or ends. Similarly, the duration τ_p of a demand p is specified in terms of the number of time intervals during which the demand is active. We use the notation $a_{p,m}$ to denote that a demand p is active during interval m, where $m = 1, 2, \ldots, M$. We note that for the fixed-window model, the values of $a_{p,m}$ are known ahead of time for all $p \in P$ and for all possible values of m, since the demand start times and durations are fixed. However, for the sliding-window model, the values of $a_{p,m}$ must be determined by the ILP.

3.1 Proposed ILP for fixed-window SLDs (*ILP_fixed*)

Before solving the *ILP_fixed*, we first calculate the parameter $t_{p,q}$, which determines if lightpaths p and q are time disjoint. For each pair of lightpaths $p, q \in P$, $t_{p,q}$ can be pre-calculated using Eqs. (1)–(2b), shown below, since the values of $a_{p,m}$ and $a_{q,m}$ are known in advance.

$$t^m_{p,q} = a_{p,m} \cdot a_{q,m} \quad \forall p, q \in P,\ \forall m = 1, 2, \ldots, M \tag{1}$$

$$t_{p,q} \geq t^m_{p,q} \quad \forall p, q \in P,\ \forall m = 1, 2, \ldots, M \tag{2a}$$

$$t_{p,q} \leq \sum_m t^m_{p,q} \quad \forall p, q \in P \tag{2b}$$

$$t_{p,q} \leq 1 \quad \forall p, q \in P \tag{2c}$$

Equations (1) and (2) determine if two different lightpaths p and q overlap in time ($t_{p,q} = 1$) or are time-disjoint ($t_{p,q} = 0$). Eq. (1) sets $t^m_{p,q} = 1$, if lightpaths p and q are both active during interval m. If Eqs. (2a)–(2c) set $t_{p,q} = 1$ if there is at least one interval (possibly more) during which both lightpaths are active; otherwise, $t_{p,q} = 0$, indicating that p and q are time disjoint. The $t_{p,q}$ values are pre-calculated and given as input to the ILP.

The following variables are defined for the ILP.

Variables:

$x_{p,e} = 1$ if lightpath p uses edge e; 0 otherwise.
$y_{p,i} = 1$ if lightpath p passes through node i; 0 otherwise.
$\omega_{p,k} = 1$ if lightpath p is assigned channel k; 0 otherwise.
$\alpha_{p,q}\left(\beta_{p,q,}\right) = 1$ if lightpaths p and q share at least one common edge (node); 0 otherwise. $0 \leq \alpha_{p,q}, \beta_{p,q} \leq 1$
$\alpha^e_{p,q}\left(\beta^i_{p,q}\right) = 1$ if lightpaths p and q share a common edge e (node i); 0 otherwise.

$\gamma^k_{p,q} = 1$ if lightpaths p and q both use channel k; 0 otherwise.
$\gamma_{p,q} = 1$ if lightpaths p and q both use the same channel; 0 otherwise. $0 \leq \gamma_{p,q} \leq 1$
$\delta_{p,q} = 1$ if lightpaths p and q use the same channel and have at least one common node; 0 otherwise.
$LAR^m_{p,q}\left(IAR^m_{p,q}\right) = 1$ if lightpath $q \in LAG_p$ ($q \in IAG_p$) during time interval m.
$LAR_{p,q}$ ($IAR_{p,q}$) = 1 if lightpath $q \in LAG_p$ ($q \in IAG_p$) during at least one time interval. $0 \leq LAR_{p,q},\ IAR_{p,q} \leq 1$
$LAR_{p,m}$ ($IAR_{p,m}$) = An *integer* value specifying the lightpath attack radius (in-band attack radius)of p during time interval m.
LAR_p (IAR_p) = An *integer* value specifying the lightpath attack radius (in-band attack radius)of p over all time intervals.
maxAR = An *integer* value specifying the maximum combined attack radius for all lightpaths.

Objective function:

$$\text{Minimize} \quad maxAR \tag{3}$$

The objective function minimizes the maximum attack radius (*maxAR*), where *maxAR* is the upper bound of $AR_p = LAR_p + IAR_p$, for all lightpaths $p \in P$. This objective minimizes the maximum Attack Radius (AR_p value) for any lightpath.

Subject to:

Flow conservation constraints:

$$\sum_{(e:i\to j\in E)} x_{(p,e)} - \sum_{(e:j\to i\in E)} x_{(p,e)} = \begin{cases} 1 & if\ i = s_p \\ -1 & if\ i = d_p \\ 0 & otherwise. \end{cases} \quad \forall i \in N,\ p \in P \tag{4}$$

$$\sum_{(e:i\to j\in E)} x_{(p,e)} \leq 1 \quad \forall i \in N,\ p \in P \tag{5}$$

Constraints (4) and (5) ensure flow conservation of lightpaths. Constraint (4) finds a valid path over the physical topology, for each lightpath. Constraint (5) ensures that the path does not contain any loops.

Wavelength continuity constraint:

$$\sum_k \omega_{p,k} = 1 \forall p \in P \tag{6}$$

Constraint (6) ensures that a lightpath must be assigned the same wavelength on each link it passes without wavelength conversion.

Defining $\alpha_{p,q}$ (link sharing) constraints:

$$x_{p,e} + x_{q,e} - \alpha^e_{p,q} \leq 1 \quad \forall p,q \in P,\ p \neq q,\ \forall e \in E \tag{7}$$

$$x_{p,e} \geq \alpha^e_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall e \in E \tag{8}$$

$$x_{q,e} \geq \alpha^e_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall e \in E \tag{9}$$

$$\alpha_{p,q} \geq \alpha^e_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall e \in E \tag{10}$$

$$\alpha_{p,q} \leq \sum_{e\in E} \alpha^e_{p,q} \quad \forall p,q \in P,\ p \neq q \tag{11}$$

Constraints (7)–(9) sets the value of $\alpha^e_{p,q} = 1$ if lightpath p and lightpath q are both routed over link e. When both $x_{p,e} = 1$ and $x_{q,e} = 1$, constraint (7) forces $\alpha^e_{p,q} = 1$. However, if either both $x_{p,e} = 0$ or $x_{q,e} = 0$, then constraint (8) and (9) forces $\alpha^e_{p,q} = 0$. So, these 3 constraints allow $\alpha^e_{p,q}$ to be defined as a *continuous* variable, even though it is constrained to take on integer values of 0 or 1 only. The use of this technique significantly reduces the number of integer variables in this formulation and hence its computational complexity. Constraints (10) and (11) determine if two lightpaths p and q share at least one (possibly more) common link(s), and if so set $\alpha_{p,q} = 1$.

Node usage constraints:

$$y_{p,i} = \sum_{e:i\to j\in E} x_{p,e} \quad \forall p \in P,\ \forall i \in N,\ i \neq d_p \tag{12}$$

$$y_{p,d_p} = 1 \quad \forall p \in P \tag{13}$$

Constraint (12) determines if a lightpath p traverses a specific node i in its selected route. If so the value of $y_{p,i}$ is set to 1. Constraint (13) states that the destination node of a lightpath must be on the selected route.

Defining $\beta_{p,q}$ (node sharing) constraints:

$$y_{p,i} + y_{q,i} - \beta^i_{p,q} \leq 1 \quad \forall p,q \in P,\ p \neq q,\ \forall i \in N \tag{14}$$

$$y_{p,i} \geq \beta^i_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall i \in N \tag{15}$$

$$y_{q,i} \geq \beta^i_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall i \in N \tag{16}$$

$$\beta_{p,q} \geq \beta^i_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall i \in N \tag{17}$$

$$\beta_{p,q} \leq \sum_i \beta^i_{p,q} \quad \forall p,q \in P,\ p \neq q \tag{18}$$

Constraint (14)–(18) very similar to constraints (7)–(11) and are used to determine if two lightpaths p and q pass

through at least one (possibly more) common node(s). If so, it we set $\beta_{p,q} = 1$

Defining $\gamma_{p,q}$ (channel sharing) constraints:

$$\omega_{p,k} + \omega_{q,k} - \gamma^k_{p,q} \leq 1 \quad \forall p,q \in P,\ p \neq q,\ \forall k \in W \tag{19}$$

$$\omega_{p,k} \geq \gamma^k_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall k \in W \tag{20a}$$

$$\omega_{q,k} \geq \gamma^k_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall k \in W \tag{20b}$$

$$\gamma_{p,q} \geq \gamma^k_{p,q} \quad \forall p,q \in P,\ p \neq q,\ \forall k \in W \tag{21}$$

$$\gamma_{p,q} = \sum_k \gamma^k_{p,q} \quad \forall p,q \in P,\ p \neq q \tag{22}$$

Similarly, constraints (19)–(22) are applied to define *channel-sharing* and set the value of $\gamma_{p,q} = 1$, if lightpaths p and q are assigned the same channel (or wavelength) k.

Defining $\delta p,q$ (node-channel sharing) constraints:

$$\beta_{p,q} + \gamma_{p,q} - \delta_{p,q} \leq 1 \quad \forall p,q \in P,\ p \neq q \tag{23}$$

$$\beta_{p,q} \geq \delta_{p,q} \quad \forall p,q \in P,\ p \neq q \tag{24}$$

$$\gamma_{p,q} \geq \delta_{p,q} \quad \forall p,q \in P,\ p \neq q \tag{25}$$

Constraints (23)–(25) define *node-channel sharing*. If lightpath p and q pass through at least one common node i (i.e. $\beta_{p,q} = 1$) and share the same channel k (i.e. $\gamma_{p,q} = 1$), then $\delta_{p,q}$ is set to 1. The value of this variable determines if lightpath p might be in the attack-group of lightpath q.

Wavelength clash constraint:

$$\alpha_{p,q} + \gamma_{p,q} + t_{p,q} \leq 2 \quad \forall p,q \in P,\ p \neq q \tag{26}$$

Constraint (26) ensures that if two or more lightpaths share a common fiber link and are not time-disjoint, they cannot be assigned the same wavelength.

LAR/IAR of lightpath p (attack radius in interval m) constraints:

$$\alpha_{p,q} + t^m_{p,q} - LAR^m_{p,q} \leq 1 \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{27a}$$

$$\alpha_{p,q} \geq LAR^m_{p,q} \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{27b}$$

$$t^m_{p,q} \geq LAR^m_{p,q} \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{27c}$$

$$\mathrm{LAR}_{p,m} = \sum_{q \in P, p \neq q} LAR^m_{p,q} + a_{p,m} \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{27d}$$

Constraints (27a)–(27d) are used to calculate *lightpath* attack radius (LAR) value for lightpath p during interval m. If two lightpaths p and q share a link ($\alpha_{p,q} = 1$) and are both active during interval m ($t^m_{p,q} = 1$) then lightpath q belongs to attack group of p during interval m, and vice versa. The lightpath attack radius of p during interval m, is the number of lightpaths in its attack group plus itself, as given in Eq. (27d).

$$\delta_{p,q} + t^m_{p,q} - IAR^m_{p,q} \leq 1 \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{28a}$$

$$\delta_{p,q} \geq IAR^m_{p,q} \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{28b}$$

$$t^m_{p,q} \geq IAR^m_{p,q} \quad \forall p,q \in P,\ \forall m = 1,2,\ldots,M \tag{28c}$$

$$\mathrm{IAR}_{p,m} = \sum_{q \in P, p \neq q} IAR^m_{p,q} + a_{p,m} \quad \forall p \in P,\ \forall m = 1,2,\ldots,M \tag{28d}$$

In a similar fashion, (28a)–(28d) are used to calculate *in-band* attack radius (IAR) value for lightpath p during interval m. We note that the values of $\mathrm{LAR}_{\mathbf{p,m}}$ and $\mathrm{IAR}_{p,m}$ [as given in Eqs. (27d) and (28d)] are not needed if the objective value being optimized is maxAR (Eq. 3). However, they are used for minimizing one of the alternative objective functions, $\mathrm{Total\_AR}_{p,m}$ (Eq. 42), and hence included in the ILP.

Ligthpaths p and q belong to same attack group:

$$\mathrm{LAR}_{p,q} \geq LAR^m_{p,q} \quad \forall p \in P,\ \forall m = 1,2,\ldots,M \tag{29a}$$

$$\mathrm{LAR}_{p,q} \leq \sum_m LAR^m_{p,q} \quad \forall p,q \in P \tag{29b}$$

$$\mathrm{IAR}_{p,q} \geq IAR^m_{p,q} \quad \forall p \in P,\ \forall m = 1,2,\ldots,M \tag{30a}$$

$$\mathrm{IAR}_{p,q} \leq \sum_m IAR^m_{p,q} \quad \forall p,q \in P \tag{30b}$$

Eqn (29a)–(29b) indicate that lightpath q belongs to the lightpath attack group of p, if there is at least one interval m when q is in attack group of p. Similarly, (30a)–(30b) is used to set the in-band attack group of p over all time intervals.

Total LAR and IAR of lightpath p (over all intervals) constraints:

$$\mathrm{LAR}_p = \sum_{q \in P, p \neq q} LAR_{p,q} + 1 \tag{31}$$

$$\mathrm{IAR}_p = \sum_{q \in P, p \neq q} IAR_{p,q} + 1 \tag{32}$$

Constraint (31) [constraint (32)] defines the total LAR (IAR) value for lightpath p over all intervals.

Maximum attack radius *maxAR* of a lightpath:

$$\mathrm{LAR}_p + \mathrm{IAR}_p - 1 \leq maxAR \quad \forall p \in P \tag{33}$$

Constraint (33) ensures that the attack radius of any lightpath (over all intervals) does not exceed *maxAR*. This variable is minimized as the objective function.

Hop Bound Constraints:

$$\sum_{e:i\to j\in E} x_{p,e} \le hmax \quad \forall p \in P \tag{34a}$$

$$\sum_{e:i\to j\in E} x_{p,e} - len_p \le l \quad \forall p \in P \tag{34b}$$

In order to avoid excessively long paths, it is important to allow the path lengths to be constrained based on the needs of the network. Constraint (34a) ensures that the maximum number of hops (i.e. path length) of a lightpath does not exceed a pre-specified upper limit h_{max}. Constraint (34b) provides an alternate method of restricting the path length. It states that the number of hops for routing lightpath p cannot exceed the shortest path length for p (i.e. len_p) by more than l hops. Since the topology is known, len_p can be pre-calculated for each source–destination pair. Constraints (34a) or (34b) can be used individually, or both together, to limit the path length.

3.2 Proposed ILP for sliding-window SLDs (*ILP_sliding*)

In this section, we extend the ILP for the fixed-window model by adding constraints for scheduling each SLD in time. These constraints are based on the formulation in [31] In this case, the exact start times of the demands are not specified, but only the larger window during which each demand must be scheduled and the duration of the demand. For each demand, the ILP determines the optimal starting time of the demand, in order to minimize the overall attack radius. So, in addition to the variables listed in Sect. 3.1, we define the following binary variables:

- $st_{p,m}$=1 if m is the starting interval for demand p and 0 otherwise.
- $a_{p,m}$=1 if demand p is active during time interval m and 0 otherwise.

We also add the following constraints to those given for *ILP_fixed* from Sect. 3.1.

Sliding window scheduling constraints:

$$\sum_{m\in M} st_{p,m} = 1 \quad \forall p \in P,\ m \in M,\ \alpha_p \le m \le \omega_p - \tau_p \tag{35}$$

$$\sum_{m} a_{p,m} = \tau_p \quad \forall p \in P,\ m \in M,\ \alpha_p \le m \le \omega_p \tag{36}$$

$$a_{(p,m+i)} \ge st_{p,m} \quad \forall p \in P,\ m \in M,\ \alpha_p \le m \le \omega_p \tag{37}$$

Time sharing constraints:

$$a_{p,m} + a_{q,m} - t^m_{p,q} \le 1 \quad \forall p,q \in P,\ p \ne q,\ \forall m = 1,2,\ldots,M \tag{38}$$

$$a_{p,m} \ge t^m_{p,q} \quad \forall p,q \in P,\ p \ne q,\ \forall m = 1,2,\ldots,M \tag{39}$$

$$a_{q,m} \ge t^m_{p,q} \quad \forall p,q \in P,\ p \ne q,\ \forall m = 1,2,\ldots,M \tag{40}$$

The constraints (35)–(37) are the demand scheduling constraints. The constraint (35) is used to determine the actual start time for the lightpath p and ensure that each demand has only one possible start time. Clearly, in order to be accommodated within the specified time window (from α_p, ω_p), a demand of duration τ_p must start during the intervals from α_p to $\omega_p - \tau_p$. The constraint (36) activates the lightpath for exactly τ_p number of intervals, and constraint (37) ensures that the lightpath is active for τ_p *consecutive* time intervals starting from $st_{p,m}$.

We note that for the fixed window model, $a_{p,m}$ and $a_{q,m}$ are constant values given as input to the ILP. However, for the sliding window these are variables whose values are determined by the ILP. Therefore, we cannot use Eq. (1) directly to calculate $t^m_{p,q}$. So, constraints (38)–(40) are used to calculate the value of $t^m_{p,q}$, in a way that ensures that constraints are still linear.

3.2.1 Alternative objective functions

A number of different objective functions can be used for RWA, for both *attack-aware* and *attack-unaware* cases. In the formulations given in Sect. 3.1, we use a traditional objective function, which minimizes the *maximum* attack radius of a lightpath. Another commonly used objective is to minimize the *total* attack radius ($AR_p = LAR_p + IAR_p$) for all the lightpaths, as given in Eq. (41). Both of these objectives [i.e. Eqs. (3) and (41)] have been proposed in the literature for conventional attack-aware RWA and do not take into consideration the temporal nature of the demands. Since our proposed formulations focus on demands that are active during a specific time window, we also propose a new objective to incorporate their temporal nature. This objective, in Eq. (42), minimizes the total attack radius $AR_{p,m} = IAR_{p,m} + LAR_{p,m}$ over all lightpaths and all intervals. In other words, we consider not only if a lightpath q belongs to the attack group of p, but also the duration for which both lightpaths are active. The longer the duration, the more it will contribute to the objective value.

Finally, for attack-unaware RWA, one of the most widely-used objectives is to route each lightpath along the shortest path. This objective is implemented in (43) and minimizes the total path length for all lightpaths in terms of the number of hops over the physical topology. This objective does not take into consideration any of the attack aware constraints in the ILP formulation. Clearly, this is not an exhaustive list of possible objectives, many other objectives can be used. We do not advocate for a particular objective function

but simply provide several options for the network operator, who can choose the one that best fits their requirements.

- Minimize the sum of attack radius for all lightpaths p.

$$\text{Minimize } Total\_AR_p = \sum_{p \in P} (LAR_p + IAR_p) \quad (41)$$

- Minimize total attack radius for all lightpaths p over all intervals m.

$$\text{Minimize } Total\_AR_{p,m} = \sum_{p} \sum_{m} (\boldsymbol{LAR_{p,m}} + \boldsymbol{IAR_{p,m}}) \quad (42)$$

- Minimize total path length

$$\text{Minimize } Total\_path\_length = \sum_{p \in P} \sum_{e: i \to j \in E} \boldsymbol{x_{p,e}} \quad (43)$$

We have used this objective for implementing the *attack-unaware* RWA approaches.

4 Simulation results

In this section, we present our simulation results obtained by the proposed ILP formulations. We evaluate the performance of the proposed approaches for different objective functions, using different network topologies and varying the number of demands. All simulations are carried out using IBM ILOG CPLEX 12.6.2 optimization studio [32]. We consider three well-known network topologies namely, DT10 (10 nodes) [33], NSFNET (14 nodes) [34], and ARPANET (20 nodes) [35]. Each value reported here is calculated as the average of five simulation runs. We evaluate the performance with respect to different objectives discussed in Sect. 3, using the following approaches:

- The proposed ILP (*ILP_sliding*) for sliding window scheduled traffic.
- The proposed ILP (*ILP_fixed*) for fixed window scheduled traffic.
- The attack-unaware RWA using the shortest available path (SPATH)

For fixed-window model, we assume that each SLD is always initiated in its earliest possible time interval; while for the sliding-window model, the start and end intervals can slide within a larger window. According to the lightpath classification in [36], the demand sets are divided into three different categories based on the overlapping level. Clearly, the longer the demand holding time (DHT), the more lightpaths tend to overlap in time, leading to increased congestion. Hence, to evaluate the proposed approaches with different levels demand overlap in time, the following three variations of demand sets are used.

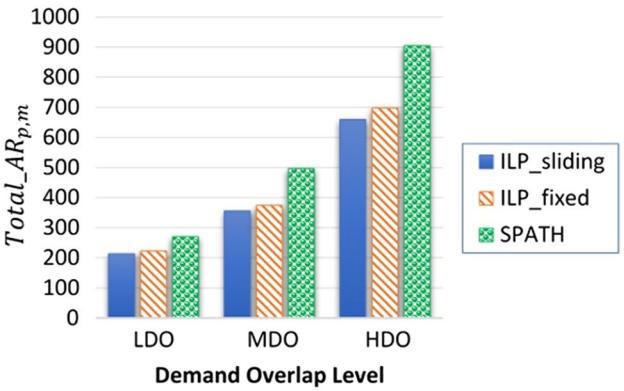

Fig. 1 Total attack radius over all intervals for 10-node network with 20 demands

1. Low Demand Overlap (LDO): For each SLD $p \in P$, the value of the demand holding time (τ_p) is between 1 and 10 time intervals, i.e. $1 \leq \tau_p \leq 10$.
2. Medium Demand Overlap (MDO): For each SLD $p \in P$, the value of the demand holding time (τ_p) is between 1 and 24 time intervals, i.e. $1 \leq \tau_p \leq 24$.
3. High Demand Overlap (HDO): For each SLD $p \in P$, the value of the demand holding time (τ_p) is between 10 and 24 time intervals, i.e. $10 \leq \tau_p \leq 24$.

The total time period for each simulation run was set 24 h, divided into time intervals of 1 h each, i.e. $M = 24$. The number of available channels per fiber (W) is set $W = 8$. The ILPs do not minimize wavelength usage but ensure that number of lightpaths sharing a link does not exceed W. The following parameters were generated randomly from a set of valid values, for each demand $p \in P$:

- source (s_p) and destination (d_p) for the demand,
- duration τ_p of the demand and
- start and end time of the window (α_p, ω_p) during which the demand can be active

Figures 1 and 2 show the total attack radius over all lightpaths and all intervals [as given in Eq. (42)] for 20 demands, routed over the 10-node DT10 network and 14-node NSFNET respectively, using the three approaches mentioned above. As expected, *ILP_sliding* outperforms both the *ILP_fixed* and *SPATH* approaches, in reducing the AR especially for medium and high demand overlapping. The performance of *ILP_sliding* and *ILP_fixed* are similar, with *ILP_sliding* providing a 3–5% reduction in total attack radius compared to *ILP_fixed*. Compared to *SPATH*,

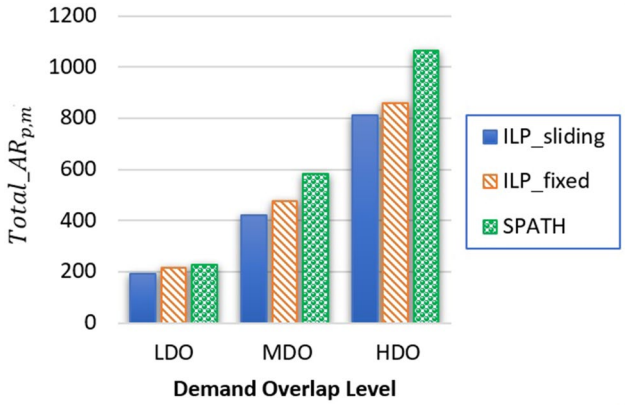

Fig. 2 Total attack radius over all intervals for 14-node network with 20 demands

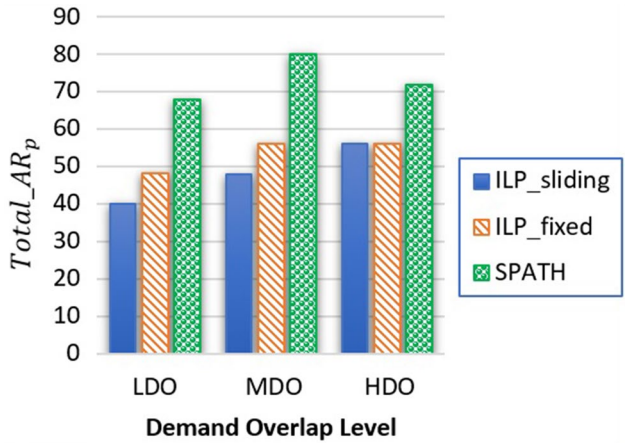

Fig. 3 Total attack radius of all demands for 10-node network with 20 demands

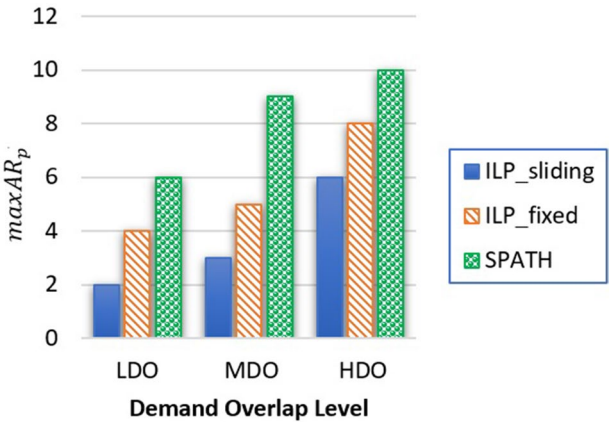

Fig. 4 Maximum attack radius values for 14-node network with 20 demands

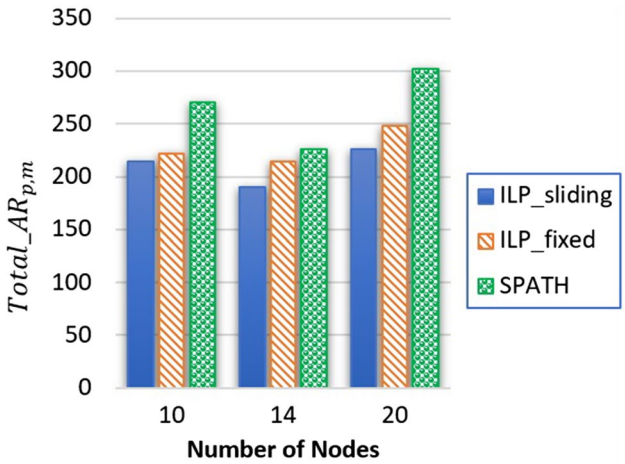

Fig. 5 Total attack radius values for different topologies with LDO demand set

ILP_sliding provides a much more significant improvement in attack radius, ranging from 20 to 28% for all levels of demand overlap. This pattern remains consistent for all topologies considered.

We note that the total value for this objective can seem high, given the number of demands. For example, in Fig. 1, the objective value for all lightpaths is around 900 for the HDO set with shortest path routing or around 45 per lightpath. This is because, for each lightpath the attack radius is summed overall all active intervals. For HDO a demand p is active for 10–24 intervals. So, if we consider $\tau_p = 15$ and assume 2–4 lightpaths are in its attack group in any given interval, then $\sum_m (\boldsymbol{LAR_{p,m}} + \boldsymbol{IAR_{p,m}})$ will be between 30 and 60 for lightpath p.

Figure 3 compares the total attack radius over all lightpaths [Eq. (41)] for the different approaches, obtained by routing 20 demands over DT10 network topology. ILP_sliding again performs better than both ILP_fixed and SPATH approaches, with improvements up to 17% and 40% compared to ILP_fixed and SPATH respectively. Similar patterns are obtained for NSFNET and ARPANET network topologies.

Figure 4 shows the maximum attack radius[Eq. (3)] obtained by the three different approaches, for 14-node NSFNET network. Unlike the case for total attack radius values, there is a noticeable difference in performance between ILP_sliding and ILP_fixed in terms of the maximum attack radius. ILP_sliding is able to reduce the maxARp value by 34–50% compared to ILP_fixed and 40–67% compared to SPATH.

Figure 5 shows the Total_ARp,m [Eq. (42)] values for different network topologies and 20 demands with LDO demands time overlap. The results demonstrate that ILP_sliding is able to consistently reduce the attack radius

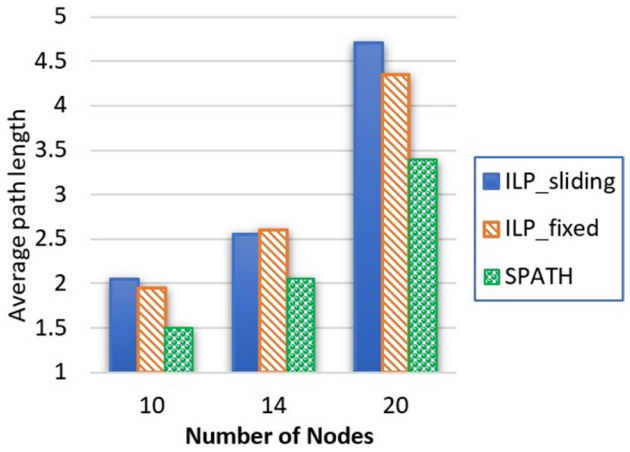

Fig. 6 Average path length for different approaches and network topologies

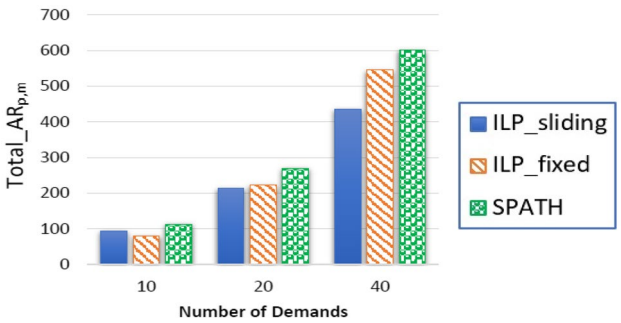

Fig. 7 Total attack radius values for different number of demands with LDO demand set

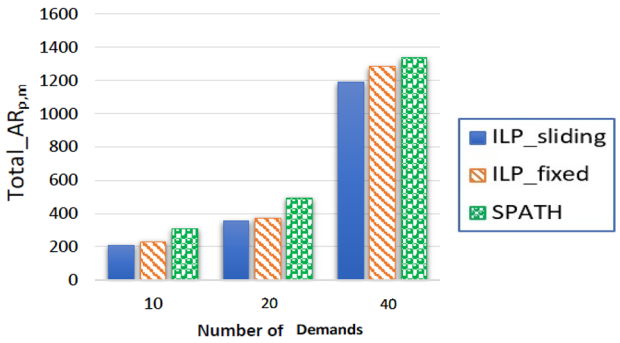

Fig. 8 Total attack radius values for different number of demands with MDO demand set

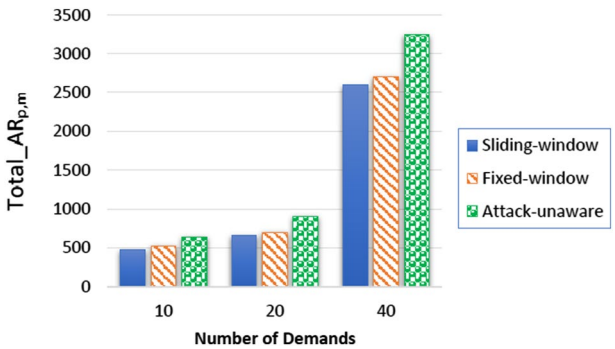

Fig. 9 Total attack radius values for different number of demands with HDO demand set

compared to both ILP_fixed and SPATH, regardless of the network topology. The results for MDO and HDO follow a similar pattern. Although, for each network, the objective value increases steadily, with the increased level of demand overlap (from LDO to HDO). This indicates that vulnerability to attacks increase with more interactions among lightpaths.

The reduction in attack radius is achieved at the expense of slightly longer routes for lightpaths. This is because the attack-aware approaches may sometimes choose longer routes along less congested paths, rather than the shortest path. Figure 6 compares the average path length obtained using our proposed attack-aware approaches versus the attack-unaware shortest path approach for the HDO demands overlap and different network topologies. The average path length of ILP_sliding and ILP_fixed approaches may be up to 1–2 hops longer compared with SPATH approach. For example, for the 14-node topology, the average path length using shortest path routing is 2.05 and using the ILP is around 2.55. Even though this translates to a percentage increase on almost 25%, the actual increase is small. Even though our attack-aware approaches may result in slightly longer paths, this is a worthwhile tradeoff to reduce the vulnerability of lightpaths to potential malicious attacks.

Finally, we note that due to their computational complexity, simulation results for ILP-based solutions of the attack-aware RWA problem are typically only feasible for smaller networks and/or lower number of demands. Therefore, we limited the number of demands in our simulations to 20 in most cases, since for larger demand sets the ILPs often did converge to an optimal solution. However, we ran some additional simulations for the 10-node network with 40 demands. Figures 7, 8 and 9 show how the Total_ARp,m [Eq. (42)] values increase with the size of the demand set for 10 node topology, for LDO, MDO and HDO cases respectively. We see that the attack radius values increase with the demand set size and the amount of demand overlap.

In this section, we have shown the total attack radius values (LAR + IAR) for different approaches and network configurations. We have observed that the LAR values contribute more towards the total attack radius (AR) compared to the IAR values. Typically, LAR contributes 65–85% of the

total AR, while IAR contributes 15–35% of the total AR. This is because for each node *i* traversed by a lightpath *p*, there can be at most deg_i lightpaths in its in-band attack group (IAGp), where deg_i is degree of node *i*. For the topologies considered in this paper, the nodal degree varies between 2 and 4, i.e. $2 \le deg_i \le 4$. For each link i → j traversed by a lightpath *p*, there can be at most $|W|$ lightpaths in its lightpath attack group (LAGp), where $|W|$ is the number of wavelengths in link i → j. For our simulations, we have used $|W| = 8$. Therefore, it makes sense that LAR contributes more heavily to the total AR compared to IAR values.

In our simulations, the total attack radius increased consistently for a given network and demand size, with the amount of demand overlap (i.e. attack radius increases as the *duration* of the demands increase). But there were significant variations in the objective values when the actual demand sets were changed, even for demand sets that had the same number of demands. This means that the attack-radius values depend not only on the number of demands but the actual demands themselves (i.e. start and destination nodes) that were selected. However, despite the variation in the actual attack-radius based objective values for different demand sets, we observed following clear trend: *ILP_sliding* consistently provides the lowest attack-radius, followed by *ILP_fixed* and *SPATH* has the highest attack radius values. This improvement was evident as we varied both the network topologies and demand set sizes.

5 Conclusions and future work

In this study we consider the attack-aware RWA problem for scheduled demands using the fixed and sliding window models. We have presented a new ILP formulation for the fixed window model, with different objectives to minimize the total and the maximum attack radius. We have also shown how this ILP can be extended to handle the sliding window model as well. Our results show that by routing the scheduled demands in a way that reduces sharing of switches and/or fibers among simultaneously active demands, we can reduce the damaging effects of jamming attacks and therefore enhance the network security. We compare and evaluate the performance of the attack-aware fixed window and sliding window scheduling algorithms through extensive simulations. The sliding-window model not only selects an appropriate route and an effective wavelength for the lightpaths, but also assigns a suitable start time for them, within a predefined time range. Our experimental results indicate that, the time flexibility associated with sliding window scheduling gives best objective values compared to fixed window and attack-unaware approaches.

In case of sliding and fixed window scheduled traffic models, the data transmission is continuous, once the lightpath is established between the source and destination nodes. The transmission process doesn't terminate until the entire data is transmitted to the other end. As a future work, it may be possible to divide the scheduled lightpath demand into two or more individual segments and send them separately within the predefined time range. This traffic model is called segmented or non-continuous sliding window scheduled traffic model [37]. It adds another degree of flexibility that can be exploited by various resource allocation techniques. In this work, we have not considered the issue of fault tolerance. In the future, an attack aware RWA for the scheduled traffic model with dedicated and/or shared path protection can be implemented.

Acknowledgements The work of A. Jaekel has been supported by research Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Skorin-Kapov N, Chen J, Wosinska L (2010) A new approach to optical networks security: attack-aware routing and wavelength assignment. IEEE/ACM Trans Netw (TON) 18(3):750–760
2. Ramaswami R, Sivarajan K, Sasaki G (2009) Optical networks: a practical perspective. Morgan Kaufmann, Burlington
3. Ramamurthy B, Feng H, Datta D, Heritage JP, Mukherjee B (1999) Transparent versus opaque versus translucent wavelength-routed optical networks. In: OFC/IOOC. Technical digest. Optical fiber communication conference, 1999, and the international conference on integrated optics and optical fiber communication, vol 1. IEEE, pp 59–61
4. Mas C, Tomkos I, Tonguz OK (2005) Failure location algorithm for transparent optical networks. IEEE J Sel Areas Commun 23(8):1508–1519
5. Furdek M, Skorin-Kapov N, Grbac M (2010) Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation. J Opt Commun Netw 2(11):1000–1009
6. Furdek M, Skorin-Kapov N (2011) Physical-layer attacks in all-optical WDM networks. In: 2011 Proceedings of the 34th international convention MIPRO. IEEE, pp 446–451
7. Deng T, Subramaniam S, Xu J (2004) Crosstalk-aware wavelength assignment in dynamic wavelength-routed optical networks. In: First international conference on broadband networks. IEEE, p 140
8. Skorin-Kapov N, Chen J, Wosinska L (2008) A tabu search algorithm for attack-aware lightpath routing. In: 2008 10th anniversary international conference on transparent optical networks, vol. 3. IEEE, pp 42–45
9. Manousakis K, Ellinas G (2013) Minimizing the impact of in-band jamming attacks in WDM optical networks. In: International

workshop on critical information infrastructures security. Springer, Cham, pp 38–49
10. Jaekel A, Bandyopadhyay S, Al-Mamoori S, Varanasi S (2015) Security-aware dynamic lightpath allocation scheme for wdm networks. In: Proceedings of the 2015 international conference on distributed computing and networking. ACM, p 12
11. Al-Mamoori S, Jaekel A, Bandyopadhyay S, Varanasi S (2015) Security-aware dynamic rwa for reducing in-band and out-of-band jamming attacks in wdm optical networks. J Netw 10(11):587–597
12. Manousakis K, Ellinas G (2016) Attack-aware planning of transparent optical networks. Opt Switch Netw 19:97–109
13. Zhao H, Al Mamoori S, Jaekel A (2016) Attack-aware rwa using knowledge of demand holding times. In: 2016 IEEE Canadian conference on electrical and computer engineering (CCECE). IEEE, pp 1–4
14. Furdek M, Chen J, Skorin-Kapov N, Wosinska L (2011) Compound attack-aware routing and wavelength assignment against power jamming. In: 2011 Asia communications and photonics conference and exhibition (ACP). IEEE, pp 1–3
15. Nizampatnam M, Al Mamoori S, Jaekel A (2017) Minimizing attack radius of scheduled connections in WDM networks. In: 2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE). IEEE, pp 1–4
16. Zang H, Jue JP, Mukherjee B (2000) A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks. Opt Netw Mag 1:47–60
17. Xin C, Wang B, Cao X, Li J (2006) Logical topology design for dynamic traffic grooming in WDM optical networks. J Lightwave Technol 24(6):2267–2275
18. Charbonneau N, Vokkarane VM (2012) A survey of advance reservation routing and wavelength assignment in wavelength-routed WDM networks. IEEE Commun Surv Tutor 14(4):1037–1064
19. Médard M, Chinn SR, Saengudomlert P (2001) Node wrappers for QoS monitoring in transparent optical nodes. J High Speed Netw 10(4):247–268
20. Rejeb R, Leeson MS, Green RJ (2006) Fault and attack management in all-optical networks. IEEE Commun Mag 44(11):79–86
21. Skorin-Kapov N, Furdek M, Zsigmond S, Wosinska L (2016) Physical-layer security in evolving optical networks. IEEE Commun Mag 54(8):110–117
22. Furdek M (2011) Physical-layer attacks in optical WDM networks and attack-aware network planning. Eur J Oper Res 178(2):1160–1167
23. Wu T, Somani AK (2005) Cross-talk attack monitoring and localization in all-optical networks. IEEE/ACM Trans Netw 13(6):1390–1401
24. Marija F, Skorin-Kapov N (2013) Attack-survivable routing and wavelength assignment for high-power jamming. In: ONDM 2013, Brest, France
25. Dahan D, Mahlab U (2017) Security threats and protection procedures for optical networks. IET Optoelectron 11(5):186–200
26. Tao D, Subramaniam S (2005) QoS-friendly wavelength assignment in dynamic wavelength-routed optical networks. Photonic Netw Commun 10(1):5–22
27. Skorin-Kapov N, Furdek M, Pardo RA, Marino PP (2012) Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms. Eur J Oper Res 222(3):418–429
28. Furdek M, Skorin-Kapov N, Wosinska L (2016) Attack-aware dedicated path protection in optical networks. J Lightwave Technol 34(4):1050–1061
29. Marija F, Skorin-Kapov N, Tzanakaki A (2014) Survivable routing and wavelength assignment considering high-powered jamming attacks. In: 2014 19th European conference on networks and optical communications (NOC)
30. Marija F, Skorin-Kapov N, Wosinska L (2011) Shared path protection under risk of high-power jamming. In: SPIE/OSA/IEEE Asia communications and photonics, 2011, Shanghai, China
31. Nizampatnam M (2016) Attack aware RWA for sliding window scheduled traffic model. M.Sc. thesis, Computer Science, University of Windsor
32. IBM ILOG CPLEX optimization studio. https://www.ibm.com/products/ilog-cplex-optimization-studio. Accessed 30 Jul 2019
33. Wang Z, Dueñas-Osorio L, Padgett JE (2015) A new mutually reinforcing network node and link ranking algorithm. Sci Rep 5:15141
34. Cui X, Li Y, Cao Y, Zhang H, Guo Y, Zheng X (2007) Dynamic priority-based alternate routing for multiple classes of traffic in intelligent optical networks. Opt Eng 46(2):025002
35. Das R, Bandyopadhyay S, Al Mamoori S, Jaekel A (2017) Dynamic provisioning of fault tolerant optical networks for data centers. In: 2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE). IEEE, pp 1–4
36. Jaekel A, Chen Y (2009) Resource provisioning for survivable WDM networks under a sliding scheduled traffic model. Opt Switch Netw 6(1):44–54
37. Chen Y, Jaekel A, Bari A (2011) A new model for allocating resources to scheduled lightpath demands. Comput Netw 55(13):2821–2837