大功率信号对光网络的影响及防护技术研究进展

张引发 任 帅 王 朋 李 明 王鲸鱼
西安通信学院光纤通信实验室,陕西 西安 710106

摘要 近年来光网络朝着高速率、大带宽的方向迅猛发展,承载着大量的信息传输任务,其安全问题受到越来越多的关注,其中,大功率信号对光网络的影响及防护技术成为光网络安全领域的最新研究热点之一。介绍了光网络中大功率信号引起的增益竞争攻击、带间串扰攻击和带内串扰攻击,分析了大功率信号引起的攻击效应对光网络中用户信号质量的攻击影响。从攻击检测和定位技术、安全路由防护技术等方面总结了针对大功率信号攻击效应的光网络安全防护技术。

关键词 光通信; 大功率信号; 增益竞争攻击; 带间串扰攻击; 带内串扰攻击; 防护技术
中图分类号 TN913.7 **文献标志码** A **doi:** 10.3788/LOP51.100003

Research Progress of Effect of High Power Signal on Optical Networks and Protection Technology

Zhang Yinfa Ren Shuai Wang Peng Li Ming Wang Jingyu
Laboratory of Optical Communications, Xi'an Communications Institute, Xi'an, Shaanxi 710106, China

Abstract In recent years optical networks are developing towards high rate and wide bandwidth. Optical networks propagate a great amount of information, and its security issues are drawing more and more attention. Impact of high power signal on optical networks and protection technology has become a hotspot for research in the area of security of optical networks. Gain competition attack, inter-channel crosstalk attack, and intra-channel crosstalk attack caused by high power signal in optical networks are introduced, and attack impact caused by high power signal on legitimate signals in optical networks is also analyzed. Security protection technologies aiming at attack impact of high power signal in optical networks are summarized from the viewpoints of attack detection and location technology, secure routing protection technology and other protection technologies.

Key words optical communications; high power signal; gain competition attack; inter-channel crosstalk attack; intra-channel crosstalk attack; protection technology
OCIS codes 060.4370; 060.4510; 190.4370; 350.5500

1 引 言

随着技术的发展和进步,以密集波分复用技术(DWDM)为基础的光网络因具有宽带宽、大容量、高速率等优势而成为现代通信网络的重要支柱和主流发展方向[1-2]。近年来,随着大规模宽带接入网络的部署,用户数量的持续增加和云计算、电子科研、多媒体、新兴社交网络以及能够随时随地访问网络的智能手机等网络服务的不断发展,光网络传输的信息量产生了巨大增长,同时光网络作为基础传送网,其与卫星通信网络、无线传感器网络、数据存储中心等也进行着海量的数据传输和交换,并且可以预见的是,光网络的信息传输量仍将呈现出持续增长的趋势[3]。因此,光网络已成为国家重要的战略基础设施[4]。

2013年6月,美国前中情局(CIA)职员爱德华·斯诺登向媒体揭露了美国国家安全局(NSA)的“棱镜(PRISM)”网络监控项目,再次引发了世界各国对网络和信息安全的重点关注。“维护网络和信息安全是维护国家安全的重要内容”已成为世界各国的广泛共识。据相关消息披露,中国的网络系统一直是美国监控和

收稿日期: 2014-04-14; **收到修改稿日期**: 2014-05-16; **网络出版日期**: 2014-08-22
基金项目: 国家自然科学基金(61072125)、中国人民解放军国防基金(2012JY002-260)
作者简介: 张引发(1964—),男,硕士,教授,主要从事光网络安全防护技术方面的研究。E-mail: yinfazhang@163.com

侵入攻击的重点目标,“棱镜门”事件显现出我国的网络系统面临着各种攻击威胁并且缺乏足够的防护能力。

光网络一度被认为具有高保密性和安全性。光网络在物理层呈开放状态,而且光网络在设计时只考虑了保证网络生存性的保护倒换设计,但对于大多数铺设在户外的光缆线路而言,除了维护人员的周期性巡线外,几乎没有采取任何保证光网络物理层安全的防护措施,并且随着光网络铺设范围的扩大和功能的增加,光网络将会提供更加广泛的服务,而服务的增加必然要求提供更多的光接口。因此,光网络的工作环境特殊、监管防护手段缺少、接入平台日益开放,这些因素都会导致光网络在用户端、传输链路以及交换节点等多处的安全性受到严重的威胁,这些安全威胁就包括本文所要研究的大功率信号对光网络的攻击影响[5-6]。由于光网络承载着大量的信息传输任务,即使攻击造成的服务破坏的时间很短,也会造成大量用户数据的丢失与破坏,因此,研究大功率信号对光网络的攻击影响及其防护技术,对于保证光网络的可靠传输和加快光网络安全防护措施建设的步伐具有重要的参考价值和现实意义。

2 大功率信号对光网络的攻击影响

Medard等[7]针对光网络的特点,首次提出了大功率信号(一般大于用户信号功率20~30 dB)会对光网络产生攻击影响。Jirattigalachote[8]详细分析了大功率信号在光网络中引起的各种攻击效应,如图1所示,光网络中一旦被注入大功率的攻击信号,可在掺铒光纤放大器(EDFA)处引起增益竞争攻击,也可在光纤链路上引起带间串扰攻击,还可在光交叉连接器(OXC)的光开关处引起带内串扰攻击,下面分别对其进行分析研究。

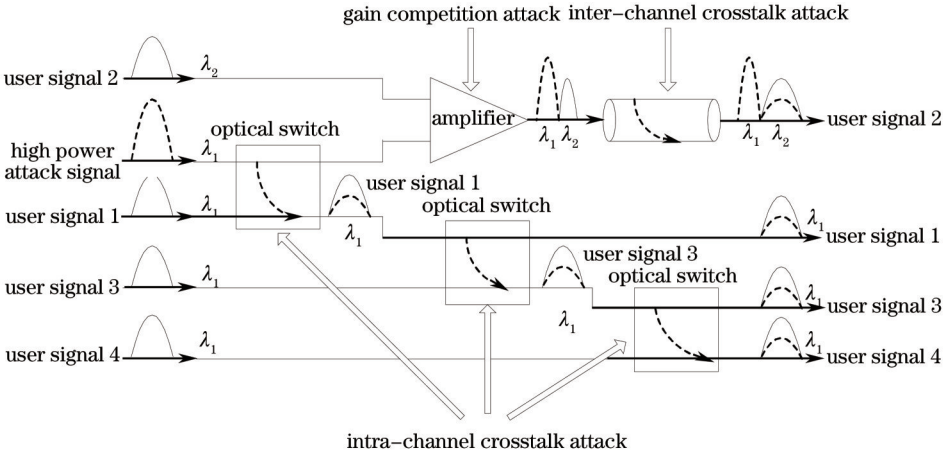

图1 大功率信号对光网络的攻击影响示意图

Fig.1 Schematic diagram of attack impact of high power signal on optical networks

2.1 大功率信号引起的增益竞争攻击

EDFA的工作原理是采用掺铒离子单模光纤作为增益介质,在抽运光作用下产生粒子反转,在用户信号诱导下实现受激辐射放大[9]。EDFA通常可为波长在1525~1570 nm之间的光信号提供放大增益,980 nm和1480 nm的大功率激光器则是其常用的抽运源。如图2所示,对于波长为980 nm的抽运源,掺铒光纤相当于一个三能级系统:基态 E_1 ($^4I_{15/2}$),亚稳态 E_2 ($^4I_{13/2}$)和激发态 E_3 ($^4I_{11/2}$)。在抽运光的照射下,E_r^{+3} 通过吸收入射光子的能量,由基态跃迁到较高的激发态,由于激发态不稳定,因此 E_r^{+3} 又会迅速跃迁到亚稳态,在亚稳态能级会有大约10 ms的寿命,因此,在源源不断的抽运下,亚稳态上的粒子数不断积累,从而实现粒子数反转。当再有外部用户信号激励时,亚稳态能级的粒子受激辐射向基态能级跃迁,产生与入射光子同频、同相、同方向的光子,形成对用户信号的相干放大。

EDFA中亚稳态能级粒子受激辐射产生的光子数是有限的,当有多路光信号进入EDFA时,所有的输入信号需要共享这些有限的光子数[10]。每个入射信号根据其功率大小获得相应比例的光子数,结果就是功率大的信号获得较多的增益,功率小的信号获得较少的增益,这就是EDFA的增益竞争特性。如图3所示,EDFA的增益竞争特性可被用来实施增益竞争攻击,即在光网络中注入大功率攻击信号,该信号的波长和用户信号的波长不同,但是在EDFA的通带范围之内,攻击信号将获得极大的增益,而用户信号则由于没有获得

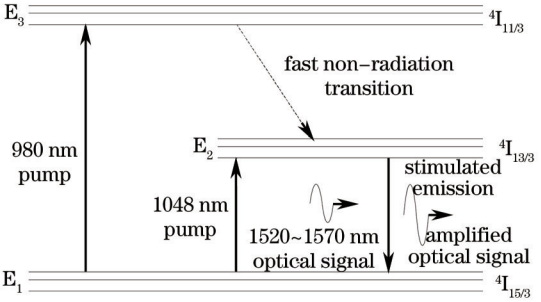

图2 E_r^{+3} 的能级结构

Fig.2 Energy level structure of E_r^{+3} ions

正常设计所需要的功率增益而得不到有效放大,造成接收端的用户信号质量劣化。2010年,Furdek等[11]通过实验验证了大功率信号在EDFA中引起的增益竞争攻击。图4为增益竞争攻击的仿真结果图,其中,攻击信号频率为192.1 THz,用户信号频率为192.3,192.5,192.7,192.9,193.1,193.3,193.5 THz。由图4可以看出,从攻击信号功率高于用户信号功率15 dB开始,各路用户信号的增益显著下降。当攻击信号功率大于用户信号功率10 dB以上时,会造成用户信号增益的下降,并且攻击信号功率越大,用户信号增益下降越明显。

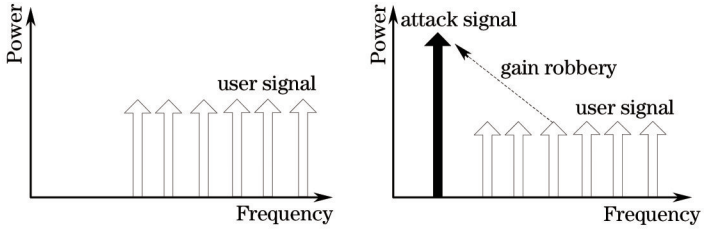

图3 大功率信号引起的增益竞争攻击示意图

Fig.3 Schematic diagram of gain competition attack caused by high power signal

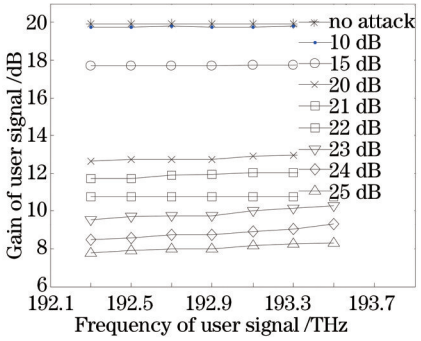

图4 增益竞争攻击仿真图

Fig.4 Simulation diagram of gain competition attack

2.2 大功率信号引起的带间串扰攻击

在长距离、高速率的传输过程中,光纤会表现出一定的非线性特性,例如自相位调制(SPM)、交叉相位调制(XPM)、四波混频(FWM)以及受激拉曼散射(SRS)等[12]。光纤的非线性效应会造成在同一条光纤中传输的相邻信道之间的相互作用和串扰影响,例如SPM和XPM与群速度色散(GVD)互相作用,会将相位调制转换为强度调制,进而产生带间串扰,带来光脉冲的加速展宽,引起脉冲波形畸变;FWM效应产生的新频率可能与用户信号频率相等或相近[13],并且会叠加到用户信号上,产生带间串扰;SRS则会引起大功率的抽运光向斯托克斯(Stokes)光的功率转移[14],进而使某信道中的能量转移到相邻信道中去,造成带间串扰。图5(a)为FWM效应产生新频率的仿真图,图5(b)为SRS效应产生信道间功率转移的仿真图。光纤中的光功率越强,光纤非线性效应对用户信号质量的影响就越严重。光纤的非线性特性可被用来实施带间串扰攻击,方法就是在光纤中的某一信道注入大功率攻击信号,该攻击信号会加剧光纤的非线性效应,引起不同波长的相邻信道之间的相互串扰,最终导致和攻击信号在同一条光纤中传输的用户信号质量的劣化。2011年,Peng等[15]搭建仿真实验系统,对大功率带间串扰攻击进行了仿真分析,结果表明,攻击信号功率越强,用户信号受攻

击影响越严重。

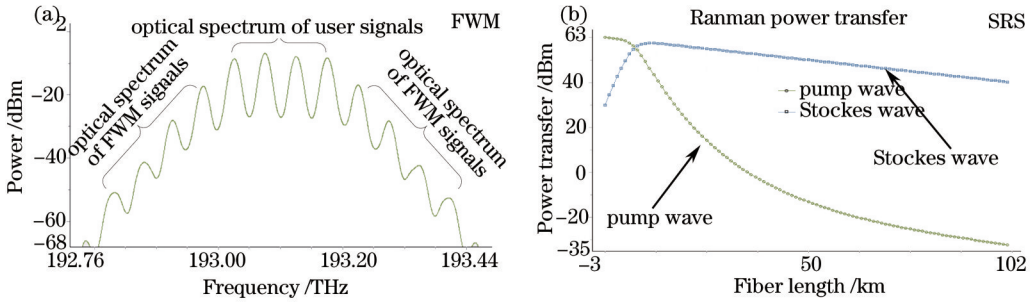

图5 大功率信号引起的光纤非线性特性(a)FWM和(b)SRS的仿真图

Fig.5 Simulation diagram of fiber nonlinear characteristics (a) FWM and (b) SRS caused by high power signal

2.3 大功率信号引起的带内串扰攻击

由于OXC处的光开关不能完全隔离各路光信号,导致使用同一波长的不同用户信号在光开关处产生功率泄露和相互串扰影响,若大功率攻击信号进入光开关,这种功率泄露会造成用户信号质量的劣化,这就是大功率信号引起的带内串扰攻击[16]。

图6(a)所示为一种典型的OXC结构,该OXC由M个解复用器、N个光开关矩阵和M个复用器组成,每条输入输出光纤复用N个不同的波长。各输入光纤的信号经解复用后,使用相同波长的用户信号进入同一个光开关矩阵进行交换,交换后的各路信号再次复用到输出光纤中继续传输。图6(b)所示的2×2光开关是构成光开关矩阵的基本单元,使用相同波长的信号1和信号2分别从输入端口in1和in2进入光开关,端口control用于控制光开关是平行连接还是交叉连接。由于光开关的非理想隔离,无论是平行连接还是交叉连接,在光开关内部都会发生功率泄露。光开关的隔离度有限是大功率带内串扰攻击得以实现的主要原因,并且由于攻击信号波长和用户信号波长相同,带内串扰攻击很难被滤波器有效地滤除[17]。

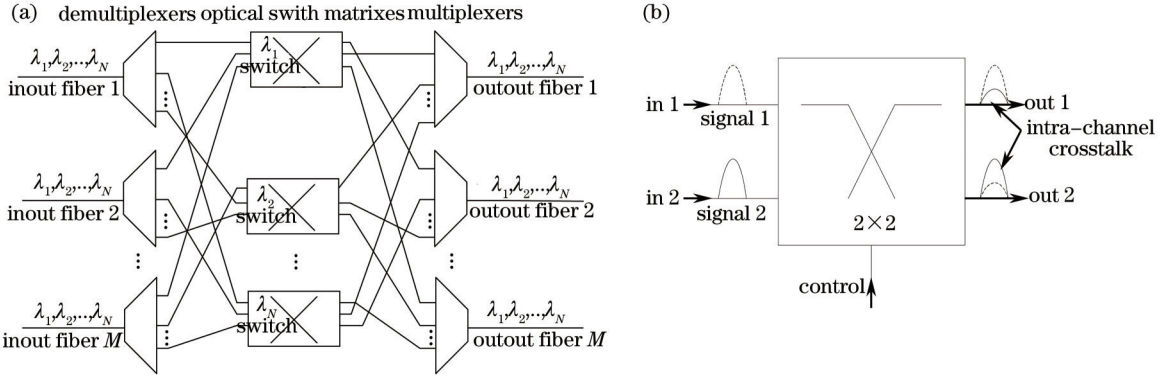

图6 典型的(a)OXC结构和(b)2×2光开关结构

Fig.6 Typical structure of (a) OXC and (b) 2×2 optical switch

2002年,Wu等[18]首次分析了带内串扰攻击模型,如图7所示。图中光开关使用平行连接方式。大功率攻击信号、用户信号1、用户信号2、…、用户信号n均使用相同的波长。大功率攻击信号和用户信号进入光开关1,由于光开关的非理想隔离,攻击信号泄露到用户信号上的光功率很大,用户信号1在光开关1处受到了带内串扰攻击,用户信号1受到攻击的同时还附加了一部分攻击光功率,获得了一定的攻击能力,会进一步攻击与其共同进入光开关2的用户信号2,同样,用户信号2也获得了一定的攻击能力,会在它通过的下游光开关处继续引起带内串扰攻击。2006年,Wu等[19]对带内串扰攻击作了进一步的分析,并研究了带内串扰攻击定位和识别方法。2011年,Sun等[20]搭建仿真实验系统,研究了大功率带内串扰攻击对用户信号质量的攻击影响及其攻击传播能力,得出了量化的仿真结果。

3 针对大功率攻击信号的光网络防护技术

需要注意的是,本文第2节分别对大功率信号引起的增益竞争攻击、带间串扰攻击和带内串扰攻击进行了独立的介绍与分析,实际情况中,如图1所示,一旦光网络中被注入大功率攻击信号,既可在光纤链路上引

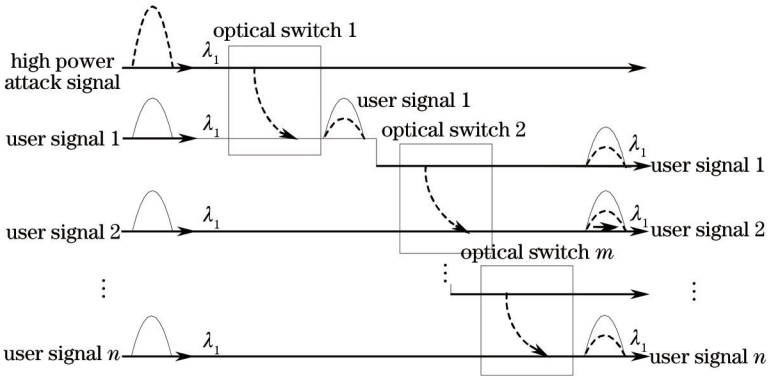

图7 文献[18]提出的带内串扰攻击传播模型

Fig.7 Model of intra-channel crosstalk attack propagation proposed in Ref.[18]

起带间串扰攻击,也会在EDFA处引起增益竞争攻击,还会在OXC处引起带内串扰攻击。发生在传输链路上EDFA处的增益竞争攻击,由于大功率攻击信号掠夺了用户信号的增益,使得用户信号得不到应有的放大,会进一步加剧带间、带内串扰攻击对用户信号的攻击影响,并且会增强攻击信号的攻击能力,造成攻击破坏范围的扩大和攻击对用户信号影响程度的加剧。因此,针对大功率信号攻击效应的光网络安全防护技术的研究尤为必要。从攻击检测和定位、安全路由等方面介绍了相关的光网络安全防护技术。

3.1 攻击检测和定位技术

1998年,麻省理工学院Saengudomlert等[21]分析了光网络中大功率信号引起的主要攻击类型和已有的攻击检测方案,并提出了一种新的基于误码率(BER)比较的攻击检测方案。该方案原理是被检测设备的输入输出端口信号的BER满足一定的函数关系 k,根据这种关系来确定阈值,如果检测结果超出了该阈值,则认为光网络中发生了大功率信号攻击,并产生告警,其检测原理如图8所示。由于这种方法要经过光电转换,所以攻击检测的响应时间依赖于光电转换时间,同时由于需要从输入和输出端提取信号,所以会影响信号功率,从而对系统的BER有一定的影响,还需进一步研究和改善。

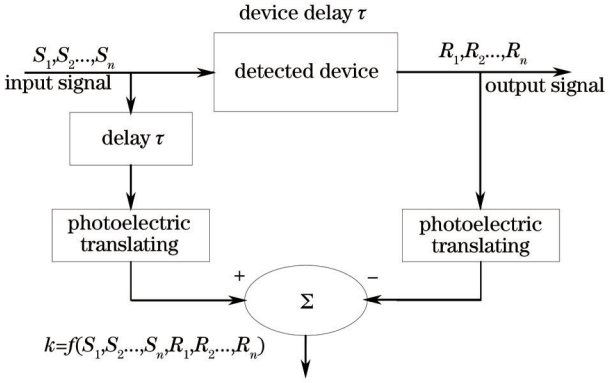

图8 基于BER比较的大功率信号攻击检测方案

Fig.8 Attack detection scheme of high power signal based on BER comparison

2000年,Shake等[22]针对长距离光纤通信系统中存在的非法大功率信号注入攻击进行了评估,指出了光网络中光纤和节点设备存在的安全脆弱性,并定量分析了光网络物理层安全脆弱性的应对措施。

Wu等[18-19]提出了光网络中带内串扰攻击的传播模型,论证了实施带内串扰攻击定位的必要条件,并提出了一种带内串扰攻击监测和定位方案,该方案的思路为:1) 通过监控信号获知光路连接的状态信息;2) 通过优化算法,只需在特定的节点处安置性能监测设备即可实现对全网的攻击监测。

Rejeb等[23-24]针对光网络中多点攻击定位问题,提出了一种可处理光网络中多点攻击的监测方案。该方案包含两个阶段:监测设备发出告警之后的攻击检测阶段和攻击精确定位阶段。在攻击检测阶段,使用贪婪算法来确定光网络中监测器件的数量,以达到使用较少的监测设备实现在全网中进行攻击监测的目的;在攻击精确定位阶段,根据告警区域,与在监测设备安置阶段预计算产生的告警矩阵进行对比,产生待选受攻击设备,最后对攻击进行精确定位。

2013年，彭炳斌[25]提出了一种基于双参数比较的分布式多点带内串扰攻击定位算法，算法在分析带内串扰攻击源特点的基础上，通过同时比较节点本身检测到的光信噪比参数和功率参数以及直接上游节点检测到的对应参数判断攻击源的位置，以此实现对多点攻击情况下攻击源的快速准确定位，其中，分布式控制方式提高了算法的时效性，而双参数比较则保证了攻击的准确定位。

3.2 安全路由防护技术

光网络的安全路由是一个新的研究领域，与攻击检测和定位技术不同，它是一种基于主动预防机制的光网络安全防护措施。近年来陆续有相关论文发表。Nina等[26-28]从路由和波长分配的角度，研究了光网络中限制大功率信号攻击影响范围的路由和波长分配算法(RWA)，其核心思想是：在路由和分配阶段，将能引起最小攻击传播效应的路由和波长分配给光路请求，从而降低全网的攻击传播效应，以此减小攻击的破坏范围。算法思想如图9所示，图9为同一组光路请求的两种不同的路由方案，当在光路LP1上注入大功率攻击信号时，在图9(a)所示的路由方案1中，LP1以及和LP1具有共用链路(同条光纤)的LP2、LP3、LP4共4条光路都会受到攻击影响；而在图9(b)所示的路由方案2中，只有LP1、LP5共2条光路会受到攻击影响。因此，通过合理的路由规划，即可实现有效限制攻击影响范围的目的，并且不需要在光网络中额外增加监测设备，这对于以低成本提升光网络的安全性具有一定的现实意义。

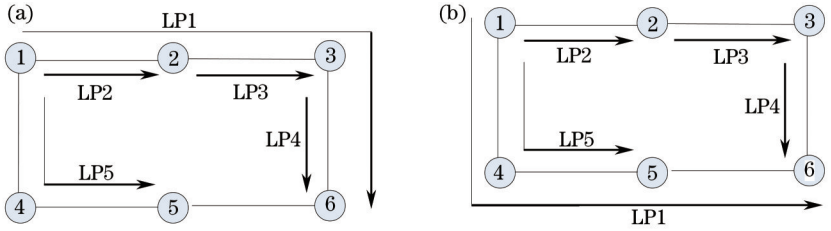

图9 同一组光路请求的两种不同路由方案。(a) 路由方案1; (b) 路由方案2

Fig.9 Two routing schemes for the same group of light-path requests. (a) Routing scheme 1; (b) routing scheme 2

2012年，孙泽宇等[29]构建了一种综合考虑光网络中大功率增益竞争攻击、带间串扰攻击和带内串扰攻击的攻击传播模型(JAR-Model)，进而提出了一种规避大功率信号攻击的RWA算法：一旦光网络中检测到功率异常大的信号，利用JAR-Model就可以迅速判断光网络中可能会受到攻击影响的节点和光纤链路，然后再对路由和波长分配做一些针对性的调整，就可以有效地避免攻击对光网络造成的危害。Tan[30]提出了一种基于蚁群算法的大功率信号攻击和EDFA放大自发辐射噪声(ASE)感知的路由算法，该算法将最大攻击范围和EDFA的ASE作为路由计算的约束条件。2013年，彭炳斌等[31]提出了一种提高光网络攻击容忍性的RWA算法，该算法将能引起最小攻击传播效应的波长分配给光路请求。2014年，任帅等[32]提出了一种限制物理层攻击影响范围的TS_RWA算法，该算法在路由分配阶段，将具有较小最大攻击范围(MAR)的路由分配给光路请求，以降低大功率信号的攻击影响范围。以14个节点、21条链路的美国国家科学基金网络(NSFNET)网络拓扑为基础，随机生成20组光路请求，然后将TS_RWA算法和常用的最短路径算法(SP_RWA)、首先适配算法(FF_RWA)获得的光路路由就MAR进行对比，结果如图10所示。从图10可以看出，相比于SP_RWA、FF_RWA算法，TS_RWA算法的MAR分别平均减小了大约21%和32%。即通过适当的优化RWA算法，就可在一定程度上限制大功率信号的攻击影响范围。

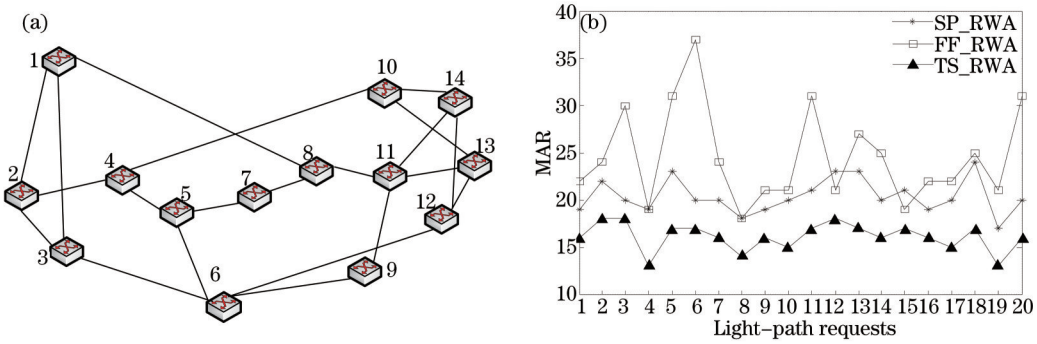

图10 NSFNET网络拓扑下MAR对比。(a) NSFNET网络拓扑; (b) 模拟结果

Fig.10 MAR comparison in NSFNET topology. (a) NSFNET; (b) simulation results

3.3 其他防护技术

针对大功率信号对光网络的影响问题,还有以下防护技术。

Jirattigalachote[8]提出了一种使用功率均衡器限制大功率攻击信号传播的方法,即当大功率攻击信号通过装有功率均衡器的节点之后,便会失去攻击能力。如图11所示,假设大功率攻击信号注入到光路LP1上,那么,和LP1共享光纤链路的LP2、LP3都会受到影响,如果节点2安装了功率均衡器,LP1上的攻击信号的功率通过该节点之后就会衰减到可以接受的水平,LP3就不会再受到攻击影响。如果在光网络中的每个节点都安装功率均衡器,不仅花费巨大,而且浪费资源。因此,该方案提出使用贪婪随机自适应搜索算法(GRASP)来寻求功率均衡器安装问题的最优解,以便以尽可能少的功率均衡器实现全网中限制攻击传播的需求。

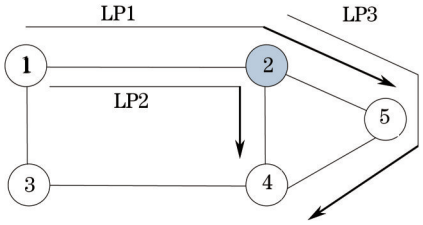

图11 功率均衡器限制大功率信号攻击传播示意图

Fig.11 Schematic diagram of limiting attack propagation of high power signal by power equalizer

Liu等[33]基于概率图模型分析了存在带内串扰攻击时不同光网络架构的可靠性,对于新建网络时的网络规划具有一定的参考意义。Huang等[34]研究了对信号进行差分频移键控(DPSK)格式调制可减轻攻击对用户信号质量的影响,DPSK调制系统的调制和解调都较为复杂,实现起来所需花销太大。

4 结 论

首先分析了光网络面临的安全威胁,然后重点介绍了大功率信号引起的增益竞争攻击、带间串扰攻击和带内串扰攻击以及它们对光网络中用户信号质量的攻击影响,最后从攻击检测和定位技术、光网络安全路由等方面总结了现有的针对大功率信号攻击效应的光网络安全防护技术。由于光网络承载着大量的数据传输任务,即使攻击造成的服务破坏时间很短,也会造成大量用户数据的丢失与破坏,因此,基于主动攻击预防机制的光网络安全路由将会成为一个新的研究热点。

参 考 文 献

1 Zeng Shuguang, Hu Jing, Wang Fei, *et al.*. Pulse stacking scheme based on wavelength division multiplexing[J]. Acta Optica Sinica, 2013, 33(5): 0514001.
曾曙光, 胡 静, 王 飞, 等. 基于波分复用思想的啁啾脉冲堆积方法[J]. 光学学报, 2013, 33(5): 0514001.

2 M Furdek, N Skorin-Kapov, M Bosiljevac, *et al.*. Analysis of crosstalk in optical couplers and associated vulnerabilities [C]. MIPRO 2010, 2010. 461-466.

3 Chris Develder, Marc De Leenheer, Bart Dhoedt, *et al.*. Optical networks for grid and cloud computing applications[J]. Proceedings of the IEEE, 2012, 100(5): 1149-1167.

4 Luo Qingsong, Yang Hua, Liu Zhiqiang, *et al.*. Security status and key technology study of optical network[J]. Journal of CAEIT, 2013, 8(4): 338-343.
罗轻松, 阳 华, 刘志强, 等. 光网络安全现状及关键技术研究[J]. 中国电子科学研究院学报, 2013, 8(4): 338-343.

5 Guanglei Liu, Chuanyi Ji. Resilience of all- optical network architectures under in- band crosstalk attacks: A probabilistic graphical model approach[J]. IEEE Journal on Selected Areas in Communications, 2007, 4(25): 2-17.

6 N Sreenath, K Muthuraj, P Sivasubramanian. Secure optical internet: attack detection and prevention mechanism[C]. 2012 ICCEET, 2012. 1009-1012.

7 M Medard, D Marquis, R A Barry, *et al.*. Security issues in all-optical networks [J]. IEEE Network, 1997, 11(3): 42-48.

8 Amornrat Jirattigalachote. Provisioning Strategies for Transparent Optical Networks Considering Transmission Quality, Security, and Energy Efficiency[D]. Stockholm: KTH School of Information and Communication Technology, 2012.

9 Meng Xiangbo. The Research of Multifunctional EDFA[D]. Beijing: Beijing Jiaotong University, 2011.

孟祥波. 多功能EDFA研究[D]. 北京: 北京交通大学, 2011.

10 Marija Furdek, Nina Skorin- Kapov. Physical- layer attacks in transparent optical networks[J]. Optical Communications Systems, 2012, (3): 123-146.

11 M Furdek, M Bosiljevac, N Skorin-Kapov, *et al.*. Gain competition in optical amplifiers: A case study[C]. MIPRO 2010, 2010: 467-472.

12 Mingliang Deng, Xingwen Yi, Jing Zhang, *et al.*. Fiber nonlinearity compensation for CO-OFDM transmission with 10.7-Gb/s NRZ-OOK neighbors[J]. Chin Opt Lett, 2012, 10(11): 110602.

13 Luo Xuan, Jiang Yang, Yu Jinlong, *et al.*. Simultaneous optical signal dropping and cleaning by utilizing four wave mixing effects based optical logic gate in optical fiber[J]. Acta Optica Sinica, 2010, 30(9): 2524-2528.
罗 旋, 江 阳, 于晋龙, 等. 基于光纤中四波混频效应光逻辑门的信号同步提取与擦除[J]. 光学学报, 2010, 30(9): 2524-2528.

14 Liu Yu, Sun Yani, Fang Lijie, *et al.*. Analysis of stimulated raman scattering effects on DWDM optical communication systems[J]. Study on Optical Communications, 2010, (1): 1-4.
刘 毓, 孙亚尼, 方立杰, 等. SRS效应对DWDM光通信系统质量影响的分析[J]. 光通信研究, 2010, (1): 1-4.

15 Yunfeng Peng, Zeyu Sun, Shu Du, *et al.*. Propagation of all-optical crosstalk attack in transparent optical networks[J]. Optical Engineering, 2011, 50(8): 085002.

16 Marija Furdek. Physical- layer attacks in optical WDM networks and attack- aware network planning[J]. European Journal of Operational Research, 2011, 178(2): 1160-1167.

17 Shoba Krishnan, Anita Borude. Security issues in all-optical networks[C]. 2011 IEEE Annual SRII Global Conference, 2011. 790-794.

18 Wu Tao, Arun K Somani. Necessary and sufficient condition for crosstalk attack localization in all-optical networks [C]. Asia-Pacific Optical and Wireless Communications 2002, International Society for Optics and Photonics, 2002. 22-33.

19 Wu Tao, Arun K Somani. Cross- talk attack monitoring and localization in all- optical networks[J]. IEEE/ACM Transaction on Networking, 2006, 13(6): 1390-1401.

20 Zeyu Sun, Yunfeng Peng, Keping Long. Attack propagation of high- powered intrachannel crosstalk in transparent optical networks[J]. Optical Engineering, 2011, 50(8): 100501.

21 Poompat Saengudomlert. Analysis and Detection of Jamming Attacks in an All- Optical Network[D]. Massachusetts: Massachusetts Institute of Technology, 1998.

22 T H Shake. Assessing network infrastructure vulnerabilities in physical layer attacks[C]. Proceedings of the 22nd National Information Systems Security Conference, 2000. 228-237.

23 Ridha Rejeb, Mark S Leeson, Roger J Green. Fault and attack management in all- optical networks[J]. IEEE Communications Magazine, 2006, 44(11): 79-86.

24 R Rejeb, M S Leeson, R J Green. Multiple attack localization and identification in all- optical networks[J]. Optical Switching and Networking, 2006, 3(1): 41-49.

25 Peng Bingbin. Research on Defense Technology of Crosstalk Attack in Optical Network[D]. Xi′ an: Xi′ an Communications Institute, 2013.
彭炳斌. 光网络串扰攻击的防护技术研究[D]. 西安: 西安通信学院, 2013.

26 Nina Skorin-Kapov, Jiajia Chen, Lena Wosinska. A new approach to optical networks security: Attack-aware routing and wavelength assignment[J]. IEEE/ACM Transaction on Networking, 2010, 18(3): 750-760.

27 Marija Furdek, Nina Skorin-Kapov, Anna Tzanakaki. Survivable routing and wavelength assignment considering high-powered jamming attacks[C]. Communication and Photonics Conference and Exibition, 2011. 1-7.

28 Marija Furdek, Nina Skorin- Kapov. Attack- survivable routing and wavelength assignment for high- power jamming [C]. IEEE 17th International Conference on Optical Network Design and Modeling, 2013. 70-75.

29 Sun Zeyu. Propagation Effect of High- Powerd Intra- Channel and Inter- Channel Crosstalk Attack in All- Optical Networks[D]. Chongqing: Chongqing University of posts and telecommunications, 2012.
孙泽宇. 全光网络中大功率带内带间串扰攻击传播研究[D]. 重庆: 重庆邮电大学, 2012.

30 S C Tan. Ant-based physical attack and amplifier spontaneous emission-aware routing[C]. 2012 IEEE ICCT, 2012. 727-730.

31 Peng Bingbin, Zhang Yinfa, Liu Tao, *et al.*. Research on a RWA algorithm to enhance the performance of attack tolerance in optical network[J]. Optical Communication Technology, 2013, 37(3): 31-34.
彭炳斌, 张引发, 刘 涛, 等. 一种提高光网络攻击容忍性的RWA算法[J]. 光通信技术, 2013, 37(3): 31-34.

32 Ren Shuai, Zhang Yinfa, Wang Jingyu, *et al.*. A RWA algorithm for limiting the scope of physical layer attack influences in optical networks[J]. Study on Optical Communications, 2014, (1): 15-18.
任 帅, 张引发, 王鲸鱼, 等. 限制物理层攻击影响范围的光网络RWA算法[J]. 光通信研究, 2014, (1): 15-18.

33 Guanglei Liu, Chuanyi Ji. Resilient architecture of all-optical networks: probabilistic graphical models for crosstalk attack propagation[C]. 2006 IEEE International Symposium on Information Theory, 2006. 2914-2918.

34 Huang Qiong, Yin Pengfei, Sun Zeyu. Tolerance in high-powered crosstalk attack of DPSK and NRZ in transparent optical networks[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2012, 24(2): 144-147.