OTN系统安全防护和加密技术应用研究

Research on the Application of Security Protection and Encryption Technology in OTN system

沈利泉[1]，刘　军[2]（1. 浙江省通信产业服务有限公司，杭州 312300；2. 华信咨询设计研究院有限公司，杭州 310052）
Shen Liquan[1], Liu Jun[2]（1. Zhejiang Communications Service Co., Ltd., Hangzhou 312300, China; 2. Huaxin Consulting Co., Ltd., Hangzhou, 310052, China）

摘　要：
OTN系统存在网络安全和光信号被探测2方面的风险。分析了OTN系统面临的安全威胁，结合OTN系统L1层的加密技术和方案，从OTN系统网络安全防护和OTN设备自身安全防护的角度，阐述了OTN传输网络系统安全方案，提出了提升OTN系统安全性的方案和建议。

关键词：
OTN；安全；加密
doi：10.12045/j.issn.1007-3043.2019.11.014
中图分类号：TN915
文献标识码：A
文章编号：1007-3043（2019）11-0065-06

Abstract:
OTN system has two risks: network security and optical signal detection. It analyzes the security threats faced by OTN system, and combined with the encryption technology and scheme of L1 layer of OTN system, it expounds the security scheme of OTN transmission network system from the perspective of OTN system network security protection and OTN equipment self security protection, and puts forward the scheme and suggestions to improve the security of OTN system.

Keywords:
OTN; Security; Encryption

引用格式：沈利泉，刘军. OTN系统安全防护和加密技术应用研究[J]. 邮电设计技术，2019(11)：65-70.

0 前言

OTN网络作为一个透明的传送通道，具有端到端传送的特性，对于每个再生段两端的站点来说，OTN系统类似一段光纤，近似处于OSI（Open System Interconnection）参考模型第1层（L1）。所以，一般认为OTN系统本身是相对安全的。

随着互联网信息网络的发展，信息安全显得越来越重要，我国已发布《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019，简称为等保V2.0版本）和《信息安全技术 网络安全等级保护定级指南》（GA/T 1389-2017）。OTN系统在网络中存在安全和防护缺陷，OTN系统是否需要进行相关安全防护和加密保护，也正逐渐成为OTN网络建设和设计需要研究和考虑的内容。

收稿日期：2019-10-08

1 OTN系统面临的安全问题

1.1 OTN系统在网络中的安全

OTN系统是将客户业务透明地从一个地方传送到另一个地方，比如OTN设备系统会将接入网的业务传送到核心机房IP承载网的核心路由器进行路由。在这个传送过程中，为了将客户业务适配到传送网的

信号速率中，传送网设备会对客户业务进行一定的封装，同时，进行一些差错控制和信号质量的监测。传送网设备不会对其他设备传过来的客户业务进行处理，这是传送设备透明性的要求。

OTN系统在通信网络中的分层模型如图1所示，OTN系统的安全问题需要从应用层、网络层、物理层和接入层等方面考虑。

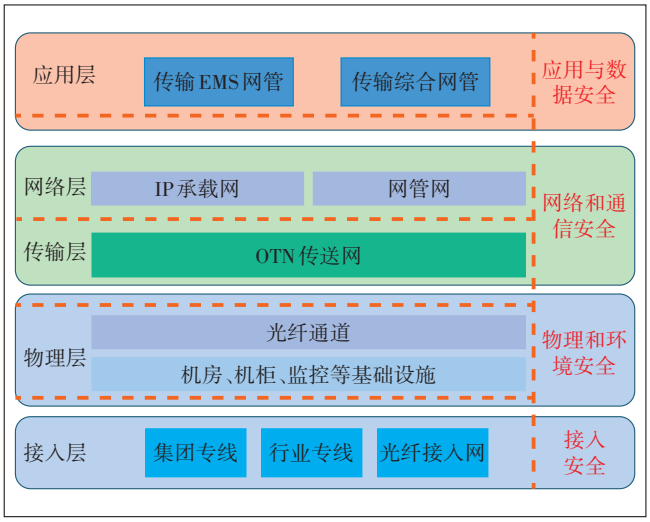

图1　OTN系统在通信网络中的安全问题示意图

a）应用与数据安全。OTN系统作为承载通道，既承载了面向用户应用的业务数据，也承载了OTN系统内部网络管理的数据，所以，一方面需要从整体安全的角度对数据、业务等层面进行安全风险分析和防护，另一方面也需对OTN系统本身的数据平面采取相关安全防护或者加密措施。

b）网络和通信数据安全。OTN传送网一般在网络层会与其他专业网络互联互通，如IP承载网、网管网等。为保证OTN系统的安全性，可以按第三方网络边界、纵向网络边界的边界防护整体思路，实施边界防护。

c）物理和环境安全。OTN系统的物理和环境安全主要从机房门禁、智能机柜、光纤信号隔离、安防监控等方面考虑相关安全防护措施。

d）接入安全。OTN传送网一般支持多业务的接入，一旦外部业务不加阻拦地接入到网络中来，就有可能破坏网络的安全边界，使外来用户具备对网络进行破坏的条件。仍需按第三方网络边界、纵向网络边界的边界防护整体思路，实施边界防护。对流经此区域的数据包严格按照安全规则进行过滤，将不安全的或不符合规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。基于数据包的源地址、目的地址、通信协议端口、流量、用户、通信时间等信息，执行严格的访问控制。

1.2 OTN设备信号被直接物理探测的威胁

OTN设备由于没有MAC地址、IP地址被用来伪造和攻击，OTN设备的电交叉又位于交叉模块和单元内，对于外部的路由器、交换机等网络网元来说，OTN设备是不可见和无法接触的。所以，对OTN系统的攻击常常集中在光层，利用OTN光通道、光纤非法窃听或者干扰通信。

对OTN系统的非法探测主要有以下途径。

a）利用不同组件的串扰。OTN系统的分波器（AWG），将1根光纤中传输的多波长信号按照不同的波长分解到不同的分波器端口，信号之间的串扰会让其中一小部分信号泄露到其他光通道，这部分泄露的信号足以让攻击者检测到它的存在，并从中恢复出一部分数据。

b）利用设备和光纤的输出端口。如果攻击者非法接入到OTN设备或光纤的输出端，就可以窃听到信道的信息。

c）利用光信号泄露，对光缆或光纤直接探测。光纤弯曲半径较小（光信号对反射面的入射角小于临界值），一小部分光信号会折射出光纤，导致信息泄露；利用特殊装置或分光技术就可以直接在光通路上提取信息、探测数据。最典型和直接的非法探测方式如图2所示，当纤芯中的光损不到1%的时候，只需要3个步骤就能利用相关检测装置和解密软件进行数据恢复和探测。

第1步截取光信号：目标光纤被放入设备适当弯曲，光学检测装置提取折射光线转发给光电转换设

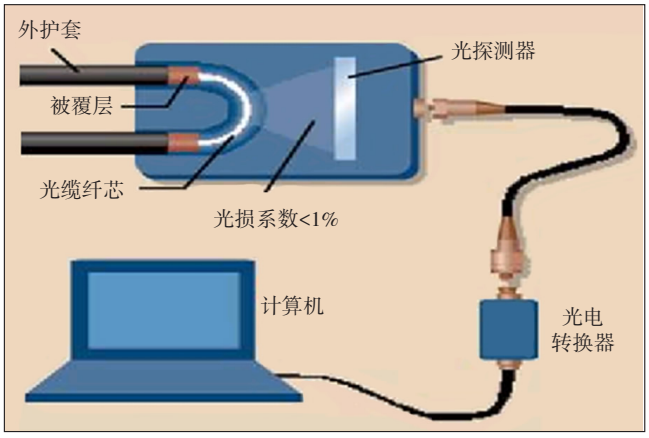

图2　光信号被非法探测示意图

备。

第2步转换成电信号：光电转换设备把光信号转换为电信号，并将数据传送到电脑。

第3步数据解读：在电脑上运行软件，进行数据解读。

综上所述，安全威胁需要接触到光通道（波分端口）和光纤，并探测到通道中的信号。所以一方面需要从物理层面保护好OTN设备及光纤光缆，另一方面需做好OTN系统在网络中的安全防护，加强自身的安全防护，并考虑对OTN传送通道中的光信号、电信号进行加密保护。

2 OTN系统的网络安全防护

2.1 OTN系统安全防护点

综合1.1所述，OTN系统的安全威胁来自OTN系统内部和边界2方面。OTN系统内部安全威胁是指OTN系统自身的健康，如软、硬件的安全问题，合法用户在使用网络资源的时候，有不合规的行为、误操作、恶意破坏等情况发生。边界安全威胁是指OTN系统的接入、与外界互联互通引起的安全问题，包括入侵、病毒与攻击等。

OTN系统数据安全的威胁来自系统内部与边界2个方面，而OTN系统接入安全的威胁主要来自边界。OTN系统的数据安全及自身相关软硬件的防范措施在第3章详细阐述。OTN系统安全防护的关键在于边界防护，应对OTN系统外的入侵就要在网络边界上建立可靠的安全防御措施。

2.2 OTN系统防护方案

2.2.1 防火墙、安全网关

在工程建设中，业务承载服务层（IP承载网、接入网）、网管通道（网管网）与OTN承载层通过边界网关（下一代防火墙、业务监控网关、多重安全网关等）进行安全防护。边界网关的功能建议如下：

a）访问控制/包过滤：安全策略的主要基础目标是限制外来资源访问边界内的网络和系统。网络应只许可必要的内部连接和服务，并限制内部用户与外部目标连接。

b）识别与认证（I&A）：通常认为在边界以内的用户是被信任的，访问内部网络的外来用户必须通过认证。通过防火墙屏蔽访问的认证方法有一次性密码、时效型密码和挑战响应案。

c）防病毒：支持恶意代码防范功能。

d）加密：部分防火墙可以提供其他安全服务，包括通信流加密和解密。以加密方式通信，发出和接收防火墙必须使用兼容的加密系统，如Internet协议安全（IPSec）标准。

e）IDS/IPS：支持入侵检测、入侵防御功能。

f）审计：审计是指跟踪分析和监督检查用户和管理员的行为。审计的目的是确定用户网络行为的本质。

g）网络地址转换：网络地址转换（NAT）可以把IP地址从一个域转换到另一个域，并给主机提供透明的路由。NAT能够让局域网使用一系列内部通信流的IP地址和2套外来通信流的地址。

h）防止渗透：防火墙应保护自己免受攻击，如果被攻破将会让黑客访问整个网络，防火墙应具备防止渗透的功能。

i）配置&第三方监视：合理配置防火墙组件是边界安全的关键。防火墙的大多数漏洞都来自于不合理配置或维护防火墙。

2.2.2 业务隔离

OTN系统网络业务服务层的不同业务主要通过隔离的手段进行边界防护，隔离方式包括物理波道隔离、子波道隔离、端口隔离、VPN隔离等；网管网也通过类似的隔离手段隔离其承载的网管业务。主要隔离手段如下：

a）不同业务之间子波道隔离+VPN隔离。

b）支撑系统之间不同业务子波道隔离+VPN隔离。

c）业务系统与支撑系统波道隔离+端口隔离+VPN隔离。

d）IP承载网、接入网与网管网波道隔离+端口隔离。

综上所述，OTN系统的网络安全防护的整体方案如图3所示。

3 OTN设备的硬件和软件安全防护

在配置和设计OTN设备和系统时，可采取相关硬件和软件方面的安全防范措施。

3.1 硬件安全

OTN设备的硬件平台，可采取如下安全防范措施：

a）采取支持FEC特性编码，对光入侵、光扰乱等攻击行为进行纠错。部分厂家的设备还支持私有的

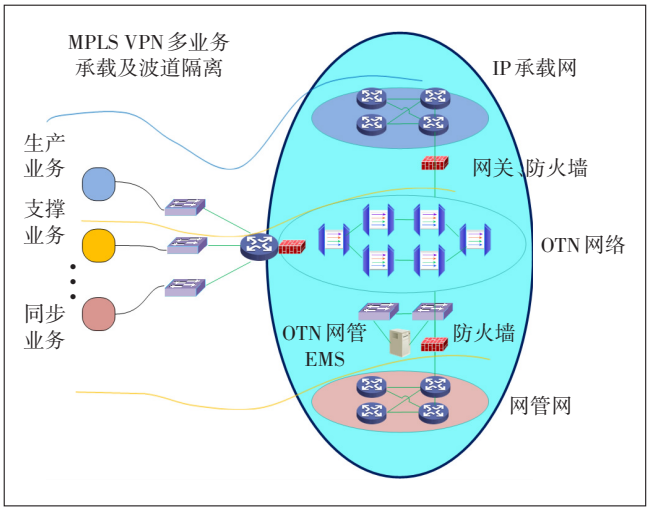

图3　OTN系统网络安全防护示意图

增强型编码，光窃听者即使截获了光信号，如不了解该编码技术也很难还原原始的数据帧内容，从而有效防止光窃听的安全威胁；该编码超强的纠错能力使得OTN系统对光入侵、光扰乱具有更强的防攻击能力。

b）OTN设备L1层加密，实现业务数据VC/ODU$_k$硬管道安全直达。

c）硬件平台设计采取控制平面、管理平面、数据平面物理隔离的设计方法，即使其中一个平面受到安全威胁，不会影响到其他平面运行。

d）充分利用OTN设备对波长转换器、光放大器、光发送单元、光分波单元等的光信号监视和告警功能，加强监视和管理。

3.2 软件安全

OTN设备软件系统在不同平面（O&M管理数据、控制平面数据和业务数据）采取相应的安全策略；各平面的数据使用不同的VLAN ID来区分和隔离，3个平面上的数据共享物理带宽，各平面使用了不同的通信地址，某一平面数据异常不会影响到其他类型的数据和安全。

数据平面通过加强以太网业务访问控制和过滤，负责隔离和处理进入设备的业务数据流，丢弃各种不合法的错包，根据硬件转发表项对业务数据报文进行转发。一方面能有效防止用户业务报文被恶意窃取、修改、删除，保证用户数据机密性和完整性；另一方面保证硬件转发行为可控，防止转发表项被恶意攻击篡改，保证转发平面稳定可靠运行。

OTN设备软件系统采取的相关安全策略如表1所示。

表1　OTN设备软件系统采取的安全策略

平面	功能名称	安全策略措施
管理平面	RADIUS认证与授权	集中式远程账户合法性校验与授权，降低账户维护成本
	TCP/IP协议栈防攻击	具备基本的TCP/IP防攻击能力，比如错误的IP报文攻击，ICMP的ping和Jolt攻击，Dos攻击等
	SSL/TLS加密通信	具备SSL3.0/TLS1.0能力，提供基于安全证书的加密管道
	SSH安全通信	提供了SSHv2的服务端能力，提供了SFTP客户端服务
	OSPF路由协议	提供了OSPFv2，具备标准的MD5认证
	NTP协议	提供了NTPv3，具备MD5认证和权限控制
	SNMP管理协议	提供了SNMPv3，具备安全认证和数据加密功能
控制平面	OSPF路由协议	具备标准的MD5认证方式，可有效保证报文完整性
	RSVP资源计算协议	具备标准的MD5认证方式，可有效保证报文完整性
数据平面	错包丢弃	丢弃各种不合法的包，比如长度小于46字节的以太报文
	业务隔离	二层逻辑隔离，水平分割，物理隔离
	严格隔离用户业务	运营商网络的MPLS业务与来自客户业务严格隔离

4 OTN系统的安全加密技术

在OTN设备系统L1层安全加密的优势主要体现在时延、带宽利用率和多业务支持，其与L2/L3层加密的对比如表2所示。

目前，对OTN设备系统光信号、电信号的加密保护，有以下几种方式：

a）基于数字包封技术的电信号加密。数字包封技术在OTN网络的光通路层得到了广泛应用。基于数字包封技术的加密可以在不区分业务的情况下，对在OTN网络上传输的数据进行加密保护，是一种有效的加密保护方法。此方法首先解波分复用，然后在每个波长上针对数字包进行加密保护。

表2　OTN设备L1层加密与L2/L3层加密的对比

加密方式	L1	L2	L3
网络延迟影响	中间节点可透传、ns级时延	无法透传，逐点加密，μs级时延	需要上三层协议层处理，ms级时延
加密范畴	物理链路层加密	链路层加密	IP业务端到端加密
带宽利用率	利用现有OTN开销字节，100%	以太网帧增加安全字节，影响线路吞吐率	每个IP分组增加验证标头，影响线路吞吐率。报文越短影响越大
多业务支持	任意业务类型	不支持非以太业务	不支持非IP流量

b）基于光包加密技术的光信号保护。光包由包头和净荷组成，首先可利用宽脉冲标记法、高强度脉冲标记法、微波副载波光标记交换法以及电光调制光标记交换法等技术提取分离出净荷，然后通过光逻辑器件对提取出来的净荷进行加密，最后组合包头和已经加密的净荷，实现数据安全保密。应用基于光逻辑器件的光包加密技术，能够满足分组交换光网络上承载的任何一种协议数据的安全保密需求。

受限于光逻辑器件的发展，基于光包加密技术缺乏相关的产品支持，目前仅有基于数字包封技术的电信号加密方式，在部分厂家设备型号中得到支持，相关产品处在试商用阶段。

4.1 OTN系统电信号加密技术

OTN系统电信号加密主要是采用客户侧业务加密形式。OTN设备配置带OTU加密模块的单板，客户业务接入配置了加密功能的OTN设备后，通过安全加密设备发送来的密钥加密，以加密的业务形式在OTN网络传送，并在接收端OTN设备上解密，实现业务数据在OTN网络中的安全传输。OTN客户侧业务加密方案如图4所示。

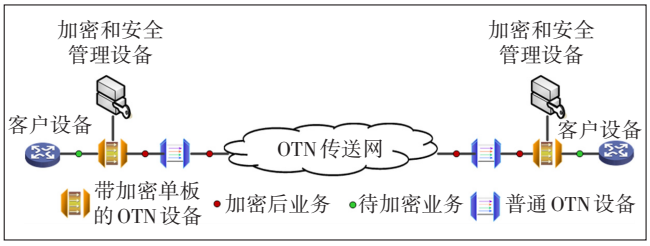

图4　OTN客户侧业务加密方案示意图

可以对任意客户业务进行加密，OTN客户侧业务加密具体实现原理如图5所示。OTN客户侧业务加密一般采用AES加密算法，客户业务先进行适配，进入合适的OPU_k容器，在OPU_k映射进入ODU_k之前，采用内部或外部密钥对OPU_k的净荷区进行AES256加密；对端在ODU_k解映射成OPU_k，采用协商的密钥对OPU_k的净荷区进行AES256解密，恢复成原有客户业务。

OTN客户侧业务加密的优势体现在如下3点：

a）对客户信号映射后的OPU_k进行加密，不影响OTN线路速率，和现网OTU线路无缝对接。

b）加密后的OPU_k数据可以被OTN网络透传和调度，不影响OTN现网的监控和管理。

c）密钥协商和加密管理使用OTN开销中的PSI字节，可被OTN现网透传。

4.2 OTN设备支持加密的现状

目前，国内主要的OTN设备供应商均能提供基于客户侧加密的OTN设备和系统。OTN设备和L1层业务加密系统由带加密单板的OTN设备、安全管理工具（例如SMT——Security Management Tool）和网络管理系统3部分组成。业务在源端加密后，经OTN网络传输至对端，对端再对业务进行解密，这样就可以接收源端发送的真实信息；双向加密过程包括认证、密钥协商和加解密。

国内支持L1层业务加密OTN设备在加密原理、加密方式和设备型号等方面的对比如表3所示。

表3　国内支持L1层业务加密OTN设备的对比

	加密原理	加密方式	支持密钥输入	安全管理平台	支持设备	应用范围
华为	AES算法	OPU_k净荷加密	支持外部、内部密钥	SSLx安全协议	OSN9800	干线、城域网
中兴	AES算法	OPU_k净荷加密	支持外部、内部密钥	SSLx安全协议	ZXMP M721/ZXONE 7000	城域网

4.3 OTN设备加密与否的分析

在实际工程建设中，应从应用场景、安全测试验证、建设、维护的角度，评判是否采用OTN设备加密，特别是考虑应用场景下业务逻辑的匹配程度。

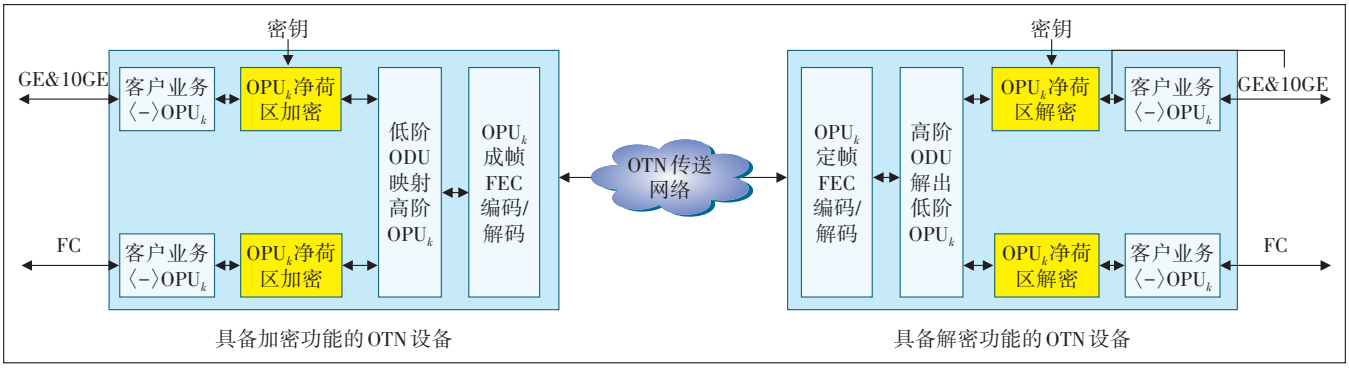

图5　OTN客户侧业务加密原理

a）应用场景分析。现有的OTN设备的加密应用都是在大客户专线接入层面，主要是金融类大客户，特别是银行专线项目，如中国工商银行、北欧Nordia银行、俄罗斯Serbank银行等。

在国内外OTN长途干线上，无类似OTN客户侧业务加密的商用案例，主要是由于现有的OTN设备加密功能都是基于源端口到宿端口中的每条业务，而每条业务需单独配置，适用于接入业务层面的单一的端到端的大客户场景，与OTN干线层面多样化、多点化的业务逻辑往往不匹配。

b）安全测试和验证分析。OTN客户侧业务加密协议、算法是非常成熟的（标准AES-256加密算法，且采用CTR模式），但在实际大规模应用之前，应注意检验业务交互逻辑上是否有安全漏洞，提前进行相关网络的安全性测试、安全验证和审计。

c）建设角度分析。通信网络的建网思路一般应是减少长途OTN干线、中继OTN站点对业务的处理，以提供便捷、高效的快速转发，而将网络的业务感知、控制、加密等放到边缘的主机节点上来做，从ATM到以太网、从IP到SDN的发展都是如此。

在OTN系统本身具有较丰富的安全防范和报警功能的情况下，特别是OTN传输系统往往承载的数据流量非常大，业务种类也非常多，数据解密和恢复时间也较长，想要持续对OTN网络非法探测难度非常大。OTN作为透明的业务传送通道，如果把加密功能放到OTN传送层（L1），则每条业务均需要配置成对的含加密或解密功能的端口，配置加解密管理终端及系统，整体投资预计将会提高15%以上，相对来说，物理防护更加直接和有效。

d）维护角度分析。若采用带有加密功能的OTN设备，需要对每台设备配置加解密软件和账户，再用加密子账户进行端口分配，然后针对每个端口的每条业务单独加密配置、维护，维护复杂。另外，带有加密功能的OTN设备本身在运行和维护上存在一些受限内容，如表4所示。

表4　OTN加密设备在应用上的主要受限

项目	特性依赖和限制内容
支路SNCP保护	不支持在同一个端口同时配置加密和支路SNCP保护
ASON	在电层ASON的关联业务场景下，无法支持加密特性
单端时延	数百纳秒
汇聚和自适应模式	单板在ODU1汇聚及ODU1_ODU0模式下，不支持加密

5 结束语

综上所述，提升OTN系统的安全性需要从OTN系统的网络安全、OTN系统自身的软硬件安全、OTN设备加密传输几个方面去考虑，同时，在实际工程建设和设计中，需结合应用场景、安全测试和验证、建设和维护等方面，评估是否有必要应用带加密功能的OTN设备。

参考文献：

[1] 刘涧疆，李鹰. 波分复用系统加密技术研究[J]. 信息安全与通信保密，2011(12)：83-85.
[2] 唐世庆，孙以泽，王琦，等. 一种光传送网的加密和密钥传送策略[J]. 光通信技术，2018(4)：10-13.
[3] 常玲，巍来，杜雪涛，等. 七号信令网络安全威胁分析与防范[J]. 计算机工程与应用，2017，53(S3)：148-152.
[4] 杨天宝. 提高OTN系统安全性的设计要点分析[J]. 数字通信世界，2017(8)：112，214.
[5] 郎为民，焦巧，胡东华，等. LTE与非3GPP接入网的系统架构研究[J]. 邮电设计技术，2010(8)：41-44.
[6] 万芬. 浅谈ASON控制平面及应用[J]. 邮电设计技术，2010(1)：74-76.
[7] 杜雪涛，袁捷，吴晓岩，等. Non-3GPP对EPS的安全接入研究[J]. 电信工程技术与标准化，2009(7)：11-15.
[8] 辛彦鹏. ASON技术及其在工程中的应用研究[D]. 呼和浩特：内蒙古大学，2012.
[9] 郭煜. 可信云体系结构与关键技术研究[D]. 北京：北京交通大学，2017.
[10] 杨力. 无线网络可信认证技术研究[D]. 西安：西安电子科技大学，2010.
[11] 中国国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国质检出版社，2019.
[12] 中国标准化委员会. 信息安全技术 网络安全等级保护定级指南：GA/T 1389-2017[S]. 北京：中国标准出版社，2017.
[13] 工业和信息化部. 传送网安全防护要求：YD/T 1744-2009[S]. 北京：人民邮电出版社，2009.
[14] 工业和信息化部. IP承载网安全防护要求：YD/T 1746-2013[S]. 北京：人民邮电出版社，2013.

作者简介：
沈利泉，高级工程师，浙江省通信产业服务有限公司副总经理，长期从事传送网、数据承载网的规划设计和新产品新技术研发管理工作；刘军，高级工程师，硕士，主要从事传送网、量子通信网络的规划和设计研究工作。