引用本文：陈孝莲，纪元，过烽，等. SD-EON 业务安全等级感知的低时延路由频谱分配算法[J]. 光通信技术，2021，45(5)：11-15.

SD-EON 业务安全等级感知的低时延路由频谱分配算法

陈孝莲[1]，纪 元[1]，过 烽[1]，郭 宏[2]，张 杰[2*]

（1.国网江苏省电力有限公司 无锡供电分公司，江苏 无锡 214000；2.北京邮电大学 信息光子学与光通信国家重点实验室，北京 100876）

摘要：光网络中普遍存在着普通业务和安全业务，为了将安全业务配置到安全链路进行传输，规避普通业务占用安全链路，降低业务请求光路建立时延，提出了业务安全等级感知的低时延路由频谱分配算法。算法将网络物理拓扑分为安全虚拟拓扑和普通虚拟拓扑，充分考虑了业务安全类别和链路差别，通过运用安全虚拟拓扑将安全业务配置到安全链路进行传输，回避 Eve 窃听到有效的安全业务数据。算法的并行建路策略减少了光路的平均建立时延和业务的阻塞率，通过实验仿真验证了算法的有效性。

关键词：低时延；路由频谱分配；安全业务；虚拟拓扑

中图分类号：TN929.1　**文献标志码**：A　**文章编号**：1002-5561(2021)05-0011-05

DOI：10.13921/j.cnki.issn1002-5561.2021.05.003　开放科学(资源服务)标识码(OSID)：

Low delay routing spectrum assignment algorithm with service security level awareness in SD-EON

CHENG Xiaolian[1], JI Yuan[1], GUO Feng[1], GUO Hong[2], ZHANG Jie[2*]

(1. Wuxi Power Supply Branch, State Grid Jiangsu Electric Power Co., Ltd., Wuxi Jiangsu 214000, China; 2. State key laboratory of information photonics and optical communications, Beijing University of posts and telecommunications, Beijing 100876, China)

Abstract: The common and secure services generally exist in optical networks. For the purpose of configuring the security service to the security links for transmission, avoiding the common services occupying the security spectrum, and reducing the optical connections set-up delay of the service requests, a low delay routing spectrum assignment algorithm with service security level awareness is proposed. The algorithm divides the network physical topology into security virtual topology and common virtual topology. The service security category and link difference are fully considered. By using the security virtual topology, the security service is configured to the security link for transmission, avoiding Eve eavesdropping the effective security service data. The parallel routing strategy of the algorithm reduces the average set-up delay of the optical connections and the blocking rate of the services, and the effectiveness is verified by experimental simulation.

Key words: low delay; routing spectrum assignment; security request; virtual topology

0 引言

随着光纤通信技术的快速发展，越来越多的业务数据在光通信网络中传输[1-2]。光网络中普遍存在着普通业务和安全业务[3]，这些业务能够通过波分复用方式在一根光纤中传输。安全传输光链路由于部署了安全传输策略具备防窃听能力[4]，但是安全业务建立光路需查找具备安全传输能力的光链路，增加了光路建立时延。这要求在光网络中为业务建立光路时考虑业务安全类别和光路建立时延，在确保业务数据安全的前提下对业务数据进行低时延、高速率传输是未来光网络的发展目标[5]。

光网络安全问题分为光层信息安全和物理层安全，其中后者对光网络设备威胁更大。为提高光网络的物理层安全性，研究光网络攻击感知路由频谱分配非常重要。文献[6]考虑了物理节点对业务请求的安全系数来进行路由频谱分配，将业务按照某种排序策略

收稿日期：2020-08-06

基金项目：国网江苏省电力有限公司科技项目(J2019124)资助；国家自然科学基金重点项目(61831003)资助。

作者简介：陈孝莲，女(1977—)，硕士，正高级工程师，长期从事无锡电力通信、信息专业管理和运维工作，2014 年入选国家电网公司信通专业领军人才，获江苏省电力公司多项荣誉。负责和参与了电力系统多个科技项目的研究，如国家“863”科技项目示范区建设、OPLC 和 OPPC 故障诊断与在线监测系统研究项目等。

*** 通信作者**：张杰(E-mail: jie.zhang@bupt.edu.cn)。

进行排序,为每个业务选择多条满足业务最低安全级别要求的光链路,通过遗传算法为业务选择最优的路由频谱分配方案。这种遗传算法满足了业务在光链路传输的安全级别要求,能够有效减小网络中的最大占用频隙号,提高光网络的频谱利用率。算法取得了很好的效果,但是在窃听模型中,假设 Eve 能力无限,Eve 能够窃听到无安全传输能力光链路的全部信息[7]。另外,光节点安全功能需配置到光链路,将光纤中所有频谱配置为安全传输链路增加网络运维费用和光路建立时延。文献[8]在业务未到达前预先计算出路由频谱分配方案来降低光路建立时延,算法充分结合了静态路由频谱分配(RSA)算法和动态 RSA 算法的优点,规避物理损伤对业务光链路建立的影响,减少了业务光路平均建立时延,增加了频谱资源利用率,但未考虑业务安全类别。软件定义弹性光网络(SD-EON)频谱使用更加灵活高效,能够获取全网设备信息和拓扑信息,充分利用虚拟拓扑等新技术更好地对光网络资源集中控制[9],考虑业务安全类别和链路差别,为业务提供低时延光路建立和高速数据传输。但是,文献[9]未综合考虑业务安全类别、链路差别和光路建立时延的相互约束关系,进行区分业务安全类别的低时延光路建立。

为解决上述问题,本文在 SD-EON 架构中提出业务安全等级感知的低时延路由频谱分配(SECURITYA-RSA)算法。在为业务请求建立光路时,从全局的角度考虑业务安全类别、链路差别和光路建立时延之间的关系,实现区分业务安全类别的光路低时延建立。

1 SECURITYA-RSA 算法

1.1 SECURITYA-RSA 算法的控制模型

为了描述 SECURITYA-RSA 算法的思想,算法使用的符号如表 1 所示。

本文假设 SD-EON 中无波长转换器,并且每个连接都是端到端的全光连接。因此,对于所有光链接,业务频谱分配保持不变。当算法进行频谱分配时,遵守频谱连续性、一致性和冲突性的约束。另外,SECURITYA-RSA 策略还遵守下列约束:

①安全业务只能在安全拓扑建立光路,使用安全拓扑频隙,频隙使用需满足:

$$S_R \geqslant C, R_s \in G^* \tag{1}$$

②普通业务只能在普通拓扑建立光路,使用普通拓扑频隙,频隙使用需满足:

$$1 \leqslant S_R \leqslant N, R_n \in G' \tag{2}$$

表 1 网络元素符号及其意义

符号	意义	符号	意义
V_i	V_i 表示节点 i,所有节点集合称为 V	$E_{i,j}$	从节点 i 到节点 j 的光链路
$G(V,E)$	网络物理拓扑,简称 G	$G'(V',E')$	普通虚拟拓扑,简称普通拓扑 G';V' 和 E'为普通拓扑中点集合和边集合
$G^*(V^*,E^*)$	安全虚拟拓扑,简称安全拓扑 G^*;V^* 和 E^* 为安全拓扑中点集合和边集合	R_n	普通业务
R_s	安全业务	S_R	普通业务或安全业务占用频隙的序号
$S_s[i]$	第 i 条光纤链路分配给安全业务频隙数	$S_n[i]$	第 i 条光纤链路分配给普通业务频隙数
N	光纤链路中频隙数	C	频隙序号常数
N_L	网络中光纤链路数	N_{th}	用于建立光路的线程数
$BIT_s[i]$	若第 i 个频隙分配给安全拓扑,则 $BIT_s[i]=1$;若无,则 $BIT_s[i]=0$。	$BIT_n[i]$	若第 i 个频隙分配给普通拓扑,则 $BIT_n[i]=1$;若无,则 $BIT_n[i]=0$。
N_r	业务总数	N_s	安全业务个数
N_n	普通业务个数	T	时延常量
N_w	安全业务被窃听个数	$f(u)$	第 u 个业务光路建立时延
ρ	安全业务被窃听比例	$A(u)$	u 个业务的光路平均建立时延

③频隙只能属于安全拓扑或普通拓扑,需满足:

$$\sum_{i=1}^{N} BIT_s[i]BIT_n[i]=0 \tag{3}$$

④安全拓扑中频隙个数和普通拓扑中频隙个数的和等于物理拓扑光纤链路中频隙总数,普通业务个数和安全业务个数的和等于总业务个数,关系式如下:

$$\sum_{i=1}^{N_L} S_s[i]+S_n[i]=N_L \times N \tag{4}$$

$$N_r=N_s+N_n \tag{5}$$

⑤在窃听模型中,假设 Eve 能力无限,在无安全传输能力的链路能窃听到全部信息,在有安全传输能力的链路窃听不到信息。安全业务被窃听比例定义为:

$$\rho=N_w/N_s \tag{6}$$

1.2 SECURITYA-RSA 算法的并行建路策略

光网络中的时延主要包括信号的传播时延、控制器的策略处理时延、通信时延、设备配置时延和软/硬件设备的处理时延等。其中,软/硬设备的处理时延在网络评估和设计阶段已经形成,难以进一步提升;信号

的传播时延、通信时延能够通过优化光链接的路由距离降低；控制器的策略处理时延、通信时延和设备配置时延能够通过并行配置和建路策略进行优化。光网络中需要建立的多条光链路，如果没有公共的点（端）或边，称为路径不重合。现在光网络中业务安全类别有安全业务和普通业务[10]，安全业务使用安全链路，普通业务使用普通链路以不同的频谱在同一根光纤中传输。根据 SECURITYA-RSA 算法的控制模型，安全业务和普通业务使用的安全链路和普通链路不重合，是 2 类路径不重合的业务。因此，为降低业务平均光路建立时延，安全业务和普通业务可以在不同的线程中通过使用安全拓扑和普通拓扑并行建立光路，并行建路方式减少了业务的排队时延、通信时延和设备配置时延。

SECURITYA-RSA 算法的并行建路控制策略如图 1 所示，安全拓扑和普通拓扑分别占用了物理拓扑中互斥的网络资源。安全业务和普通业务分别使用安全拓扑和普通拓扑并行计算路由频谱分配方案、配置设备和建立光路，减少光路建立时延。多线程分别连续应用安全虚拟拓扑和普通虚拟拓扑并行建立光路。普通业务在普通拓扑建立光路，Eve 窃听不到安全业务数据信息；安全业务在安全拓扑建立光路，由于业务数据进行了安全加密传输，Eve 窃听不到有效的数据信息。

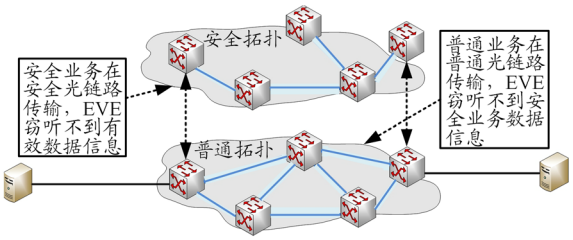

图 1 SECURITYA-RSA 算法的并行建路控制策略

传统 RSA 算法中，例如最短路径首次频谱适应算法（SPFF-RSA）计算开销小、复杂度低，常用作标准算法与新设计的路由频谱分配策略进行性能对比。SPFF-RSA 算法步骤如下：①业务到达；②计算路由；③分配频谱资源；④业务光路建立成功或阻塞。但是，算法在进行光路建立时，受算法控制模型限制，业务的光路逐个建立，遇突发业务网络的时延性能劣化。SECURITYA-RSA 算法的步骤为：①业务到达；②判断是普通业务还是安全业务；③并行为安全业务和普通业务分配路由频谱资源；④业务光路建立成功或阻塞。引用文献[2]中业务光路平均建立时延公式，假设安全业务个数等于普通业务个数，则串行和并行路由频谱分配策略业务光路平均建立时延分别如式（7）和式（8）所示。

$$A(N_r)=T\times(N_r+1)/2 \tag{7}$$

$$A(N_r)=T\times(N_r/N_{th}+1)/2 \tag{8}$$

并行路由频谱分配 SECURITYA-RSA 算法的光路建立时延随着 N_{th} 的增加近似线性下降，明显小于串行 RSA 算法的光路建立时延。SECURITYA-RSA 算法的流程图如图 2 所示。

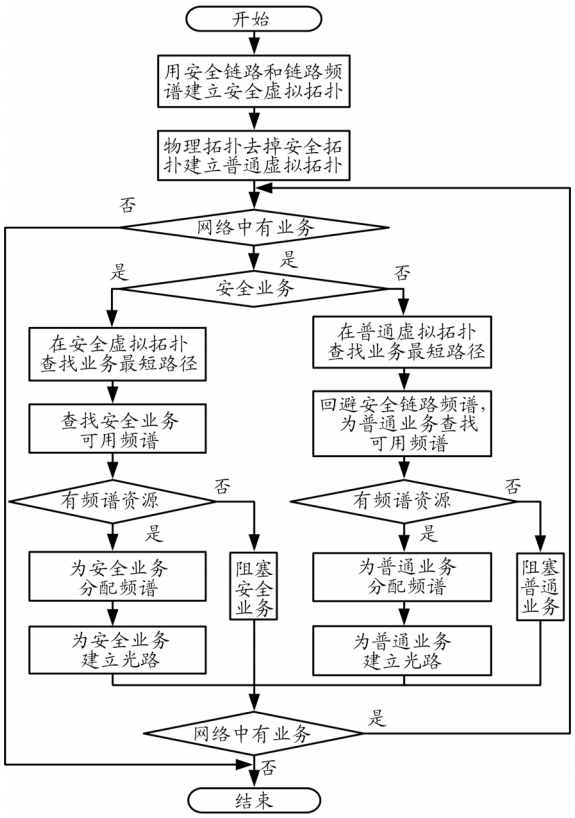

图 2 SECURITYA-RSA 算法的流程图

SECURITYA-RSA 算法有主函数线程、业务释放线程、RSA 线程和业务产生线程，按线程优先级由低到高分别为：①主函数线程，负责创建上述线程，设置线程优先级，开启线程，计算光路平均建立时延、安全业务被窃听概率等；②业务释放线程，负责释放持续时间大于预设时间的业务，释放频谱资源，频谱资源用于再建立光路；③业务产生线程，产生安全业务和普通业务，线程中产生了少部分突发业务，用于测试算法的可靠性；④RSA 线程，通过运用安全拓扑和普通拓扑为安全业务和普通业务计算路由频谱分配方案、配置设备和建立光路。

2 仿真结果和分析

2.1 仿真参数设置

本文用 VC++编写了仿真程序，在 VS2010 开发平台上运行，算法采用的 NSFNET 网络拓扑如图 3 所

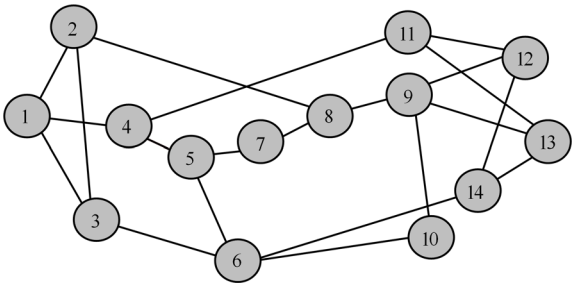

图 3 NSFNET 拓扑

示,拓扑包含 14 个节点和 21 条双向光连接链路。算法运行的参数配置具体如下:光纤链路中有 8.95 THz 频谱资源,划分的最小频隙为 12.5 GHz;假设业务请求到达网络的时间服从泊松分布,持续时间服从负指数分布;业务由安全业务和普通业务组成,安全业务个数与普通业务个数比例为 0.5,安全业务和普通业务均匀分布在节点间;突发业务占全部业务的 0.1。为简化网络模型,本文不使用波长转换器。图 4 是安全拓扑,用最小生成树产生,由 13 条双向光链路组成;物理网络的频谱高位(4.475 THz)用作安全光链路频谱,适应光网络现有路由频谱分配算法,有利于设计的安全策略部署在光网络。

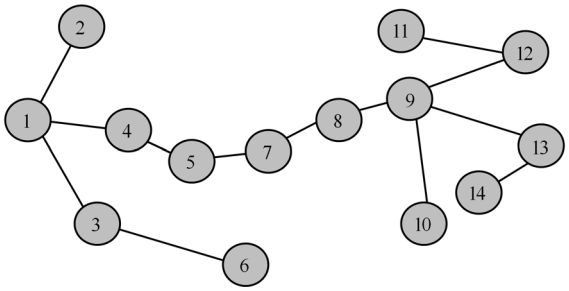

图 4 安全拓扑

SPFF-RSA 算法分别使用最短路径(SHORT PATH)算法和频谱首次适应(FIRST FIT)算法分配路由和频谱资源;SPFF-RSA 算法无安全策略,普通业务也用安全链路,不回避有安全传输能力拓扑;若安全业务路径不在安全拓扑或安全业务使用普通业务频谱,则被窃听。单线程业务安全等级感知路由频谱分配(ST-RSA)算法有安全策略,普通业务回避有安全传输能力拓扑,算法通过 SHORT PATH 算法和 FIRST FIT 算法查找安全业务使用的光路和频谱。

2.2 结果讨论

在上述的仿真环境下,假设 Eve 能力无限,安全业务在无安全传输能力链路传输则被窃听。本文分别运行 SECURITYA-RSA 算法、ST-RSA 算法和 SPFF-RSA 算法,就光路平均建立时延、频谱资源利用率、阻塞率和安全业务被窃听比例等性能进行对比分析。算法的时延性能比较如图 5 所示。可以看出,与 SPFF-RSA 算法相比,SECURITYA-RSA 算法的光路平均建立时延较低,这是因为该算法在安全虚拟拓扑和普通虚拟拓扑并行建立光路,并行分配资源和配置光路设备,减少了业务平均光路建立时延。与 ST-RSA 算法相比,SECURITYA-RSA 算法的光路平均建立时延更小,该算法通过虚拟拓扑减少了查找满足条件的安全链路和频谱资源所需时间。与 SPFF-RSA 算法相比,ST-RSA 算法的光路平均建立时延更大,这是因为 ST-RSA 算法需要区分业务安全类别,查找满足条件的安全链路和频谱资源,增加了业务光路建立时延。

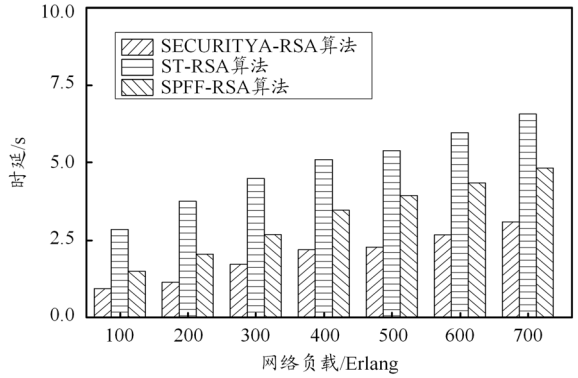

图 5 光路平均建立时延

SECURITYA-RSA 算法、ST-RSA 算法和 SPFF-RSA 算法的频谱利用率和阻塞率分别如图 6 和图 7 所示。当网络负载低于 400 Erlang 时,与 SPFF-RSA 算法对比,SECURITYA-RSA 算法和 ST-RSA 算法的频谱资源利用率略高,这是因为 SECURITYA-RSA 算法和 ST-RSA 算法进行了安全业务路由频谱分配设计,安全业务只能在安全链路频谱传输,增加了频谱资源使用;当网络负载大于等于 400 Erlang 时,与 SECURITYA-

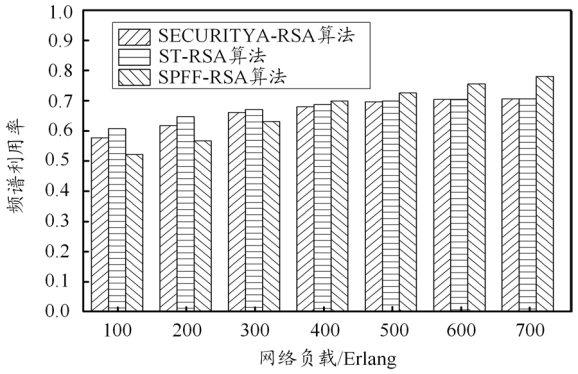

图 6 频谱利用率

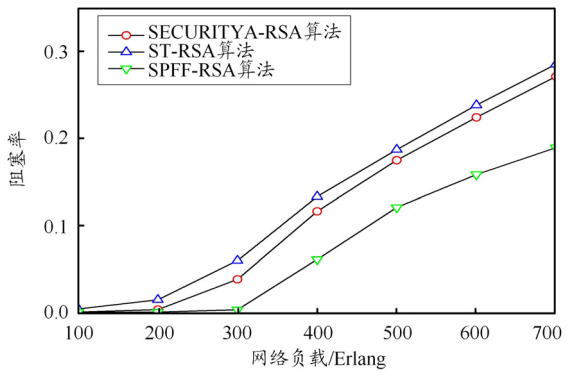

图 7 阻塞率

RSA 算法和 ST-RSA 算法对比，SPFF-RSA 算法的频谱资源利用率略高，这是因为 SECURITYA-RSA 算法和 ST-RSA 算法受限于安全策略频谱使用规则，频谱使用趋于饱和。SPFF-RSA 算法没有频谱使用限制，频谱资源利用率能逐步提高。SECURITYA-RSA 算法的阻塞率低于 ST-RSA 算法阻塞率，这是因为 SECURITYA-RSA 算法并行建立光路，有更低的光路建立时延，能够快速建立光路，增加了频谱资源利用率，间接降低了业务阻塞率；SPFF-RSA 算法的阻塞率低于 SECURITYA-RSA 算法，这是因为 SPFF-RSA 算法无安全策略，不区分业务安全类别和链路差别，频谱使用更高效，阻塞率更低。

安全业务被窃听比例如图 8 所示。可以看出，SECURITYA-RSA 算法和 ST-RSA 算法安全业务被窃听比例等于 0，这是因为 SECURITYA-RSA 算法和 ST-RSA 算法使用安全链路频谱为安全业务建立光路。安全业务在安全链路进行传输时，数据进行加密传输，Eve 在安全传输链路窃听不到安全业务信息，增加了安全业务的安全性。SPFF-RSA 算法安全业务被窃听比例较高，大部分业务被窃听。这是因为 SPFF-RSA 算法无安全策略，在无安全传输能力链路传输的安全业务被全部窃听。

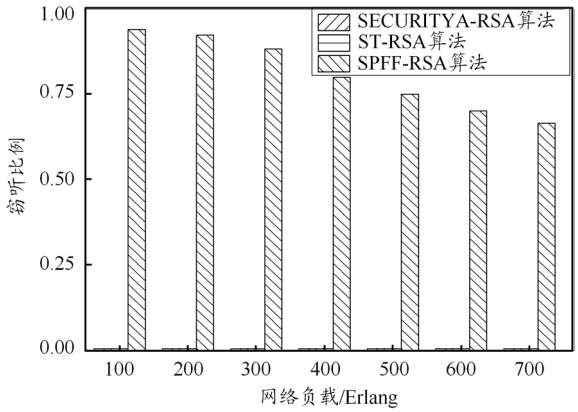

图 8 安全业务被窃听比例

3 结束语

本文提出业务安全等级感知的低时延路由频谱分配 SECURITYA-RSA 算法。算法采用多线程技术为普通业务和安全业务计算路由，分配频谱资源，配置光路上的设备，建立光路。由于使用并行建立光路和虚拟拓扑相结合的方法，在安全业务不被窃听的前提下，SECURITYA-RSA 算法减少了业务的平均光路建立时延和阻塞率。为简化算法控制模型，算法未考虑遇突发事件时安全光链路中断在线切换已建路安全业务。另外，光网络增加安全光链路，算法需离线配置，降低了算法效率。在后续工作中，我们将根据网络变化和安全链路变化，自动重构安全拓扑，自动重路由已建立安全业务光路。

参考文献：

[1] HOROTA A, REIS L, FIGUEIREDO G, et al. Routing and spectrum assignment algorithm with most fragmented path first in elastic optical networks[J]. IEEE Latin America Transactions, 2016, 14(6): 2980–2986.

[2] GUO H, ZHANG J, ZHAO Y, et al. Delay aware RSA algorithm based on scheduling of differentiated services with dynamic virtual topology construction[J]. IEEE Access, 2020(8): 44559–44575.

[3] WANG W, ZHU M, WANG J, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//IEEE International Conference on Intelligence and Security Informatics (IEEE ISI 2017), July 22–24, 2017, Beijing, China. Piscataway: IEEE, 2017: 43–48.

[4] 张杰. 内生安全光通信技术及应用 [J]. 无线电通信技术，2019，45(4)：337–342.

[5] 张旭，张杰，李亚杰，等. 基于量子噪声流加密的光纤物理层安全传输技术[J]. 光通信技术，2020，44(4)：18–22.

[6] 宣贺君，王宇平，徐展琦，等. 弹性光网络中考虑节点安全性的频谱分配算法[J]. 中国激光，2016，43(12)：199–206.

[7] JIAO H, PU T, ZHENG J, et al. Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model[J]. Optics Express, 2017, 25(10): 10947–10960.

[8] 郭宏，杨润利，王文彦，等. 基于物理损伤感知的低时延 RSA 算法[J]. 光通信技术，2017，41(5)：15–18.

[9] 朱静. 应对物理层攻击的软件定义多域多芯弹性光网络设计与服务算法研究[D]. 北京：中国科学技术大学，2019.

[10] 马乐，张杰，王博，等. 光通信物理层安全中量子噪声流加密综述[J]. 激光与光电子学进展，2020，57(23)：230603-1–230603-19.