Secure Transport Service Provisioning Over Partially-secured Optical Networks

Huifang Xiong[1], Wei Wang[1], Qiaojun Hu[1], Yongli Zhao[1], Yongyuan Liu[2], Xiaoyu Yu[1], Yajie Li[1], Jie Zhang[1]
[1]School of Electronics Engineering, Beijing University of Posts and Telecommunications, 100876, China
[2]Beitsing Communications Technology Co., LTD. 100082, Beijing, China
jie.zhang@bupt.edu.cn

Abstract—**In partially-secured optical networks, we develop four algorithms to allocate bandwidth for services with heterogeneous security requirement. Results show that the algorithms can reduce the exposure length and service blocking probability.**

Keywords—physical-layer security, partially-secured optical networks, security demand, service provisioning.

I. Introduction

As optical networks are carrying more and more traffic and mission-critical applications, security issues are becoming more significant for optical networks [1]. Many kinds of communication services in optical networks raise security requirements according to the sensitivity of user contents or applications. For example, the private lines for financial and political users always have a high demand for communication services security.

Since optical communication systems carry applications' data transparently, it is vulnerable to eavesdropping, interruption, and other types of attacks. With the incidents of eavesdropping and destruction of optical networks in recent years, the stereotype that optical networks have inherent security has been gradually broken [2]. Major telecom operators and suppliers are increasingly interested in physical layer security, which has promoted the research and development of physical layer security technologies [3].

The existing physical layer security technologies can be divided into optical domain encryption, monitoring & early warning, security reinforcement, network regeneration, and network confrontation [4]. By using optical signal processing, the optical communications community has explored several methods to protect optical channels in the physical layer [2], including error-free key distribution [5], all-optical logic for encryption [6] and optical steganography [7].

In physical-layer secured optical networks, the traditional traffic grooming algorithms are no longer applicable for mapping sub-wavelength services with security demands onto optical channels with security attributes. In this case, the security capabilities were taken into consideration in various optical networking issues (e.g., energy-efficient service mapping in IP over WDM networks [8], routing and spectrum allocation issues in EON [9], and traffic grooming in WDM networks [10]).

However, in real optical networks, it is hard to assume all the network elements with physical-layer security capability, as the physical-layer security comes with new network equipment and it is impossible to upgrade all the network elements simultaneously. Therefore, in the upgrading process, the upgraded infrastructure with security capabilities will coexist with traditional infrastructure, forming partially-secured optical networks. In partially-secured optical networks, parts of the optical channels are secured with the physical-layer security approaches, while others are not. In this case, it is of significant importance to re-investigate the security-aware service provisioning problem for partially-secured optical networks.

In this work, we model the partially-secured optical networks and propose four algorithms for provisioning sub-wavelength transport services with heterogeneous security demands. Simulation results show that the best proposed algorithm can reduce services' exposure length by an average of 60% and blocking probability by an average of 8%, by orchestrating the communication and security resources.

II. Secure Optical Network Models

A. Partially-secured Optical Network Model

In partially-secured optical networks, the lightpaths or optical channels could be secured with physical-layer encryption approaches or not. Note that, the optical channels between two un-upgraded nodes or between one upgraded node with one un-upgraded node will remain insecure. Without losing generality, we model the physical-layer security attribute in a channel-oriented manner for simplification and thus we do not need to worry about the security capability of each optical node. In this case, we model the connectivity of all optical channels as a graph $G(V, E)$, where V represents the set of optical switch nodes and E is the set of optical channels. The bandwidth and security status of optical channel $l \in E$ are given by B_l and a binary flag S_l. Compared with insecure optical channels, the bandwidth in secure channels can be deemed as secured naturally.

B. Transport Service Model with Security Demand

In partially-secured optical networks, one sub-wavelength service request can be represented by $r(s, d, w, t)$, in which s and d specify the source and destination nodes, w represents the bandwidth demand, and t indicates the security demand.

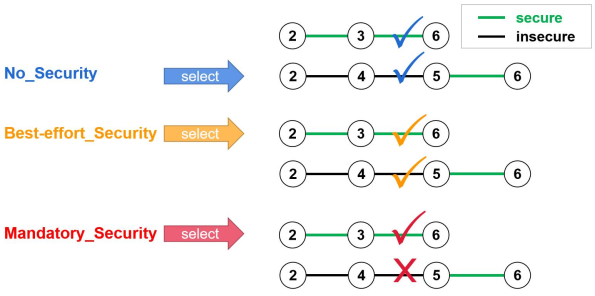


Fig. 1. Three types of security demands for connection requests.

This work is supported by NSFC (62101063, 62021005, 61831003) and Shenzhen Virtual University Park (Svup010).

We define the following three types to denote the general security demand for transport services.

1) No_Security, meaning the connection request does not require to go through secure channels, at all.

2) Best-effort_Security, meaning the connection request prefers to go through secure channels, but insecure channels are also acceptable to it.

3) Mandatory_Security, meaning the connection request does not accept insecure channels and needs to go through secure channels throughout the end-to-end path.

C. Problem Statement

In partially-secured optical networks, the service provisioning problem is different from that of traditional optical networks. In addition to meeting users' bandwidth requirements, we also need to ensure that users' security requirements are satisfied. In addition, the security status of different channels in partially-secured optical networks is different, which greatly affects the provisioning process of transport services. Therefore, it is necessary to re-investigate the service provisioning process in partially-secured optical networks. The service provisioning problem that considers the security demand is formulated as follows. Given a partially-secured optical network graph $G(V, E)$, in which only parts of the optical channels are secured with physical-layer security approaches, and a service request $r(s, d, w, t)$, we find a candidate path that can meet the desired security t between s and d and allocate bandwidth w.

III. Security-aware Service Provisioning Algorithm

We propose four security-aware service provisioning algorithms to allocate bandwidth for requests with different security demands.

A. Minimum Exposure-Ratio Algorithm

In partially-secured optical networks, an end-to-end path for a transport service may traverse through both secure and insecure channels. In general, more insecure channels in the end-to-end path mean less security, because the eavesdropper has a higher possibility of performing successful attacks via insecure channels. In this regard, we introduce a new metric exposure-ratio (ER) to measure the security level of an end-to-end path, and it is given by Eqn. (1), in which l_{insec} is the length of all insecure channels and l_{sec} is the length of all secure channels' length. Note that, in the security context, one may claim that the security of a connection with one insecure hop is the same as the security of a connection with multiple insecure hops. However, from the infrastructure perspective, going through more insecure channels means a higher probability of being eavesdropped successfully, under the assumption that the specific path for a service is unknown to the eavesdropper.

$$E_p = \frac{l_{\text{insec}}}{l_{\text{insec}} + l_{\text{sec}}} \tag{1}$$

In this case, we propose the minimum exposure-ratio (MER) algorithm. In Algorithm 1, firstly, the MER algorithm picks out all paths that meet the bandwidth requirement. Secondly, it picks out the paths that best meet the security requirement. Finally, it selects the path with the minimum path length. The path selection criterion for different types of security is different, as follows:

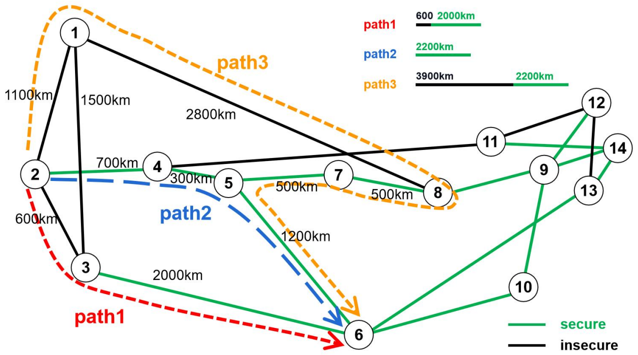


Fig. 2. Examples of path selection for security-aware service provisioning algorithms.

For the No_Security service requests, the MER prefers the path with the maximum E_p (e.g., path-3 with the maximum E_p in Fig.2), to save the secured bandwidth for security-sensitive requests. For the Best-effort_Security service requests, the MER prefers the path with the minimum E_p (e.g., path-2 with the minimum E_p in Fig.2). For the Mandatory_Security service requests, the MER only takes the path whose $E_p = 0$ (e.g., path-2 whose $E_p = 0$ in Fig.2).

Algorithm 1: Minimum Exposure-Ratio (MER) Algorithm

```
input  : A topology $G(V, E)$, a request $r(s, d, w, t)$;
output: The $best\_path$ for request $r$;
search for simple paths as a set $P$, from $s$ to $d$;
for $p$ in $P$ do
    $BW_p \leftarrow$ the min $B_l$ of channels in $p$;
    if $BW_p > w$ then
        put $p$ into $P'$
    end
end
for $p$ in $P'$ do
    $L_p \leftarrow$ the total path length of $p$;
    $l_{insec} \leftarrow$ the length sum of insecure channels of $p$;
    $Ep\_p \leftarrow l_{insec}/Lp$ ;
    if $t ==$ "$No\_Security$" then
        put $p$ with max $Ep\_p$ into $P*$
    end
    if $t ==$ "$Best-effort\_Security$" then
        put $p$ with min $Ep\_p$ into $P*$
    end
    if $t ==$ "$Mandatory\_Security$" then
        put $p$ with $Ep\_p == 0$ into $P*$
    end
end
if $len(P*) > 1$ then
    for $p$ in $P*$ do
        $best\_path \leftarrow p$ with min $L_p$
    end
end
output $best\_path$;
```

B. Strict Minimum Exposure-Ratio Algorithm

For the Best-effort_Security connections, the path selected by MER may go through insecure channels, resulting in a higher risk of data leaking. So, we propose the strict minimum exposure-ratio (S-MER) algorithm as an enhanced alternative. S-MER also takes the path ER as the decision indicator when making path selection. But compare to MER, S-MER provides stricter quality of security for the Best-effort_Security requests. The criterion is as follows:

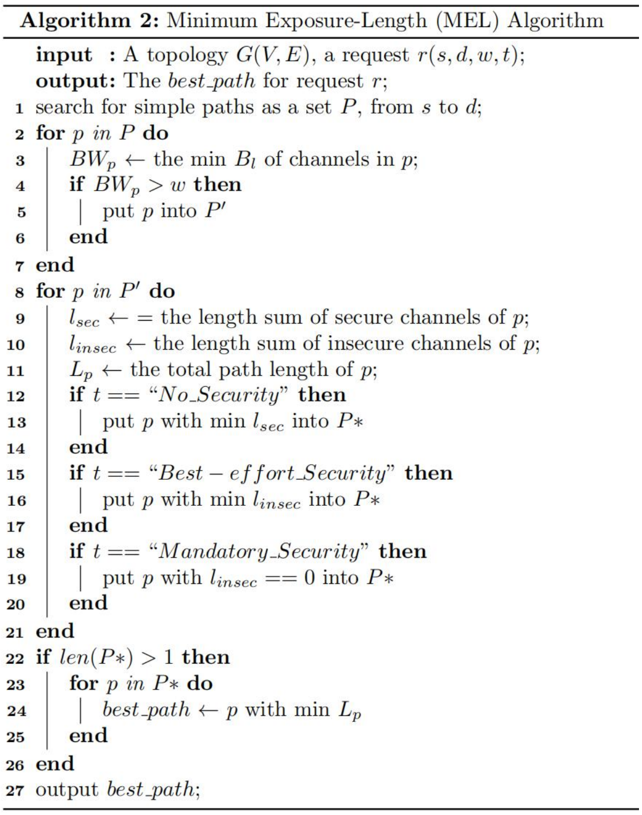
For the No_Security service requests, the S-MER prefers the path with the maximum E_p (e.g., path-3 with the maximum E_p in Fig.2). For both the Best-effort_Security and the Mandatory_Security service requests, the S-MER only takes the path whose $E_p = 0$ (e.g., path-2 whose $E_p = 0$ in Fig.2).

C. Minimum Exposure-Length Algorithm

In general, MER and S-MER can provide good solutions for security-aware services, but they have limitations in some special scenarios. In the first two algorithms, the ER is used to measure the security level of an end-to-end connection, but it may not accurate enough in some cases, as one may claim that longer insecure links/channels lead to more possible locations for eavesdropping operations. Therefore, we further introduce another metric exposure length (EL), which is the length (l_{insec}) of all insecure channels in the end-to-end path. Accordingly, we propose the minimum exposure-length (MEL) algorithm.

The procedures of MEL are shown in Algorithm 2, and the path filtering steps are similar to that of the MER algorithm. In the path selection phase based on security requirements, MEL takes the EL as the decision indicator. The specific criterion is as follows:

For the No_Security service requests, MEL selects the path with the minimum l_{sec} to save security resources (e.g., path-1 with the minimum l_{sec} in Fig. 2). For the Best-effort_Security service requests, MEL selects the paths with the minimum l_{insec} (e.g., path-2 with the minimum l_{insec} in Fig. 2). For the Mandatory_Security service requests, MEL selects the paths whose $l_{insec}= 0$ (e.g., path-2 whose $l_{insec}= 0$ in Fig. 2).



Algorithm 2: Minimum Exposure-Length (MEL) Algorithm

```
input  : A topology $G(V,E)$, a request $r(s,d,w,t)$;
output: The $best\_path$ for request $r$;
search for simple paths as a set $P$, from $s$ to $d$;
for $p$ in $P$ do
    $BW_p \leftarrow$ the min $B_l$ of channels in $p$;
    if $BW_p > w$ then
        put $p$ into $P'$
    end
end
for $p$ in $P'$ do
    $l_{sec} \leftarrow =$ the length sum of secure channels of $p$;
    $l_{insec} \leftarrow$ the length sum of insecure channels of $p$;
    $L_p \leftarrow$ the total path length of $p$;
    if $t ==$ "$No\_Security$" then
        put $p$ with min $l_{sec}$ into $P*$
    end
    if $t ==$ "$Best-effort\_Security$" then
        put $p$ with min $l_{insec}$ into $P*$
    end
    if $t ==$ "$Mandatory\_Security$" then
        put $p$ with $l_{insec} == 0$ into $P*$
    end
end
if $len(P*) > 1$ then
    for $p$ in $P*$ do
        $best\_path \leftarrow p$ with min $L_p$
    end
end
output $best\_path$;
```

D. Strict Minimum Exposure-Length Algorithm

Similar to S-MER, we further propose the strict minimum exposure-length (S-MEL) algorithm to provide enhanced security for the Best-effort_Security service requests. The path selection criterion for S-MEL is as follows:

For No_Security connections, S-MEL selects the paths with the minimum l_{sec} to save security resources (e.g., path-1 with the minimum l_{sec}, in Fig. 2). For both Best-effort_Security and Mandatory_Security connections, S-MEL selects the paths whose $l_{insec} = 0$ (e.g., path-2 whose $l_{insec} = 0$ in Fig. 2).

IV. Illustrative Numerical Results

In the simulation, we use the NSFNET as the simulation topology. According to the security features in partially-secured optical networks, each link could be secured by physical-layer approaches or not, and we have introduced the ratio of secure links (RSL) to control the proportion of the physical-layer secure links. We consider that each link has one single optical channel for accommodating sub-wavelength services. Each channel/link is initialized with 10,000 Gbps bandwidth capacity. For each round of the simulation, we generate connection requests following the Poisson process, with leaving rate fixed at 0.1. The bandwidth demand of each request is generated randomly, following a uniform distribution within the range [0, 5] Gbps. The security demand is also generated randomly, following the uniform distribution among the three security types.

We conducted two groups of simulations. In the first group, we test the performance of the proposed algorithms under different RSLs, which increase from 30% to 80% with a step of 10%. In this case, the arrival rate of connection requests is fixed at 70%. In the second group, we test the performance of the four algorithms under different workloads by increasing the request arrival rate from 40%-90% with a step of 10%. In this case, the RSL is fixed at 60%. We compare the performance of the proposed algorithms with the shortest path algorithm (SPF), in terms of the blocking probability/ratio, the average exposure length, and the end-to-end security ratio.

A. Blocking Probability/Ratio

The blocking probability (BP) is a typical metric for network performance and it is given by Eqn. (2), in which N_f is the number of blocked service requests and N_a is the number of all service requests.

$$R_{block} = \frac{N_f}{N_a} \tag{2}$$

Fig. 3 shows the BP under various RSLs. MEL and MER achieve the lowest BP. As to the comparison among S-MER, S-MEL, and SFP, their superiority is sensitivity to the RSL. When the RSL is less than 60%, the BP of S-MEL and S-MER is higher than that of SPF, while their BP becomes lower than that of SPF after the RSL exceeds 60%. That's because S-MEL and S-MER follow a strict security constraint for the Best-effort_Security requests and Mandatory_Security requests, and such constraint will lead to increased competition on secure channels for lower RSL (secure links are not sufficient). With the increase of RSL, the competition over secure channels is relieved, so the BP of all algorithms decreases.

Fig. 4 shows the BP under various workloads. MEL achieves the lowest BP, and the SPF achieves the highest BP, for all workloads. Moreover, the BP of S-MER and S-MEL is higher than that of MER and MEL. This makes sense because S-MER and S-MEL have stricter security constraints for the service with security demand. With the increase of the given workload, the BP of all algorithms increases, and MEL outperforms MER. This is indicating that the MEL algorithm can help the network accommodate more transport services.

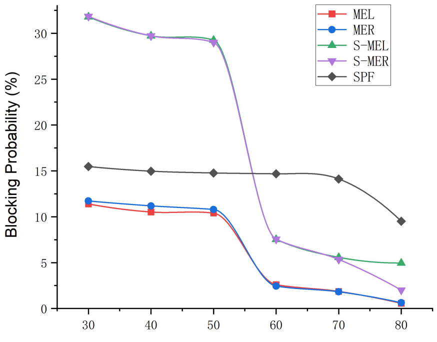


Fig. 3. Blocking probability under various RSLs.

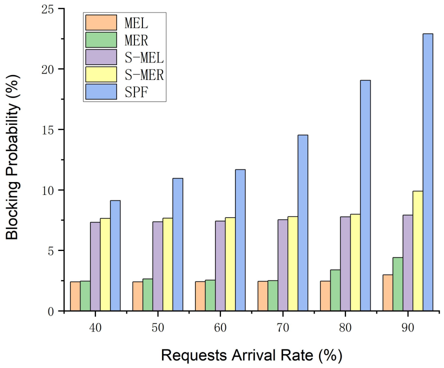


Fig. 4. Blocking probability under various traffic loads.

B. Average Exposure Length

To measure the security strength of the transport services in optical networks, we proposed a new metric - average exposure length (AEL). The AEL is calculated as the average value of the insecure link length (l_{insec}) for all the services with Best-effort_Security or Mandatory_Security demand.

Fig. 5 shows the AEL under various RSLs. The AEL of S-MEL and S-MER is always zero for all RSLs. The reason is that they don't accept insecure channels for both Best-effort_Security or Mandatory_Security service requests. MEL and MER achieve higher AEL than S-MEL and S-MER. This is because the MEL and MER algorithms relax the security constraint for the Best-effort_Security services. Moreover, the AEL of MEL is lower than that of MER, because the nature of MEL is to minimize the insecure length of each service path. With the increase of RSL, more links/channels become physically secured, and thus the competition over secure channels decreases, decreasing the AEL. When RSL reaches 80%, all algorithms achieve similar AEL perfomance.

Fig. 6 shows the AEL under various workloads. Similar to Fig. 5, the AEL of S-MEL and S-MER is always zero, and the SPF achieves the highest AEL, for all the workloads. Moreover, MEL outperforms MER in terms of AEL. Again, this is also because the nature of MEL is to minimize the insecure length of each service path.

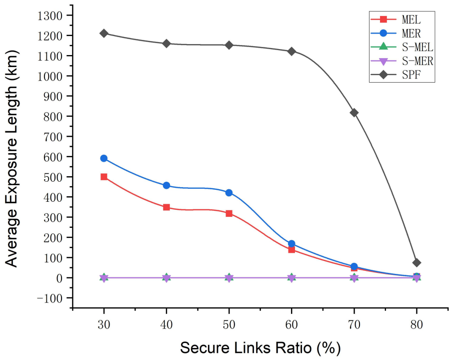


Fig. 5. Average exposure length under various RSLs.

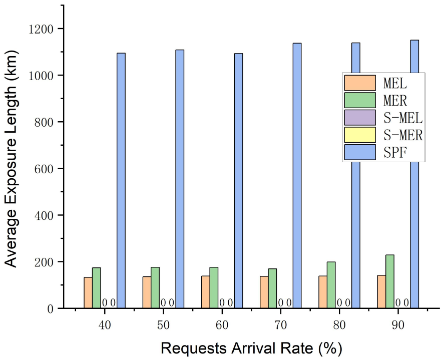


Fig. 6. Average exposure length under various traffic loads.

C. End-to-End Security Ratio

To measure the security transport services quality, we proposed a new metric - end-to-end security ratio (E2ESR), as Eqn. (3). In Eqn. (3), N_{ss} is the number of the successfully provisioned Best-effort_Security and Mandatory_Security requests whose path doesn't go through any insecure channel, and N_{sa} is the number of all successfully provisioned Best-effort_Security requests and Mandatory_Security requests.

$$R_{a\text{-}safe} = \frac{N_{ss}}{N_{sa}} \tag{3}$$

Fig. 7 shows the E2ESR under various RSLs. It can be noted that the E2ESR of S-MEL and S-MER reaches 100% for all RSLs. This is because S-MEL and S-MER force all links in the end-to-end path of the Best-effort_Security and Mandatory_Security connections are secured. MEL and MER perform worse than S-MEL and S-MER. This is because the MEL and MER algorithms relax the security constraint for the Best-effort_Security services. Moreover, for most RSLs that are less than 70%, MEL achieves higher E2ESR, but MER achieves higher E2ESR for RSLs over 70%. This result indicates that the MEL works well for most network settings, while the MER is more suitable for networks with more than 70% of the links are physically secured. All the proposed algorithms outperform SPF because the SPF is not aware of the security. With the increase of RSL, more channels become physically secured and thus the E2ESR performance for MEL, MER, and SPF improve accordingly.

Fig. 8 shows the E2ESR under various workloads. Similar to Fig. 7, the E2ESR of S-MEL and S-MER reaches 100%, and the SPF achieves the lowest E2ESR, for all the workloads. This is again determined by the enhanced security constraint of S-MEL and S-MER and the security unawareness of SPF. MEL and MER achieve similar E2ESR under lower workloads, but MEL outperforms MER under heavy workloads. This is because the MER's objective of minimizing the ER will lead to traffic detouring through some longer paths, exacerbating the congestion when the network is overloaded.

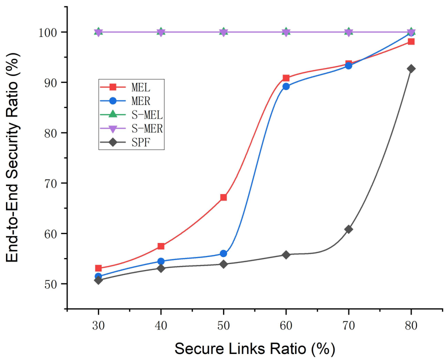


Fig. 7. End-to-end security ratio under various RSLs.

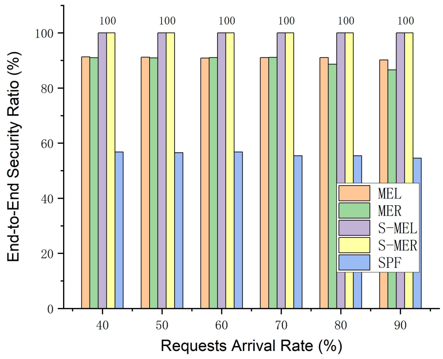


Fig. 8. End-to-end security ratio under various traffic loads.

Discussions: In summary, compared with the SPF algorithm, our proposed algorithms can better utilize the networks' security capabilities by reducing BP & AEL and increasing E2ESR. Comparing the proposed algorithms, S-MEL and S-MER can provide a higher quality of security for services in terms of AEL and E2ESR, with the cost of higher BP. In contrast, MEL and MER achieve lower BP, with higher AEL and E2ESR. Moreover, MEL outperforms MER in most cases. The overall result suggests that the MEL algorithm might be the best choice for balancing the networking and security performances, while S-MEL and S-MER could be better candidates for the network when the priority of security is higher.

V. Conclusions

In this paper, we focused on the service provisioning problem for optical networks with physical-layer security capabilities. We built a partially-secured optical network model and proposed four security-aware service provisioning algorithms for accommodating sub-wavelength transport services with heterogeneous security demands. Simulation results showed that the minimum exposure-length (MEL) and minimum exposure-ratio (MER) algorithms can better utilize the bandwidth and security resources jointly, in terms of the service's exposure length and the blocking probability. In addition, the strict minimum exposure-length (S-MEL) and strict minimum exposure-ratio (S-MER) algorithms can provide a higher quality of security to the service request with security demand, with the cost of a higher blocking probability.

References

[1] M. Furdek, et al., "Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats [Invited]," in Journal of Optical Communications and Networking, vol. 13, no. 2, pp. A144-A155, February 2021

[2] M. P. Fok, Z. Wang, Y. Deng and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 725-736, Sept. 2011

[3] N. Skorin-Kapov, M. Furdek, S. Zsigmond and L. Wosinska, "Physical-layer security in evolving optical networks," in IEEE Communications Magazine, vol. 54, no. 8, pp. 110-117, August 2016, doi: 10.1109/MCOM.2016.7537185.

[4] N. Skorin-Kapov, J. Chen and L. Wosinska, "A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment," in IEEE/ACM Transactions on Networking, vol. 18, no. 3, pp. 750-760, June 2010, doi: 10.1109/TNET.2009.2031555.

[5] K. Zhu, J. Zhang, Y. Li, W. Wang, X. Liu and Y. Zhao, "Experimental demonstration of error-free key distribution without an external random source or device over a 300-km optical fiber," Opt. Lett, vol. 47, pp. 2570-2573, 2022.

[6] J. M. Castro, I. B. Djordjevic and D. F. Geraghty, "Novel super structured Bragg gratings for optical encryption," in Journal of Lightwave Technology, vol. 24, no. 4, pp. 1875-1885, April 2006

[7] B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express, vol. 14, pp. 3738–3751, 2006.

[8] Y. Lui, G. Shen, and S. K. Bose, "Energy-Efficient Opaque IP over WDM Networks with Survivability and Security Constraints," in Asia Communications and Photonics Conference 2013, AF3G.4.

[9] F. Yousefi, A. G. Rahbar, "Novel crosstalk, fragmentation-aware algorithms in space division multiplexed- Elastic Optical Networks (SDM-EON) with considering physical layer security," Optical Switching and Networking, Volume 37, 100566, 2020.

[10] T. Liu et al., "Security-aware Service Mapping in Physical-layer Secured Optical Transport Networks," 2022 20th International Conference on Optical Communications and Networks (ICOCN), Shenzhen, China, 2022, pp. 1-3, doi: 10.1109/ICOCN55511.2022.9901265.