

电力软交换系统安全隔离技术研究

李炳林, 卜宪德, 郭云飞

(中国电力科学研究院, 江苏 南京 211106)

摘 要: 电路交换向软交换系统演进必须先解决软交换系统的安全问题。基于 P2DRR 模型, 电力系统提出了二次系统的安全防护总体要求。本文在分析电力软交换系统安全风险的基础上, 从系统安全隔离的角度, 利用 MPLS VPN 技术建立软交换系统分组专用网, 并针对与电力其他业务系统网络、其他软交换系统网络、终端接入网络的不同的隔离要求, 分别采用安全隔离装置、会话边缘控制网关、边缘通信代理技术提出了相应的网络隔离方案。

关键字: 电力软交换; 安全模型; 网络隔离; VPN; 通信代理

0 引言

随着电网的不断发展, 电力交换系统从传统的语音通信朝着实现视频会议和远程视频监控的高清化、满足协同办公的互动化、体现电力各部门业务流程的个性化、多种业务和媒体流的融合化及不同桌面终端应用的多媒体化方向发展。基于电路的交换系统已无法满足这些新的需求。以软交换为核心技术的下一代交换网络是基于分组交换的网络, 在原有电路交换机的基础上, 将业务功能(业务提供)、控制功能(呼叫和信令控制)和接入功能(中继和用户接入)相分离, 形成软交换网络的应用服务器、控制设备、信令网关和各种接入媒体网关。由于功能的分离, 各种接入媒体网关的设置可以更加灵活, 软交换机的控制能力和管理范围可以很大, 业务的提供可以更加丰富、快捷^[1]。然而, 事物都具有两面性, 软交换在为我们带来便利的同时, 也带来了更加严峻的安全问题。传统电力交换系统的传输采用TDM专线, 用户之间采用面向连接的通道进行通信, 其他用户很难插入偷听与破坏。软交换网络的承载部分采用的是分组网络, 主要以IP网为主, 通信协议和媒体信息主要采用IP数据包的形式进行传送, 软交换网络中接入节点比较多, 用户的接入方式和接入地点都非常灵活, 相对传统网络来说, 软交换的网络环境更为复杂, 势必将面临着更加突出的安全问题^[2-3]。

国家电网公司将在“十二五”通信规划中明确了电话交换网主要采用电路交换技术体制, 同时积极跟踪、研究和试点应用软交换技术。在充分发挥现有设备和系统作用的基础上, 按照渐进、共存、互补的原则逐步由电路交换向软交换演进^[4]。但由于电力调度在电力生产运行中的特殊作用, 任何一条错误的调度指令或短暂故障, 将直接影响电网的稳定运行, 必须解决好电力软交换系统的安全问题, 否则将阻碍软交换在电力中的推广应用。

1 电力软交换系统安全威胁

为保证电网的稳定运行, 电力软交换系统必须确保系统中信息的完整性、保密性、可用性和及时性^[5]。电力软交换系统一个复杂的系统, 无论是软硬件系统、通信协议、数据信息管理、业务系统交互, 都是复杂的工程。这就不可避免地会有设计不完善的地方, 安全隐患是必然存在的^[6], 它的主要安全隐患表现在以下几个方面。

1.1 网络安全

传统的电路交换系统按国、网、省、地、市建成五级交换网络, 各级都有各自的交换中心, 每个用户独占一条链路进行通话, 资源有保证。软交换系统采用IP分组网作为传输承载, 网络层级减少, 通信信道不为软交换系统专用, 网络中承载的业务种类多, 容易遭到外来恶意攻击破坏。由于IP分组网尽力而为的传输特性, 当其他同业务系统或网络病毒占用大量带宽, 会导致软交换系统访问速度很慢甚至无法访问时, 无法为用户提供任何服务。

1.2 设备安全

网络上的设备一般都是常年不间断地运行，难免会出现硬件故障，这些故障可以造成数据的丢失，通信的中断，从而对用户服务造成损害。如果是某些核心的设备出现故障，则有可能导致整个网络的瘫痪。

1.3 软件系统安全

软交换系统是构建在特定的操作系统之上的。通用的操作系统如 Windows、Unix、Linux 等本身存在大量的安全漏洞，攻击者可利用漏洞对系统发起攻击。另外，各种通信软件在实现的时候不一定非常完善，可能存在这样或那样的漏洞，给黑客以可乘之机。应用软件在使用过程中，部分数据往往被用户有意或无意地删除，造成不完整。不同应用软件之间可能出现相互冲突，在更新时存在文件互相覆盖或改写，从而引起一些不安全的因素。另外，软件系统因各种原因，更新升级周期短，不同软件间不同版本的不兼容、以及数据库信息的不完整也带来了系统的安全问题。

1.4 协议安全

协议的安全隐患体现在网络中互相通信的协议本身存在的安全方面的不健全，以及协议实现中存在的漏洞问题。协议任本质上也是一种软件系统，因此任设计上不可避免地会存在一些失误。比如：TCP/IP 协议设计就只仅仅建立在研究试验的基础上，没有考虑安全性。黑客可以通过专用工具对网络扫描，掌握有用的信息，探测出网络的缺口，从而进行攻击。另外，IP 地址可以人为地用软件设置，这就形成 IP 地址假冒的欺骗，无法保证来源的真实性。在软交换系统中，包含多种多样的协议，主要的协议包括 H248、SIP、MGCP、H.323、BICC、SIGTRAN 等，正是这些协议促成了网络的互通。每种协议都存在网络服务中断和遭受攻击的隐患。

1.5 信息安全

信息安全主要包括软交换与终端之间信令消息的安全、用户之间媒体信息的安全以及用户私有信息(包括用户名、密码等)的安全。由于软交换网络采用开放的 IP 网络传输信息，在网络上传输的数据就很容易被监听，如果软交换与终端之间的信令消息被监听，有可能导致终端用户私有信息的泄漏，导致监听者可以利用监听到的信息伪造成合法用户接入网络；如果用户之间媒体信息被恶意监听，将导致用户私密信息的泄漏。

2 电力软交换系统安全模型

电力软交换系统是承载在IP分组数据网中，系统的安全要求网络中的数据与资源必须实现五个基本目标：

(1) 可用性：可用性就是指网络服务对用户而言必须是可用的，也就是确保网络节点在受到各种网络攻击时仍然能够提供相应的服务。

(2) 保密性：保密性保证相关信息不泄露给未授权的用户或实体。

(3) 完整性：完整性保证信息在传输的过程中没有被非法用户增加、删除与修改，保证非法用户无法伪造数据。

(4) 真实性：真实性保证和一个网络节点通信的对端就是真正的通信对端，要鉴别通信对端的身份。防止假冒节点获得未被授权的资源和敏感信息。

(5) 不可否认性：不可否认性保证一个节点不能否认其发送出去的信息。这样就能保证一个网络节点不能抵赖它以前的行为。

“电力二次系统安全防护总体方案”采取的通信网络安全模型P2DRR如图1所示。

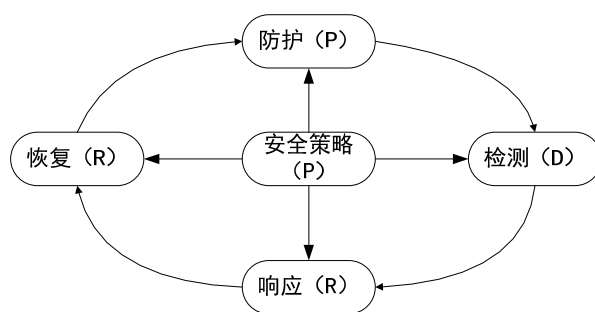


图1 P2DRR安全模型

P2DRR是Policy(策略)、Protection(防护)、Detection(检测)、Response(响应)和Recovery(恢复)的缩写。防护、检测、响应、恢复组成了一个“完整的、动态”的安全循环，在安全策略的整体指导下保证系统的安全。

Policy(安全策略): 安全策略是安全模型的核心，所有的防护、检测、响应、恢复都是依据安全策略实施的，是安全防护的方向和支持手段。策略体系的建立包括：安全策略的制订、评估执行等。

Protection(防护): 防护是预先阻止攻击可能发生的条件产生，让攻击者无法顺利地入侵，防护可以减少大多数的入侵事件。主要有隔离、防火墙、加密、认证、缺陷扫描等方法。

Detection(检测): 检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具，通过不断地检测和监控网络和系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。检测的对象应该主要针对构成安全风险的两个部分：系统自身的脆弱性及外部威胁。

Response(响应): 紧急响应在安全系统中占有最紧要的地位，是解决安全潜在性最有效的办法。就是要解决紧急响应和异常处理问题。要解决好紧急响应问题，就要制订好紧急响应的方案，做好紧急响应方案中的一切准备工作。

Recovery(恢复): 恢复是事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。一般可通过系统升级、软件升级、打补丁、除去后门等措施修补系统缺陷。

在此安全模型下，制定了电力二次系统安全防护的总体方案^[7]：

安全分区：根据系统中业务的重要性的对一次系统的影响程度进行分区，所有系统都必须置于相应的安全区内；对实时控制系统等关键业务采用认证、加密等技术实施重点保护。

网络专用：建立调度专用数据网络，实现与其他数据网络物理隔离。并以技术手段在专网上形成多个相互逻辑隔离的子网，以保障上下级安全区的纵向互联仅在相同安全区进行，避免安全区纵向交叉。

横向隔离：采用不同强度的安全隔离设备使各安全区中的业务系统得到有效保护，关键是将实时监控系统与办公自动化系统等实行有效安全隔离，隔离强度应接近或达到物理隔离。

纵向认证：采用认证、加密、访问控制等手段实现数据的远方安全传输以及纵向边界的安全防护。

3 电力软交换系统安全隔离技术

电力软交换系统设备主要包括控制层的软交换设备和信令网关，接入层中的各种媒体网关，包括中继媒体网关、综合接入媒体网关、媒体服务器、综合接入设备 IAD 和各种智能终端、业务层的应用服务器等。其网络结构如图 2 所示。

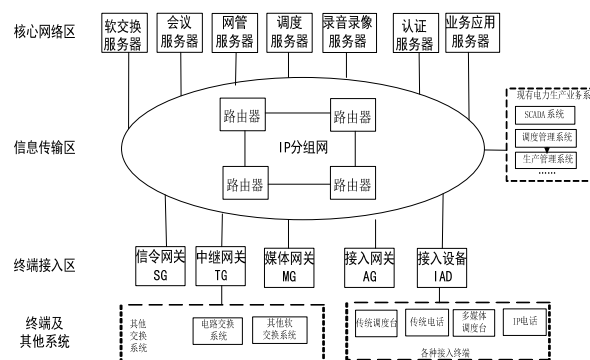


图2 电力软交换系统网络结构

电力软交换系统网络可分为四个部分，第一部分为核心网络区，包括软交换服务器、调度服务器、网管服务器、应用服务器等，为系统的核心设备，任一服务器发生故障，会导致系统无法提供相应的服务，一般可集中部署在中心机房。第二部分为信息传输区，主要由路由器、交换机等网络设备组成，共同组成IP分组网络。第三部分为系统接入区，包括各类网关和接入设备，实现软交换网络与其他交换网络、电力其他业务系统的互联、各种业务终端的接入，一般分散部署在系统的边界。第四部分为业务终端及其他第三方系统。系统中一、二、三部分构成了电力软交换的核心系统。电力软交换系统的安全就是保证核心系统中的关键设备以及设备间通信网络的安全。

在P2DRR安全模型中，有效的防护措施是安全的基础。有效的电力软交换系统专网专用及与外界隔离方案可大大降低攻击、入侵、破坏等安全事故发生概率。电力软交换系统与外界的连接主要分为三类，一类是与电力其他生产、运行业务系统的连接；一类是与电路交换、其他软交换系统的互联；还有一类是与业务终端的互联，提供软交换系统功能。每种连接要求交换的信息类型不同，可采取不同的隔离措施。

3.1 VPN 专网技术

电力软交换的核心设备和网关设备是通过IP分组网连接在一起的，为提供服务方便，各种网关设备都是分散部署。在公用分组网中，通过VPN（Virtual Private Network）可以模拟点对点专用链路的方式，建立一个临时、安全的连接，达到与专用网络相类似的安全性能，可以对不同用户间、用户与核心网络间、不同业务网之间的路由信息进行隔离。实现VPN主要有两类技术：通过隧道协议实现和用多协议标记交换（MPLS）的标记交换路径实现。所谓隧道，实质上是一种封装，即将一种协议（协议X）封装在另一种协议（协议Y）中传输，从而实现协议X对公用网络的透明性。这里协议X称为被封装协议，协议Y称为封装协议。常用的隧道协议有IPSec。IPSec利用认证协议AH，安全加载封装ESP和密钥交换协议IKE，实现数据传输的保密性、完整性、身份认证以及重播检测。利用IPSec实现VPN，需要为每个用户建立一个构建虚拟路由器VR（Virtual Router），VR之间通过IPSec隧道互联，在构建大型网络时，需要建立的隧道数和节点数的平方成正比。

MPLS是基于标记的IP路由选择方法。这些标记可以被用来代表逐跳式或者显式路由，并指明服务质量（QoS）、虚拟专网以及影响一种特定类型的流量在网络上的传输方式等各类信息。MPLS采用简化了的技术，来完成第三层和第二层的转换。它可以提供每个IP数据包一个标记，将之与IP数据包封装于新的MPLS数据包中，由此决定IP数据包的传输路径以及优先顺序。而与MPLS兼容的路由器会在将IP数据包按相应路径转发之前仅读取该MPLS数据包的包头标记，无须再去读取每个IP数据包中的IP地址位等信息，因此数据包的交换转发速度大大加快。MPLS实现了VPN间路由隔离、传输核心信息隐藏、不同VPN之间用户无法相互攻击等功能，有效保障了网络安全。

对于电力软交换系统，可以采用MPLS VPN技术，构建相对独立的VPN网络。MPLS VPN网络主要由CE、PE和P等3部分组成：CE（Custom Edge Router，用户网络边缘路由器）直接与业务终端或第三方系统网络相连，它“感知”不到VPN的存在；PE（Provider Edge Router，骨干网边缘路由器）设备与用户的CE直

接相连，负责VPN业务接入；P（Provider Router，骨干网核心路由器）负责快速转发数据，不与CE直接相连。利用MPLS VPN构建软交换系统网络如图3所示。

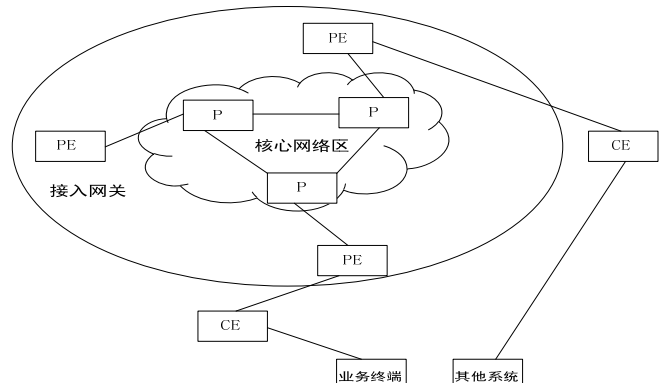


图3 MPLS VPN软交换网络

3.2 采用隔离装置隔离技术

电力其他生产业务系统如 SCADA 系统、调度生产系统、信息管理系统等，与电力软交换系统之间交互的信息主要包括电力网络监控数据、设备信息、视频信息、地理信息等。这些电力业务系统有些处于生产控制大区，有些处于管理信息大区，系统可参照“电力二次系统安全防护总体方案”，采用正反向隔离装置进行横向隔离。

3.3 会话边缘控制网关技术

电力软交换系统需要与原基于电路的交换系统、以及其他的软交换系统进行互联，系统间互联互通需要采用相应的协议。软交换系统中采用的信令协议主要包含H.323、SIP、H.248、MGCP、SIGTRAN等几种。这些信令信息的交互需要很高的可靠性和快速的接续速度，同时也必须是双向的，无法采用电力系统中正、反向隔离装置。为解决传输协议的安全、异质网络互联问题、NAT穿越问题等，可通过会话边缘控制器(SBC，Session Border Control)进行网络隔离，系统间所有信令和媒体流都需要经SBC转接。SBC主要由信令代理(Signaling Proxy)和媒体代理(Media Proxy)这两个逻辑功能实体组成。当终端向软交换注册时，SBC会给每个终端分配一个信令代理端口，所有消息都会经过这个端口转发给软交换，同时SBC会用自身地址和这个端口来替换消息体中终端的地址信息。因此在软交换系统中维护的用户地址信息，实际上是SBC的地址和SBC分配给终端的端口号。呼叫建立时，SBC会给终端分配一对RTP代理端口(收、发)，并以此替换通信消息中对RTP接收端口的描述，再转发给软交换。即：每个终端收到的对方RTP信息实际上是SBC分配的RTP代理端口号，RTP流经SBC在两个终端间建立连接。因此，不同系统中的终端经SBC实现了有效的隔离。

SBC一般放置在各自网络边缘，软交换系统将收敛于各自的SBC，从这里连接到网络中的核心设备。如图4，软交换系统A和B通过SBC进行隔离连接。SBC主要完成的功能包括：

安全保护：SBC作为系统的最外层，能根据特定协议进行报文过滤，阻断未经允许的协议对软交换系统的访问，隔离网络层攻击。

网络管理：SBC可以监视所有经过的媒体流，提供实时的QoS报告，衡量端到端的抖动、时延和丢包；还可以代替边缘路由器添加QoS标记，避免其被用户任意篡改。

协议修复及互通：SBC可以修复非标准终端发来的协议消息，将其转换为标准形式；异构网络间的协议互通和转换也可以在网络边缘处由SBC来完成。

NAT/Firewall穿越：SBC可以被看作软交换系统的代理，通过自己维护路由器、防火墙中的IP地址/端口与实际终端设备的对应关系建立呼叫连接，所有信令和媒体流经过SBC的协调和修改，可以在系统侧及用户侧正确地传输。

3.4 通信代理技术

对于软交换系统中各种业务终端的接入,可采用通信代理的方式来进行有效的隔离。使用代理技术,终端与软交换、终端与终端之间的通信都必须通过代理来完成。采用通信代理的电力软交换系统结构如图4。

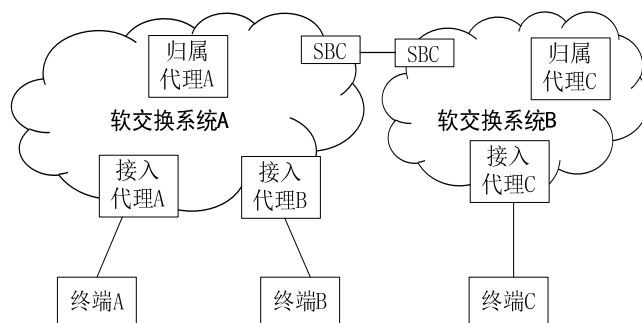


图4 采用通信代理的电力软交换系统结构

在软交换系统中引入两种代理,归属代理和接入代理。每个软交换系统都有一个归属代理和多个接入代理,接入代理部署在系统的边缘,负责终端的接入。为终端分配两个基本属性:呼叫号码(系统中唯一标识)和通信IP地址。呼叫号码由归属代理统一分配。通信IP地址由接入代理管理,不同的接入代理可以采用不同的IP地址段,组成不同的VPN网。这样,软交换系统核心网络可与终端外部网络有效隔离。终端间的通信过程如下:

1) 接入代理通过代理通告报文广播其存在,终端也通过代理请求报文,可有选择的向所属的接入代理请求代理通告报文。

2) 终端收悉这些代理通告后,通过交换其随带身份标识向接入代理发送注册请求信息,注册请求转发到归属代理处理。

3) 归属代理判断是否是自己所属终端,如果是,则作出响应,将结果发送到接入代理;若不是,则将请求信息转到其他的软交换系统的归属代理处理。

4) 接入代理获得注册响应认可后,允许终端注册系统,并为终端分配一个通信地址,并将终端通信地址告知归属代理。归属代理登记完成终端呼叫号码、终端归属代理、终端通信地址的对应关系表。

5) 终端A与终端B通信时,终端A发往B的数据包被其接入代理A接收,代理A利用隧道技术封装该数据包,并将封装后的数据包发送到归属代理,由归属代理转送到终端B所属的接入代理B,由代理B接收,解除封装,并最终传送到终端B。

6) 终端A与终端B之间的通信,采用的都是终端本身唯一标识地址,即呼叫号码。通信地址只用于终端与接入代理之间通信。

4 结束语

软交换系统在公网已经获得了广泛成熟的应用,但由于电力系统特殊的安全需求,现有基于电路的调度交换网能否平稳向软交换网演进,必须解决好软交换系统的安全问题。本文仅从网络隔离的角度阐述了几种安全措施,但网络的安全是全方位的,需根据“电力二次系统安全防护总体方案”要求,从网络分层、边界隔离、信息加密、终端认证、运行管理等方面提供全方位的安全防护措施。

参考文献:

- [1] 赵慧玲.网络交换技术的发展[J].电传技求,2006(1):38-41.
- [2] 李海花.软交换网络中的安全机制[J].电信网技术,2003(12):10-13.
- [3] 姜华. NGN 组网的安全性分析与安全策略[J].现代电信科技,2003(12):6-8.
- [4] 王庆铸,连纪文,黄旭峰. 电力“十二五”语音交换网的演进[J].电力系统通信,2011(5):77-81.
- [5] 丁道齐. ICS/MCS 安全性类型和面临的挑战[J].电力系统通信,2010(2):1-7.

[6] 杨旺功,叶茂,陈继努,等.NGN安全隐患及防御措施研究[J].网络安全技术与应用,2007(9):47-49.

[7] 国家电监会.电监安全[2006]34号 电力二次系统安全防护总体方案[Z].

作者简介:

李炳林(1970-),男,通信作者,硕士,高级工程师,主要研究方向:电力系统自动化及其通信技术,E-mail: libl2000@sina.com;

卜宪德(1978-),男,硕士,工程师,主要研究方向:电力系统通信;

郭云飞(1976-),男,硕士,工程师,主要研究为:电力系统通信。