5G时代大容量光接入网的安全技术

Security Technology of Large Capacity Optical Access Network in 5G Era

张宏熙/ZHANG Hongxi
（中兴通讯股份有限公司，广东 深圳 518057）
(ZTE Corporation, Shenzhen 518057, China)

摘要：5G时代，光接入网会逐步承载5G应用，并向固移融合（FMC）的方向不断演进。在这种应用场景下，光接入网的安全将面临更多的威胁和挑战。无源光纤网络（PON）在演进到下一代PON2（NGPON2）的过程中，安全能力也逐步加强。5G网络面向垂直行业的安全应用使得光接入网面临着切片化的变革。光接入网必将融入到5G网络中，和5G网络一起为用户构建端到端的安全防护网。

关键词：光接入网；无源光网络；安全；5G技术

Abstract: In the 5G era, optical access network will gradually carry 5G applications and evolve to fixed-mobile convergence (FMC). The security of the optical access network will face more threats and challenges. In the process of the evolution from passive optical fiber network (PON) to the next generation PON2 (NGPON2), the security of PON is also gradually strengthened. At the same time, the security requirements of 5G network for vertical industry make the optical access network face the revolution of slicing. It is considered that optical access network will be integrated into 5G network, which can build the end-to-end security protection network.

Key words: optical access network; passive optical network; security; 5G technology

DOI：10.12142/ZTETJ.201904007
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1006.002.html

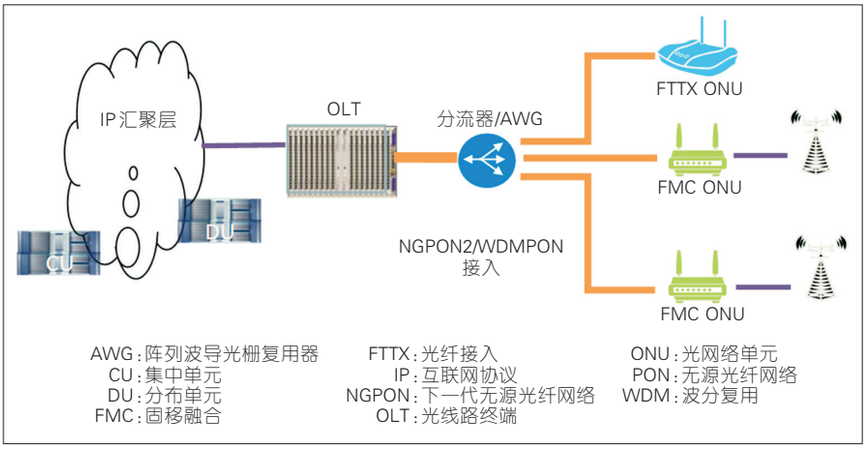
网络出版日期：2019-07-19
收稿日期：2019-05-26

1 5G时代光接入网的发展趋势

光纤接入网络经过十几年的高速发展，经历了光进铜退、光纤到小区，目前已经进入光纤到户的阶段。随着高清视频业务的不断兴起，以及移动网络从4G往5G的成熟演进，光接入网必将逐步承载大视频以及5G相关的业务，并伴随着虚拟化、云化的变革，朝着固移融合（FMC）（具体如图1所示）的方向发展。

因此，5G光接入网在承载传统接入业务的基础上，还将承载着更多的大视频业务以及移动业务，包括5G前传及中传业务。4 K/8 K高清视频业务的发展，对用户带宽的提升提出新的需求，目前光接入网的带宽从100 M、1 G逐步过渡到10 G。因此，光纤接入（FTTX）技术从1 G无源光纤网络（PON）演进到10 G PON，并向下一代（NG）PON演进。在高带宽提升的同时，5G移动前传或中传的承载，对光接入段的时钟精度要求在20 ns以下，时延要求500 μs以下。波分技术更适合传递低时延的业务，国际电信联盟电信标准化部门（ITU-T）G.989已经对NGPON2技术定义出了标准规范。另外，IEEE 1588技术会更多地应用在光接入的相关领域，并从IEEE 1588V2升级到IEEE 1588V3，以更好地保证时钟及时间的高质量传递。

FMC要求网络提供者给不同



▲图1 光接入网络固移融合的场景

服务等级(QoS)的业务或不同运营商的业务提供一个共享的接入平台，或者说在承载5G网络后，5G时代各垂直行业多样化的业务需求会间接反映到光接入网络上面。网络切片正是满足这类需求的重要技术，目前已经在各大运营商中开始部署。

视频业务的发展对网络带宽的优化提出了新的需求，通过光线路终端(OLT)的内置刀片部署边缘内容分发网络(CDN)节点是一个有效的解决方案。该方案可以降低视频业务的时延，增强边缘处理能力，让OLT成为边缘云计算平台的节点。同时，基于网络扁平化和虚拟化的要求，将宽带网络网关(BNG)下移以和OLT的转发面融合，同时控制面上移云端，电信网络软件定义网络(SDN)/网络功能虚拟化(NFV)化给业务的快速部署带来优势。

中兴通讯的大容量光接入平台(TITAN)支持未来NGPON2的大带宽接入，也支持5G前传和中传；内置刀片技术支持边缘计算处理能力，也支持切片技术、SDN/NFV的虚拟化演进。

2 5G时代光接入网的安全挑战

5G网络对于增强移动宽带(eMBB)、海量机器类通信(mMTC)、高可靠低时延(uRLLC)这3大应用场景和相关安全要求都有明确规划。5G网络是一个大容量的网络，在承载5G后，光接入网的光网络单元(ONU)从光纤到户(FTTH)的一个用户或少量用户转变为5G和FTTH融合的FMC接入，尤其是5G网络支持广连接、高覆盖的物联网接入，容量的提升要求其安全性也要上一个台阶。另外，5G是一个开放的网络，海量的设备会暴露在更靠近用户的区域，更易被黑客控制或攻击。一旦遭到安全攻击，影响面会非常大。如何避免受到网络攻击，如何避免敏感信息不被泄露，如何保证设备的可用性不受影响，如何在受到安全攻击的情况下又如何把损失降低到最小，都是需要我们持续研究的课题。本文中，我们将重点探讨5G安全挑战下的PON网络安全技术。

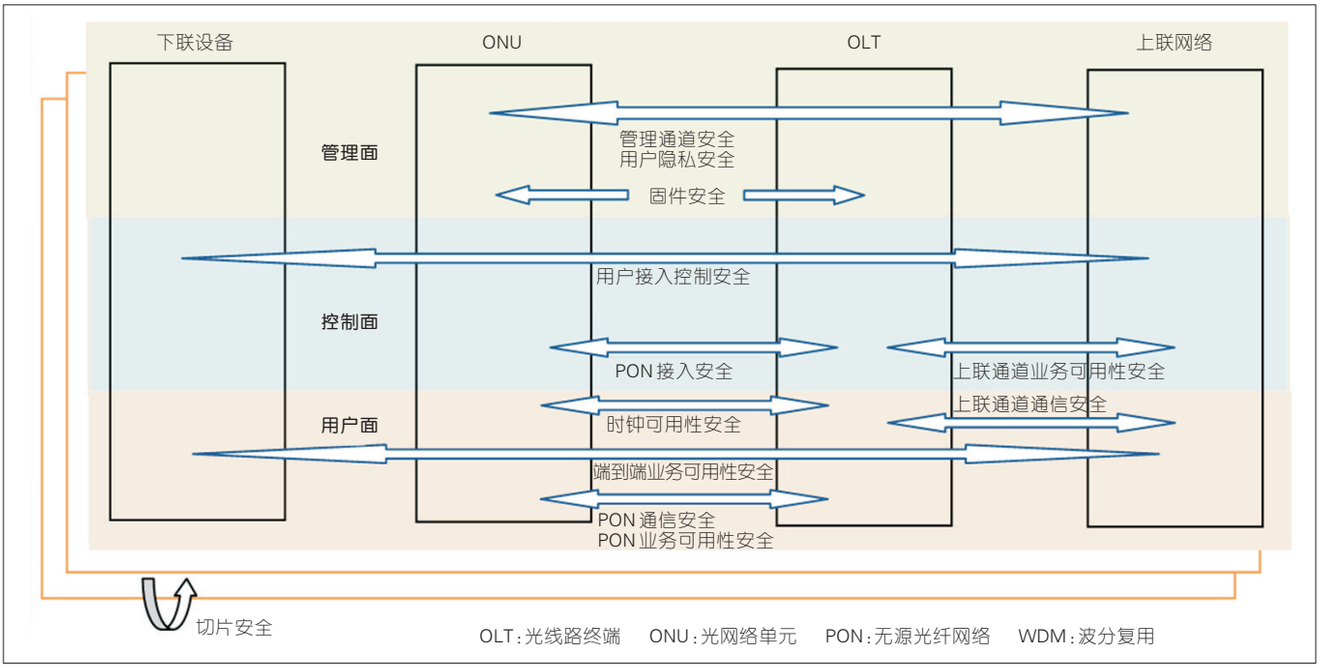
5G网络的承载，必然让光接入网络的架构产生重大变革。边缘节点的下沉，对接入网络的安全级别要求提高，原有针对核心网络的攻击模型需要引入接入层；为了支持切片功能，软件架构会进行重构，以便支持切片的快速部署、差异化服务及可剪裁等特性；为了提高通信系统的灵活性、可扩展性，提升业务的部署速度，还会考虑引入信息技术(IT)。

对于5G安全架构，NFV/SDN化和微服务化是其发展的必然趋势。5G安全架构会面临新的挑战，其安全功能也会和其他的功能一样在新架构里灵活地进行编排和部署。虚拟化、云化相关的云安全联盟已经在这方面进行了深入研究。本文中，我们会基于切片技术引入的光接入网架构变化做探讨。

3 光接入网的安全架构

参照ITU-T X.805的标准建议，我们对光接入网的安全架构进行分析。ITU-T X.805建议的安全架构分为3层(应用安全层、业务安全层、基础设施安全层)、3面(端用户平面、控制平面、管理平面)。针对3层3面的资产，我们定义了8个安全维度(接入控制、认证、不可否认、数据保密性、数据完整性、通信安全、可用性、隐私性)、5类安全威胁(摧毁、破坏、移除、泄露、中断)。

图2是光接入网络的安全架构，包括基础设施层的3个平面(用户面、管理面、控制面)相关的安全模型。其中，光接入网络主要涉及



▲图 2 光接入网络的安全架构

基础设施层，少量位于服务层。文章中，我们重点探讨基础设施层的安全。

（1）用户面。主要涉及 PON 层的通信安全、PON 业务可用性安全、端到端业务可用性安全、时钟可用性安全、切片安全等。

（2）控制面。主要涉及 PON ONU 接入安全以及用户接入控制安全等。

（3）管理面。主要涉及管理通道安全、用户隐私安全，以及固件安全等。

对于各层的安全，我们分别做如下考虑：针对 PON 层通信安全，主要考虑应用 PON 层加密技术；针对 PON ONU 接入安全，主要考虑应用 PON 接入认证技术；针对 PON 接入业务可用性安全，主要考虑应用 PON 保护技术；针对端到端业务可用性安全，主要考虑分布式的防拒绝服务（DoS）攻击技术；针对时钟同步安全，主要考虑时钟和时间传递的保护和备份技术；针对切片安全，主要考虑切片隔离和权限控制技术；针对用户隐私安全，主要考虑数据保护技术和脱敏技术；针对固件安全，主要考虑数字证书技术。

4 关键安全技术

4.1 PON 网络通信安全技术

通过建模分析，我们可以发现 PON 网络的通信安全主要存在以下威胁：

（1）在 PON 系统中，下行数据向 PON 上所有 ONU 进行广播。如果有恶意用户对 ONU 进行更换或重新编程，那他就能够分析出所有用户的所有下行数据。这是 PON 安全系统会遇到的“窃听”威胁。

（2）上行数据可以来源于接入特定 ODN 的所有 ONU。如果有恶意用户对 ONU 进行更换或重新编程，那他就可以通过伪造报文的方式来仿冒其他的 ONU。

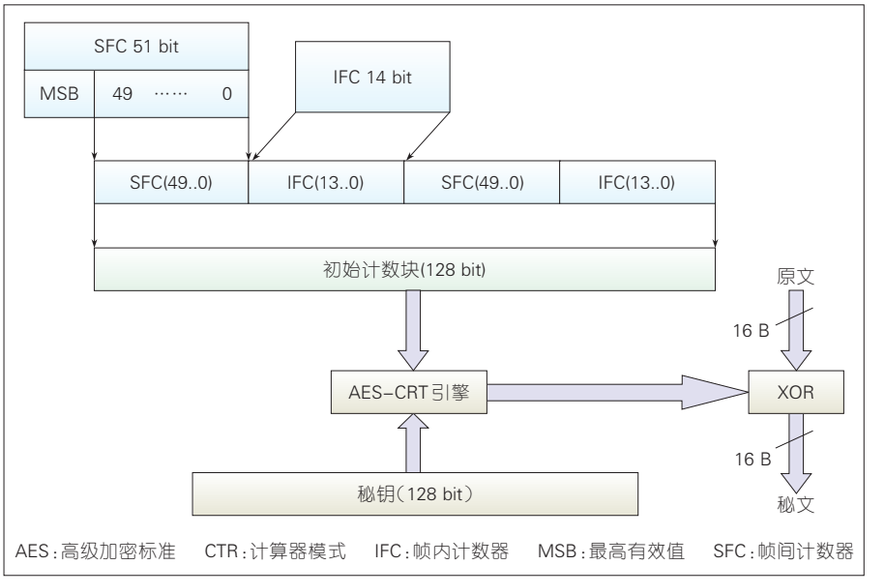
（3）攻击者还可以在基础设施上的不同点连接恶意设备（例如通过篡改街道机柜、备用端口或光纤电缆），以拦截或产生流量。根据不同位置，设备可以模仿 OLT 的行为，或可以模仿 ONU 的行为。

当然，点对点（PtP）模式的波分复用（WDM）-PON 相对于传统的 PON 网络或时分波分复用（TWDM）-PON 网络，安全威胁要弱一些，因为这种模式下不同用户通过波长进行了隔离。其主要的威胁来源于恶意破坏物理设备以模仿 OLT 或 ONU 设备的行为，或由于阵列波导光栅复用器（AWG）的性能问题或恶意干扰导致的不同波长间的串扰。对于物理设备的恶意破

坏，则需要加强其管理，提升 AWG 的抗干扰性能，并且强化 ONU 的认证机制。

针对加密技术，吉比特无源光网络（GPON）可采用 ITU-T G.984.3 建议的高级加密标准（AES）技术，它以 16 字节（128 bit）为单位进行操作，可以使用 128，192 或 256 bit 的秘钥。AES 加密采用计数器（CTR）模式，计数器宽度为 46 bit，由 16 bit 的帧内计数器和 30 bit 的帧间计数器组合而成。46 bit 的计数器复制 3 次后保留并使用最低的 128 bit，按照 AES 算法生成密码进行数据加密。加密秘钥则由 ONU 产生，并定期和 OLT 进行交互，OLT 收到秘钥后，和 ONU 同步进行切换。这些交互的具体过程借助 PON 物理层的维护管理（PLOAM）通道来完成。

ITU-T G.984.3 仅要求下行的加密，而 ITU-T G.984.3 以后的标准（XGPON 开始，包括 ITU-T G.987、ITU-T G.9807[4]和 ITU-T G.989[5]等）则要求了双向加密。双向加密中，这 64 bit 是由 14 bit 的帧内计数器和 51 bit 的帧间计数器的低 50 位组合而成（如图 3 所示）。另外，秘钥交互过程也更复杂，由 OLT 发起的多次交互来完成。秘钥交互和切换通过 PLOAM 通道完成。另外，ITU-T G.984 仅规范了下行单播数据的加密，而 ITU-T G.987 以后的标准则规范了上下行的单播，以及下行组播通道的加密。下行组播通道的加密秘钥由 OLT 生成，并通过光网络单元管理控制接口（OMCI）通道传递给 ONU。



▲图 3 下一代无源光网络的网络加密方法

在管理通道完整性安全方面，ITU-T G.984.3 仅要求 PLOAM 通道和 OMCI 通道采用循环冗余查核（CRC）校验，而 ITU-T G.987 以后的标准则要求这 2 个通道采用基于 AES 加密方式的消息认证码（AES-CMAC）的方式进行加密。

其他方面的加密技术，还包括 ITU-T G.983.1 定义的搅动（Churning）算法、中国电信在基于以太网的无源光网络（EPON）技术规范中要求的三重搅动技术等。PON 系统采用 CTR 模式的 AES 加密技术，相当于一次一密，安全性相对比较高，其薄弱环节在于秘钥（图 3 中的秘钥）从 ONU 到 OLT 的传递过程。从 ITU-TG.987 开始，各个标准均对秘钥的加密传送进行了规范，并要求采用电子密码本模式（ECB）的 AES 方法，但是其使用的秘钥是加密秘钥（KEK），存在一定的安全风险。在不考虑 PON 互通性的前提下，采用非对称的加密方式进行秘钥管理将能够较大程度地提升安全性。

针对 PtP 类型的 WDM-PON 系统，加密技术没有在标准里被定义。针对移动前传和中传，尤其是仅针对接口进行透传处理的场景，加密可主要依靠基站和分布单元（DU）/集中单元（CU）间的数据进行，如 MACSec 技术等。

在接入认证方面，ITU-T G.984 定义了 ONU 序列号和密码 2 种认证方式。序列号或密码通过 ONU 经由 PLOAM 通道上报，OLT 会将其和预设置的序列号或密码进行关联判断。ITU-T G.987 以后的标准定义了基于 Register ID 的认证方式，可以经由 OMCI 通道进行双向认证，也可以通过 IEEE 802.1X 进行双向认证。

未来的 PON 网络认证技术，应在已有标准化的认证技术基础上，增加对 ONU 的为许可证（license）控制、数字证书校验等新技术，即在

OLT上增加对ONU的许可控制，限制PON口下接入的终端型号，以及对应型号的接入数量。此外，如果在OLT上增加数字证书认证技术，针对ONU的固件进行基于数字证书的认证，可以最大程度地防止对ONU固件的篡改。可行的一种方式是在ONU上线的过程中对OLT和ONU上存放的数字证书进行比较。对于不一致的情况，则不允许上线。

4.2 PON网络流氓ONU防护技术

在PON网络里，存在这样一种威胁：由于某个ONU工作异常或攻击者通过ONU进行更换或重新编程，不依据OLT下发的授权时隙发送上行数据，或不依据OLT分配的逻辑通道ID发送上行数据。这样会影响到其他ONU的正常工作。由于上行时隙的重叠或逻辑通道的冲突，会导致其他ONU产生误码甚至业务中断，引起可用性问题。

我们可以从3个方面来应对该威胁：

（1）检测。

针对连续长发光型的流氓ONU，可以通过PON口的告警来识别。出现这种情况时，PON口会出现严重的误码，甚至上行突发丢失、出现信号丢失告警或ONU掉线告警。更严格的识别方法包括定期在非授权时隙进行检测，看能否发现从ONU送上来的连续光信号。

针对瞬间长发光型的流氓ONU，也可以通过PON口的告警来识别。出现这种情况时，PON口会出现误码，某些ONU的窗口漂移告警、上行突发丢失及ONU的掉线告警（一般是和流氓ONU相邻的ONU）。更严格的识别方法具体包括定期在非授权时隙进行检测，看是否有可能检测到非授权时隙瞬间发光。

针对逻辑通道非法抢占的情况，一般体现为某些逻辑通道业务异常或告警，辨识上会更困难一些。

（2）定位。

针对连续长发光型的流氓ONU，可以通过OLT对ONU顺序下发关光的指令或顺序物理断开ONU的方式。如果某个ONU关光后，长发光异常消失，则流氓ONU得到定位；如果某个ONU开电前后系统由正常进入异常状态，则流氓ONU也可得到定位。

针对瞬间长发光型的流氓ONU，可以通过检查动态带宽分配（DBA）列表中出现告警的ONU位置统计信息，得到流氓ONU及受影响ONU清单；通过和连续长发光型的流氓ONU类似的方式，进行该清单中ONU的关光或物理断开的方式，最终定位出流氓ONU。

针对逻辑通道非法抢占的情况，可以通过检测ONU上线时间，结合逻辑通道相关业务异常的时间，对非法强占逻辑通道的流氓ONU进行初步定位，并依次得到流氓ONU及受影响ONU清单，再通过类似连续长发光型的流氓ONU类似的方式，进行该清单中ONU的关光或物理断开，最终定位出流氓ONU。

（3）隔离或防护。

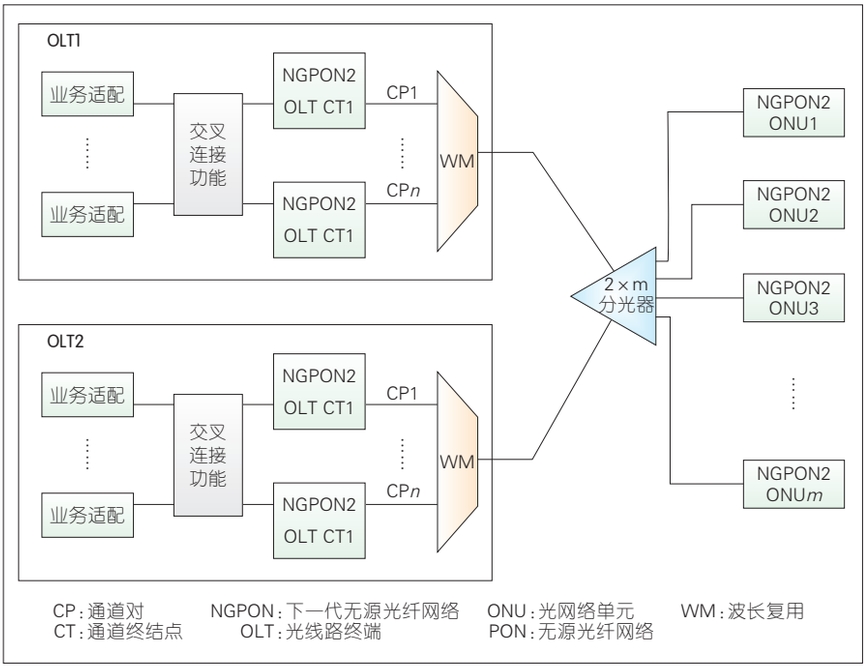
针对定位出的流氓ONU，可以远程发送下线指令，或采用人工关电来进行隔离。对于非法抢占逻辑通道的流氓ONU，也可以采用逻辑通道编号和ONU认证信息绑定的方式进行防护。上行的非法逻辑通道的业务无法匹配绑定清单中的条目，OLT会对该业务进行忽略。

以上的方法适用于普通的PON网络和NGPON2的网络。针对多波长的场景，在每个可能的波长中都需要进行检测和防护。但是，从某种意义上说，以上的方法仅能防范部分的流氓ONU，对于非常恶意的光层的干扰，还需要做进一步的研究。

4.3 PON保护技术

PON网络在应用时，一个比较严重的可用性风险是光路的故障，包括PON接口或OLT节点的故障。为应对这方面的可用性风险，做到失效时安全，PON网络标准定义了4类保护方式：Type A、Type B、TypeC、TypeD，最常用的是TypeB保护。以上保护类型，针对OLT上的PON口，需要进行冗余设计。一般主备端口位于不同的板卡或不同的OLT节点。针对5G接入，考虑到接入用户量比较大，之后将会越来越多地应用跨OLT的保护方案，而且由于基站距离短、密度大，所以更多使用TypeB保护，即主要保护主干光纤和OLT节点。针对AWG设备，则主要是依赖于物理方面的安全保护。图4为典型的Type B类型的PON的保护方案（定义在ITU-T G.989中）。

和普通PON类似，NGPON2可



▲图 4 PON 网络典型的 Type B 保护技术

以实现同一波长对之间的保护，即在这种情况下，不管是单波长的 ONU 或多波长的 ONU 都可以达到保护的效果。这主要是通过检测某个特定波长的光信号的告警来实现的。对于多波长的 ONU，如果各波长之间是负荷分担的，则可以定义多个波长组合成的一个逻辑链路，那么 Type B 则实现的是多波长的逻辑链路组间的保护。这种情况下可以定义为仅有一个波长出现故障即实现保护，或者只有所有的波长都出现故障了再进行业务保护。不论是 TWDM PON 还是 PtP WDM PON，保护的流程都是类似的。ONU 也可以采用不同的波长分别连接主备 OLT 端口。特别是在跨 OLT 保护的场景中，实现起来较为方便，可以减少 OLT 节点间的协议交互。当然，ONU 可以采用波长调谐方式实现在主备波长之间的切换，这在 ONU 支持可调谐或无色的情况下是非常适用的。

4.4 时钟安全技术

5G 前传和中传的承载，依赖于时钟传递和 IEEE 1588 时间传递技术。时间或时钟方面的信号劣化或中断，对基站的工作是致命的。

在时钟传递方面，OLT 需要支持多种或多路时钟源，包括外部大楼综合定时供给设备（BITS）时钟、同步以太网时钟源、全球定位系统（GPS）时钟源、IEEE 1588 时钟源等。在运营过程中，根据时钟源定义的优先级，需要优选出质量最好、优先级最高的时钟源。在主用时钟信号发生质量劣化或出现丢失告警时，可以马上切换到下一优先级的时钟。如果系统可以同时同步 2 路以上的时钟源，则可以使备选时钟质量得到较好的保证，同时切换过程可以做到基本无损。PON 光线路的时钟需同步于 OLT 的系统时钟源，可保证时钟信号在 PON 链路上的有效传递。对于 PtP 类型的 WDM-PON 网络，则只要 OLT 和 ONU 间特定的一个波长进行同步以太网信息的传递即可。

在时间传递方面，OLT 上也需支持多种或多路时间同步信号源，包括 GPS 时间、1 秒脉冲（PPS）+ 日期时间（TOD）信号、1588 协议端口等。精确时钟协议（PTP）模块进行时间信号的同步及时间源的优选。在运营过程中，根据时间源定义的优先级，优选质量最好、优先级最高的时间源。在主用时间信号发生质量劣化或者出现丢失告警的时候，可以马上切换到下一优先级的时间源。如果系统可以同时同步 2 路以上的时间源，则可以使备选时钟质量得到较好的保证，同时切换过程可以做到基本无损。时间信息在 PON 链路上的传递，主要依靠超帧信息作为基准，而且靠 OMCI 信令进行定期校准。对于 PtP 类型的 WDM-PON 网络，则只要 OLT 和 ONU 间特定的一个波长进行 IEEE 1588 协议的传递即可。

针对时钟的锁相环以及时间的 PTP 模块，系统需要考虑冗余备份，以便在发现故障的情况下可以自动切换到备用的模块。主备模块可以位于专用的时钟板卡上，也可以位于业务控制板上。如果位于业务控制板上，应结合业务板卡的运行情况综合进行板卡切换。不同的模块间应考虑主备时钟及时间信号的跟踪机制，以确保在主模块故障后可

以做到无损切换。

4.5 切片安全技术

光接入网络目前已经引入切片技术，但是主要应用在 OLT 侧，以面向不同的运营商共享同一物理设备的方式为主，主要有基于板卡、基于 PON 口、基于 ONU 等方式划分切片的应用。引入 5G 承载后，场景会有革命性的变化。以垂直行业应用为基础将会是切片划分的主要场景。因此，切片将会是从基站到核心网络的端到端的隔离，即切片经由光接入网时，ONU 会按照业务切分，在 OLT 上，将会在 PON 口内部按照不同的业务颗粒度进行切分。这种场景下，切片间的安全攻击、切片内业务可用性威胁都要基于光接入网络的特性来应对。

为了达到切片隔离的效果，首先需要保证切片内的业务调度。仅靠逻辑的隔离是不够的，需要在 QoS 层面对业务进行保证。不同的切片应用在转发面上不同的 QoS 单元中，例如 PON 接入层面，需要给不同的切片业务分配不同的逻辑通道，以对业务进行专门控制。在上行方向，需要能基于 Tcont 或 Tcont 组进行切片划分，不同的 Tcont 或 Tcont 组需要能保证 QoS 的调度等级，以达到某个切片被攻击但不会扩散到其他切片的效果。当然，对于 PtP 的 WDMPON 的场景，隔离就相对容易一些，可以采用不同波长或波长组为单位进行切片划分。

另外，在管理层面，切片的安全功能需要纳入端到端切片的场景中进行统一编排，从基础设施层、业务层到应用层都需要做到隔离。因此，管理面上的用户接入及业务控制是非常重要的。对于切片间的互相访问要进行严格地鉴权，禁止非法的跨切片互访。特别地，为防止跨切片的攻击，如果涉及不同的切片采用相同的虚拟网络的场景，应该在切片间配置防火墙进行隔离。

4.6 端到端业务可用性安全技术

端到端的业务安全是依据纵深防御的安全原则进行部署的。从 PON 接入层到切片层，再到用户业务管道，都需要进行部署。在防 DoS 攻击技术上，可以从接入节点到 ONU、OLT 再到核心网络建立起端到端追踪监测系统。通过各个设备的联动，在某个节点发现疑似 Dos 攻击的情况下，可以快速定位到攻击源头。同时，这也体现了一个分布式的网络防御架构，在接入网络复杂的情况下，可以在更靠近攻击源头的地方及早发现并遏制。完备的入侵检测系统（IDS）正是构筑在这样的分布式系统基础上的。

4.7 CDN 下沉相关安全技术

在可用性安全方面，需要考虑 CDN 设备和其他模块的隔离。在这方面，防火墙技术、防 Dos 攻击技术是非常重要的技术。来自于合法用户的仿冒核心网设备的攻击会是识别的难点，因此防火墙技术需要防止来自用户侧的攻击，也需要防止来自网络侧的攻击。根据 CDN 设备归属的业务，将 CDN 设备划入对应的切片也是必须的措施。另外，数据安全也非常重要，必须识别关键的隐私数据，并对该数据部署加密的存储和传输，以及分析使用方面的脱敏等措施。

5 结束语

光接入网络安全技术的部署对 5G 时代的光接入网的应用能起到一定的防护作用。当然，随着 5G 技术的发展和应用的深入，相关的安全继续也需要不断演进。光接入网必将融入到 5G 网络中，和 5G 网络一起，为用户构建端到端的安全防护网。

参考文献

[1] ITU-T. Gigabit-Capable Passive Optical Networks (GPON): Transmission Convergence Layer Specification: ITU-T G.984.3[S]. 2009
[2] ITU-T. 10-Gigabit-Capable Passive Optical Networks (XG-PON): Transmission Convergence (TC) Layer Specification: ITU-T G.987.3[S]. 2009
[3] ITU-T. 10-Gigabit-capable symmetric passive optical network (XGS-PON): ITU-T G.9807.1 [S]. 2016
[4] ITU-T. 40-Gigabit-Capable Passive Optical Networks (NG-PON2): Transmission Convergence Layer Specification: ITU-T G.989.3[S]. 2015
[5] ITU- T. Security Architecture for Systems Providing End-to-End Communications: ITU-T X.805 [S]. 2003
[6] National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2[R/OL].[2019-05-25]. https://aisel.aisnet.org/amcis2017/TREOs/Presentations/51/
[7] 任建勇. 光接入网的安全技术研究[J]. 信息网络安全, 2009,(10): 61. DOI:10.3969/j.issn.1671-1122.2009.10.022
[8] 张位. 光接入网络的安全性及其增强技术研究[D]. 成都: 电子科技大学, 2017
[9] 乔婧, 潘武, 杨静. 全光网络的安全及防范分析[J]. 光通信技术, 2008, 32(3): 10. DOI:10.3969/j.issn.1002-5561.2008.03.003

作 者 简 介

张宏熙，中兴通讯股份有限公司上海研发中心总工；主要研究领域为光接入网、光线路终端系统、通信产品安全等；先后主持及参与过多个光接入项目的研发；已申请专利 10 余项。