DOI：10. 16516/j. gedi. issn2095-8676. 2015. S1. 036

PTN 安全防护能力与广域控制保护适用性分析

黄维芳，金鑫，文安，魏承志，刘年
（中国南方电网有限责任公司，广州 510620）

摘要：从业务接入与网络传输过程详细分析了 PTN 安全防护能力，提出 PTN 虽然安全防护能力比一般数据网络设备高，但也属于逻辑隔离性质；广域控制保护业务属于电网生产控制类业务，不能采用 PTN 与其他管理业务混合承载。
关键词：PTN；安全防护；广域控制保护
中图分类号：TN915　　**文献标志码**：A　　**文章编号**：2095-8676(2015)S1-0161-04

PTN Security Capability and Applicability Analysis of Wide Area Protection and Control System

HUANG Weifang, JIN Xin, WEN An, WEI Chengzhi, LIU Nian
(China Southern Power Grid. Co., Ltd. Guangzhou 510620, China)

Abstract: This paper analyzes PTN security access and network capacity from a business transfer process, proposed PTN network security capabilities, although higher than the average of data network equipment, but also belong to the logical isolation in nature. Proposed wide-area control and protection business is power production control class of business, can not be used PTN network management business mix with other bearer.
Key words: PTN; safety protection and wide area control

PTN(分组传送网，Packet Transport Network)可以提供一种“柔性”传输管道，更加适合承载 IP 业务，PTN 本质上是一种基于分组的路由架构，该架构能够支持多种双向点对点通道和各种粗细颗粒业务，并且具有端到端的组网能力。通过继承了 SDH 技术点对点连接的完美 OAM 体系，PTN 具备传统路由器不具备的丰富的保护方式，当发生网络故障时能够实现基于 50 ms 的电信级业务保护倒换，实现传输级别的业务保护，保证网络具备错误检测、保护切换和通道监控能力。PTN 对增强以太网和传统路由器技术具有上述优势是，这也正是 PTN 区别于两者的重要特点。

PTN 可满足电力系统综合业务承载需求，可实现变电站、调度所、配电所、电力营业厅、智能抄表、电力智能大厦、电力智能小区等多种业务的接入[1-2]。业务在网络中采用通道/PW、路径/LSP 的方式传送，以保证网络流量可规划，保证业务 QoS、时延、抖动等指标[3-4]。近年来 PTN 技术的不断成熟，在智能电网中迫切需要利用 PTN 技术的满足了日益增长的基于 IP 的智能电网新业务的接入需求，大幅改善可靠性、互动性、实时性等方面的指标，从而促进智能电网中电力通信的发展[5]。

从传输时延和丢包率来看，PTN 的 LSP 通道隔离性能(相关性)接近物理通道隔离能力[6-7]。另外，PTN 技术在电力通信中应用还需要满足电力业务安全防护规定的要求，PTN 技术安全防护能力需进一步研究。

1　电力业务安全防护要求

国家发改委 14 号令对电力监控系统通信做了一定的要求，总体来说体现四句话：“安全分区、网络专用、横向隔离和纵向认证。”

收稿日期：2014-12-01
作者简介：黄维芳(1986)，男，江西宜春人，工程师，硕士，主要从事电力系统继电保护研究工作(huangweifang@csg. cn)

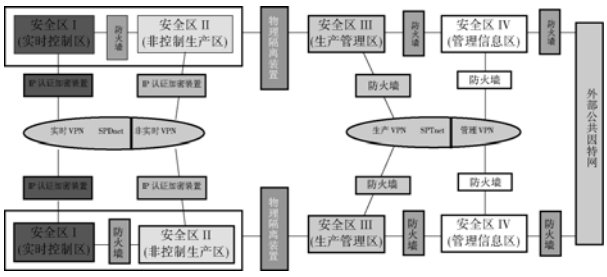

图1 发改委14号令安全等级划分示意图

Fig. 1 Schematic Diagram of the National Development and Reform Commission Order No. 14 Safety Classification

安全分区：把SCADA(EMS)系统和电力交易系统等对生产相关对安全要求等级较高的信息定义为调度数据网专用网络数据区。而把解决办公自动化，信息管理系统对实时性和安全性要求不是很高的业务划分为电力信息网络。

网络专用：14号令要求电网中如电力调度数据网与电力综合数据网络实现物理隔离。

横向隔离：在调度数据网中各种数据业务实现业务的VPN隔离，同样在综合数据网中也要实现各种不同类型业务的VPN隔离。

纵向认证：电力控制业务安全区的边界部署纵向认证加密装置；管理信息安全区的纵向边界部署硬件防火墙。

2 PTN安全防护能力分析

由PTN的转发模型可以知道，在PTN设备中，线路复用过程不会导致各类业务间报文互穿和业务相互影响；网络安全和业务隔离度主要取决于查表转发和调度过程的行为；一般而言，PTN设备中的查表转发和调度机制更先进，网络更安全和隔离度更高。

PTN采用MPLS-TP协议进行业务的转发，针对每个业务建立不同的标签交换路径(LSP)。每个业务独享属于自己的LSP通道，如图2所示。

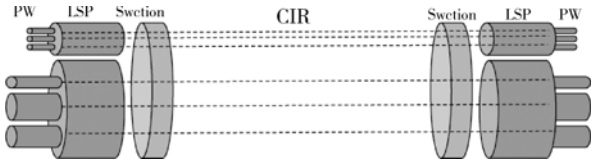

图2 PTN业务隔离模型

Fig. 2 PTN Communication Isolation Model

PTN网络主要是通过MPLS VPN技术对各类业务进行深度的隔离。MPLS VPN通过标签交换的方式，每个标签对应一个用户的数据流，易于用户间数据的隔离，在公有网络上可以提供私有数据网络，满足业务对安全性和私密性的需求。

PTN设备可以按需要虚拟成数千甚至数万个交换机，不同的业务由不同的虚拟交换机完成，各种业务报文缓存的独占性或可管理性决定了业务在设备中的隔离性能。

在PTN设备中各虚拟交换机的表项是相互隔离的，比如每个虚拟交换机的MAC地址表的大小是单独可配置的，不存在某个虚拟交换机的MAC地址表无限扩大，挤占其它虚拟交换机的MAC地址空间的可能性。

虚拟交换机的转发表项是独立配置的，相互不干扰，相互隔离。

PTN交换机中的各种业务的缓存大小是单独配置预留的，即各种业务的缓存是相互隔离的。

各种业务的缓存相互隔离，当某种业务拥塞时，不能任意占有交换机的缓存，只能占有该业务的配置缓存，这种规则就使得各种业务的拥塞不会相互干扰，避免了一种业务的拥塞影响其他业务的正常转发。

在PTN设备中，在5个不同层级上采取了隔离技术，包括PW通道层隔离、LSP通道层隔离、交换资源表隔离、Buffer资源隔离、业务分类隔离，可保障正常使用的各业务报文之间的独立性和安全性。

基于PTN技术原理和实际测试，可进行网络业务安全防护能力分析：

1)PTN的转发层面通过管道技术(Tunnel/PW)，使得各业务流之间完全隔离，不同用户之间的报文无法互通，避免了彼此之间的干扰或侵入。

2)PTN基于端口或子端口接入业务并做透明传输，不对业务自身包含的协议进行处理，可避免从协议层面发起的攻击。

3)PTN的业务报文完全由硬件转发，软件不参与，软件层面的故障不会影响业务。

4)PTN采用独立的管理通道，业务报文无法侵入到管理通道中，确保网元管理与业务配置层面的安全。

5)PTN可能的被攻击点主要在网络边缘(接入侧)和网络传输途中(传输节点)。

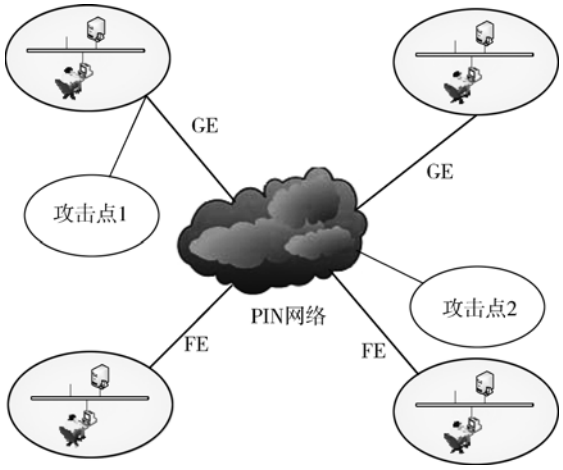

图 3　PTN 安全攻击位置示意图

Fig. 3　Schematic Diagram of the PTN Network Security Attack Position

2.1　攻击点 1(业务接入)分析

1)PTN 基于端口或子端口接入业务并做透明传输，客户侧过来的攻击报文会被直接透传，攻击不到 PTN。

2)PTN 有 MAC 地址黑白名单和 802.1X 认证功能，防止接入点非法接入。

3)PTN 采用管道技术(Tunnel/PW)做隔离能够，也只会影响到该接入点涉及管道的业务，不能侵入 PTN 其它节点的管道业务，包括窃取与篡改信息。

4)PTN 能针对每条业务流做带宽限制，可避免某条业务流恶意冲击其它业务流。

2.2　攻击点 2(网络传输)分析

1)网络传输途中的攻击首先需要在 PTN 中串入监听设备(该项操作难度很高)，这台监听设备很容易被 PTN 的 ARP 机制、OAM 机制、光纤自动发现机制等检测出来，这是第一道防护。

2)串入监听设备后，需要解析 PTN 报文中的 VLAN 信息、LSP 管道信息、内层 PW 隧道信息，很难构造与原网络完全一致的报文。

3)这些网络内部私有信息很难被外界识别，形成第二道防护。

4)之后还需要进一步解析用户报文中的二层、三层等信息后才能看到客户真实的报文，且客户重要的报文还可采用加密措施，形成第三道防护。

3　网络链路抓包分析

由于 PTN 采用 MPLS-TP 协议，内核其实还是 LSP 标签的交换，只是采用了静态 MPLS，转发平面采用了面向连接的方式。由此可见，如果能够通过接入 HUB 的方式，是可以实现抓包、改包等一系列的操作。烽火 PTN 设备镜像端口，抓包结果如下图所示。图中可见，传输的每一个包都可以解析出来，包中的字节可以很容易对应起来，MPLS 标签、PW 标签等信息都可以通过抓包获取。报文的净荷内容 61 850 Sample 也可以很容易的通过分析软件分析出来，那么有针对性的修改报文内容送回传输管道就可以引起故障，甚至保护误动作。

PTN 没有相应的机制，阻止伪装成相同封装的

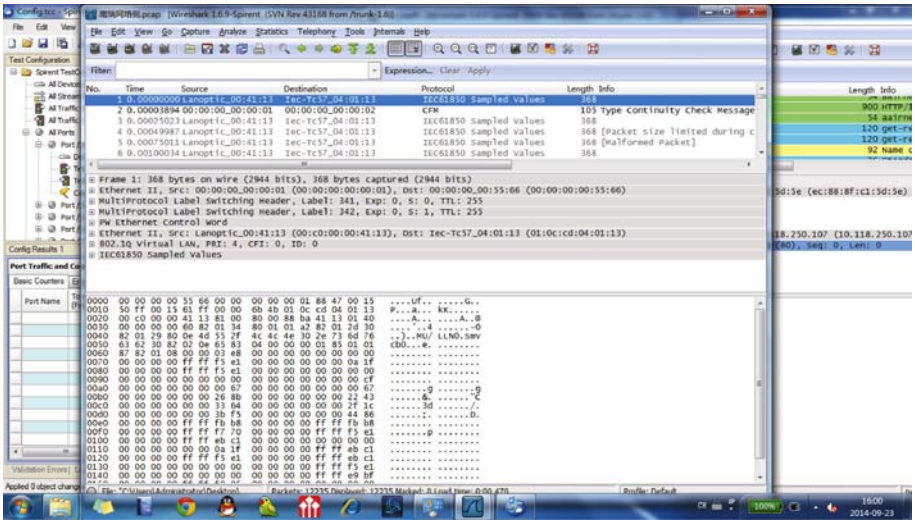

图 4　PTN 链路数据报文抓包解析实例图

Fig. 4　PTN Link Data Packet Capture Analysis Example

包在管道中进行发送和接收；保护装置采用的应用层通信协议是直接建立在链路层之上的，在收到后，会进行CRC校验判断收到的数据包链路上传输无误，也无法判断数据来源的安全性，必须有相应的加密机制才行。但采用软件加密，势必会带来传输延时的损耗，有可能会不满足采样值传输时间的要求，超过保护装置的缓存容限。因此，关于PTN的安全性、业务隔离性还有待研究。

4 PTN承载广域控制保护业务的安全性

广域控制保护系统是通过采集电力系统多点的信息，实现对故障进行快速、可靠、精确的切除，同时分析故障切除对系统安全稳定运行的影响，并采取相应的控制措施，同时实现继电保护和自动控制功能的系统。广域控制保护系统对安全性的要求非常高，既要对通信数据报文进行安全防护，还需要对逻辑通道进行安全隔离。

广域控制保护系统业务承载的数据通信网络常用技术为以太网技术、PTN技术裸光纤组网。由于都是基于以太报文交互，通过普通数据仪表检测裸光纤可以抓取到链路上相关报文(包括业务报文以及相关协议报文)，并能解析出MAC地址、VLAN号、Tunnel号、PW号等基本信息，如果对这些报文进行修改，例如修改VLAN号，会造成业务隔离失效，不正确的数据报文串入其他信道，干扰广域控制保护装置的正常工作。特别如果恶意攻击者篡改报文数据内容，可以影响广域控制保护系统的正常通信数据，造成电网误动、误控制，造成电网事故。

5 结论

通过分析电力通信数据安全防护要求和PTN通信机制。PTN采用标签隔离技术，解决了传统IP网络的安全访问问题，但仍属于逻辑隔离，而非物理隔离，不能满足电力系统二次安全防护要求的电力生产业务专网隔离的要求。广域控制保护业务属于电网生产控制业务不能采用PTN与其他管理业务混合承载。

参考文献：

[1] 饶威，丁坚勇，陶文伟．分组传送网技术在智能电网电力通信中的应用[J]．广东电力，2011，7(11)：54-57.
RAO Wei，DING Jianyong，TAO Wenwei. Application of Network Packet Transmission Technology in Electric Power Communication in Smart Grid [J]. Guangdong Electric Power，2011，7(11)：54-57.

[2] 宋旅宁．电力通信网中对于PTN技术的应用探讨[J]．信息通信，2014，9(17)：201-202.
SONG Lüning. Discussion on The Electric Power Communications Network for The Application of PTN Technology [J]. Communication，2014，9(17)：201-202.

[3] 刘岩，汪强，徐小兰，等．PTN技术在智能电网的应用[J]．现代电信科技，2013，5(7)：56-58.
LIU Yan，WANG Qiang，XU Xiaolan，et. al. Application of PTN Technology in Smart Grid [J]. Modern Science & Technology of Telecommunications，2013，5(7)：56-58.

[4] 蒋凯明．PTN技术在电力通信中的应用[J]．河北企业，2013，10(28)：89-90.
JIANG Kaiming. The Application of PTN Technology in Electric Power Communication[J]. Hebei Company in Hebei，2013，10(28)：89-90.

[5] 钟成．电力通信SDH/MSTP网络向PTN网络演进的策略研究[J]．电力信息与通信技术，2013，11(12)：27-33.
ZHONG Cheng. Discussion on Network Evolution Strategies From SDH/MSTP to PTN for Power Communication [J]. Electric Power Information and Communication Technology，2013，11(12)：27-33.

[6] 杜洁，李洋．PTN通信系统的通道隔离度分析[J]．云南电力技术，2013，2(6)：54-59.
DU Jie，LI Yang. Reliability Analysis [J]. Yunnan Electric Power Technology Isolated PTN Communication System Channel，2013，2(6)：54-59.

[7] 薛金，余江，常俊，等．基于PTN技术的配电通信网隔离度评估研究[J]．电力系统保护与控制，2013，8(16)：60-65.
XUE Jin，YU Jiang，CHANG Jun，et al. Research on Isolation Degree for Distribution Communication Network Based on PTN Technology [J]. Power System Protection and Control，2013，8(16)：60-65.

(责任编辑 高春萌)