



专题:业务平台安全

短信平台安全域改造研究初探

黄斯炜¹, 李 洪²

(1. 中国电信股份有限公司湖南分公司网络运行维护部 长沙 410011;

2. 中国电信集团公司网络运行维护事业部 北京 100032)

摘 要: 以对信息安全的保护为关注目标,在信息系统安全保护的技术层面上,对安全域划分和边界整合改造进行深入分析与探讨。选取中国电信某省分公司的短信平台为典型案例,对其包含的短信中心、互通网关等系统进行安全域改造研究分析,研究结论可以为电信运营商其他业务平台的信息安全保护、业务连续性等方面提供良好的指导。

关键词: 短信;信息安全;安全域

doi: 10.3969/j.issn.1000-0801.2013.08.010

Preliminary Study on the Security Domain Transformation of SMS Platform

Huang Siwei¹, Li Hong²

(1. Department of Network Operation & Maintenance, Hunan Branch of China Telecom Co., Ltd., Changsha 410011, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: Taking the protection of information security as the focus, the technical level in the security protection of information system, the partition of security domain and boundary integration transformation were analyzed and discussed. China Telecom SMS platform was selected as a typical case, and the security domain transformation of systems as message counters and gateways were researched and analyzed. The conclusion could provide good guidance for other service platform of information security, business continuity.

Key words: short message, information security, security domain

1 引言

随着信息技术的发展以及国家政策导向的变化,对信息安全越来越重视,特别是国家4部委联合颁发了《信息安全等级保护管理办法》以及一系列具体等级保护基本要求,对我国信息系统的安全提出了基本要求。根据等级保护管理办法的要求,工业和信息化部也发布了一系列信息安全文件,要求基础电信运营商对网络和系统进行安全保障。中国电信根据工业和信息化部的政策要求,下发《关于

构建中国电信互联网及相关网络安全策略体系及推进相关工作的通知》、《安全域划分与边界整合技术规范》等文件明确网络安全防护边界,进行出口统一防护。根据上述一系列规定,对中国电信某省分公司的短信平台安全域改造和划分进行相关研究。

2 安全域改造分析研究

2.1 整体思路

将大型复杂系统的安全问题,变化为小区域简单系统



的安全保护问题,并在保证所有系统与网络对各种互联需求有效提供的前提下,对安全域的边界进行合理有效的整合,对区域内的系统与网络接口进行合理有效的整理和合并,缩减接口数量,提高区域内系统与网络接口的规范性,有效实现大规模复杂系统的安全等级保护。

2.2 研究内容

(1)安全域划分

安全域划分以“同构性简化”为原则,对复杂的大型网络进行简化后设计保护体系,实现有效的安全管理,具体有以下3个原则。

- 业务保障原则:保障网络承载业务的正常、高效运行。
- 结构简化原则:简单的网络结构便于设计防护体系。
- 立体协防原则:访问控制、链路冗余、身份鉴别、内容检测、检测审计等各种安全功能实现安全域防护。

(2)安全域内加固

在进行安全域划分与边界整合之后,对所有安全域内的重要设备进行安全加固,因为各安全域内使用的设备具有不同的互联需求,其所面临的威胁也不尽相同,因此其安全需求也存在很大差异。安全域内加固主要考虑生产服务器、维护终端、第三方维护控制、合作伙伴连接防护、互联网安全防护。

(3)边界安全和区域安全

区域边界安全:安全域的保护,其区域边界安全是最基础的保护措施,通过对区域边界的控制能够保护安全域不会受到来自其他区域的安全威胁。

重点区域安全:通过在安全域内部进行审计、清理、监视、测量等技术手段,完成安全域内安全事件的应急响应和清除。安全域的区域安全以安全状况的监控为主要手段,通过监控本安全域内部的安全事件并进行及时的应急响应和清除,是安全域的关键安全处置手段。

2.3 研究的重点与难点

2.3.1 安全域改造难点

进行安全域改造过程,需要大量的调查研究工作,需要针对每个系统进行相应的难点分析,主要从以下几个难点:

- 对业务平台的防护目标进行分析,分析各种服务及数据流和活动,识别其各要素,分析在网络、系统、

应用、数据层的承载情况以及存在的重点等;

- 业务平台防护目标的安全风险分析,主要识别数据、应用、系统、网络等层次的安全威胁、脆弱性情况,分析其可能性及受到侵害的影响等;
- 业务平台边界整合的业务关联分析;
- 业务平台结构变更的业务关联分析;
- 确定防护目标的安全需求分析,以其承载业务为出发点,分析各业务的安全防护要求,如服务域(关注可用性)、维护域、计算域等各域的安全要求;从其自身的安全威胁、脆弱性情况及安全发展趋势走向进行分析、总结,并提出改进需求;
- 业务平台的合规性分析;
- 业务平台的综合分析,根据以上内容综合分析出全面的信息安全风险。

2.3.2 安全域改造的重点

对于安全域的改造,将以下几个方面的分析内容作为改造过程中的重点:

- 安全域改造实施的原则分析;
- 安全域改造实施内容的流程、顺序分析;
- 安全域改造实施技术的标准化、规范化、流程化等内容分析;
- 安全域改造实施的业务保障原则;
- 安全域改造实施业务平台的信息安全性保障分析;
- 安全域改造实施人员保障分析;
- 安全域实施改造后的业务服务状态、安全性、连续性、维护、审计等测试。

3 安全域改造实施方案研究

3.1 研究现状

中国电信某省分公司 CDMA 网的短信中心分为 3 套,均独立成网;各平台交换机与短信平台汇聚交换机互联,上行设备分别与 DCN、互联网以及其他运营商互连互通,满足业务的需求,网络拓扑结构如图 1 所示。

短信平台涵盖网元较多,除传统的短信中心、短信网关外,还包括 MSP、短信综合应用平台,外连彩信、WAP 网关、ISMP、ISAG,整个拓扑结构较为复杂。

3.2 风险分析

短信平台系统在设计建设之初已经考虑了系统相关安全需求,建立了比较完善的安全机制,但通过对短信平台系统的实地调研与分析,目前存在以下安全隐患:

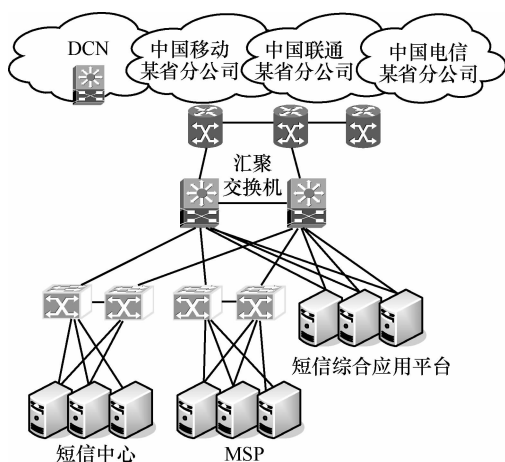


图1 短信平台整体网络结构

- 短信平台各功能模块没有明显的安全域划分,没有有效的安全保护措施;
- 短信平台整个平台外界的相连出口众多,边界没有统一出口,整个网络显得比较复杂与无序;
- 短信平台各设备没有进行安全配置,各设备仅根据实际情况进行相应的配置等操作,未根据中国电信集团的安全配置规范进行配置;
- 各业务系统间的互联互通缺乏统一的控制规范,安全问题容易扩散;
- 平台缺乏有效的安全防护机制,针对攻击流量平台无监测功能,不具备有效的防御措施;维护区域具有审计功能的安全接入网关跳板设备;网络、系统等之间缺少有效的访问控制等措施;对入侵防范等措施有一定的缺失;整个短信平台系统的防病毒防范机制缺失;
- 内网缺少专用补丁服务器,各服务器无法及时更新补丁,针对所有设备操作无专用的日志服务器进行记录和审核。

3.3 短信平台安全域改造目标

安全域的划分就是做好各区域的安全边界,通过资源位置进行划分的目标是将相同网络安全等级的资源,依照对企业的重要性、其面临的外来攻击风险、自身内在的运行风险的不同,合理地划分成多个网络安全区域。划分的依据是将相同网络安全层次内客户端之间的连接控制在同一安全域内,尽量消除不同安全层次之间的联系,实施逻辑隔离或物理隔离。

完成划分网络安全域,是做好系统安全保护基础的第

一步。因为通过安全域划分可以确定网络边界,形成简洁、清晰、稳定的组网架构,实现各系统之间严格的访问控制安全互联,可解决系统的安全问题,有效地实现各网络之间和支撑系统之间的安全隔离和访问控制,达到“化复杂为简单、尽在掌控”的目的。安全域的划分加强了网络的可控性,可以有效地防止渗透攻击。针对业务,划分成以下几个区域,网络目标如图2所示。

(1) 交互网络域

由连接具有相同安全等级的维护域、计算域和服务域的网络设备以及网络拓扑组成。作为安全子域以及承载网的统一接口区域,一般分为专线接入区、互联网接入区和内网接入区。网络域通常包括交换机、路由器、入侵防护、防火墙、入侵检测等设备,是安全域的承载子域。

- 专线接入区主要指 VPN 或者专线网络接入 IP 承载网的逻辑接入分区;
- 互联网接入区主要指上联互联网的逻辑接入分区;
- 内网接入区主要指直连到公司内部网络(如 DCN 等)的逻辑接入分区。

(2) 计算域

计算域是指在安全域范围内进行存储、传输、处理业务数据的计算机或集群组成的区域,如磁盘阵列、数据库服务器等。

(3) 服务域

服务域由支撑业务运营的基础组件和提供安全服务管理控制组件组成,包括对内服务区和对外服务区。

(4) 维护管理域

维护管理域由能访问同类数据或进行业务处理、业务维护的维护终端组成。维护域可根据用户维护终端所在的不同地理位置,分为远程维护区和本地维护区;可根据不同的维护用户主体,分为第三方维护区和局方维护区。

而维护域的安全需求,建议以限制权限、加强认证和审计以及严格遵守安全配置标准的技术手段为主,同时使用安全防护工具,如口令管理等保护措施、部署防病毒系统。此外,还需要加强对终端的安全管理,逐步实现终端配置标准化,从软件、硬件平台、用户 ID、管理工具、服务水平及系统的建立和使用等方面实现终端防护的统一管理和安全监控。

3.4 改造实施思路

短信平台改造从步骤上分为以下几步。

- (1) 增加汇聚交换机、路由器、防火墙、IPS 等安全防护

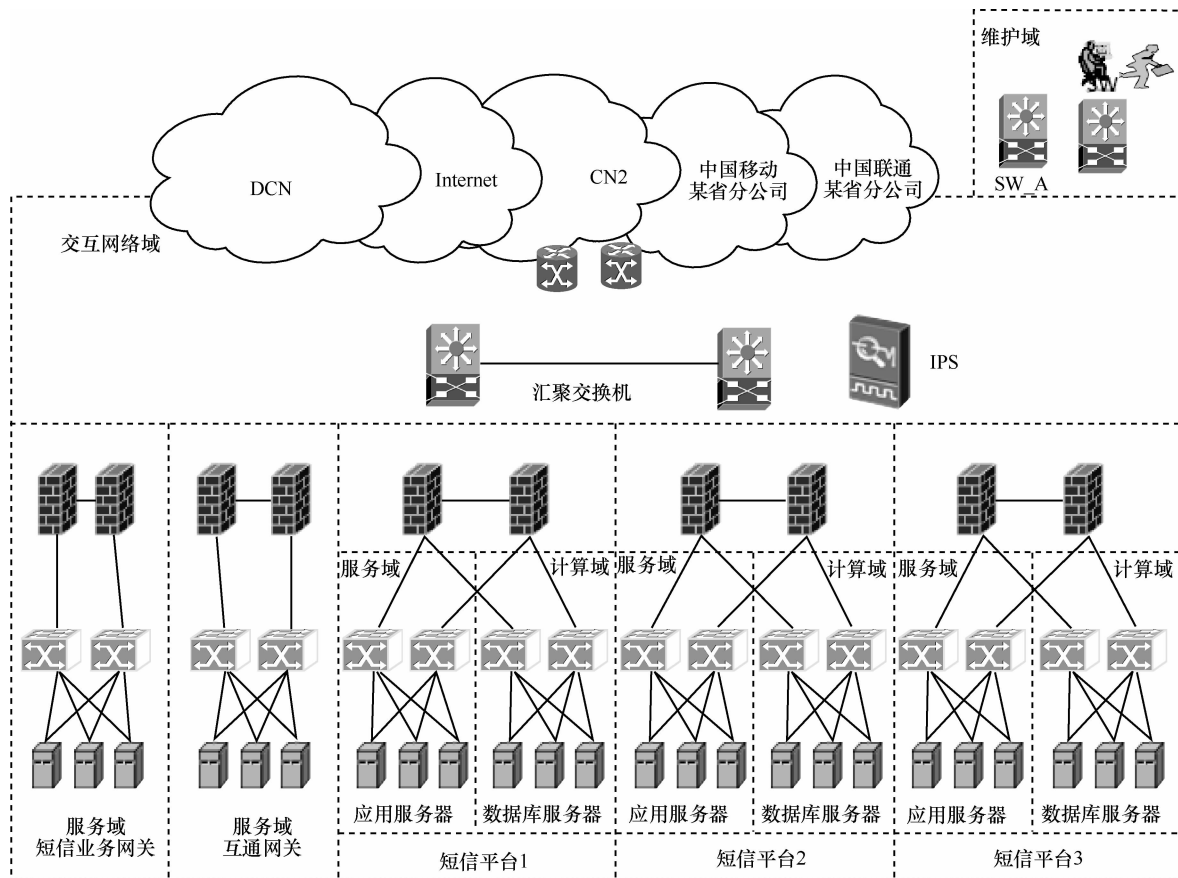


图2 短信平台目标网络

产品,通过设备将安全域的边界统一;将增加的汇聚交换机分别与 DCN、Internet、CN2 设备互联,与中国移动某省分公司、中国联通某省分公司、中国电信某省分公司通过 2 Mbit/s 链路与原 Cisco 3845 路由器互联,IPS 则根据业务需求进行部署;通过防火墙与交换机的整合,形成各安全域边界的统一,网络拓扑如图 3 所示。

安全策略与防护手段,达到安全域要求。

4 安全域改造实施内容

根据安全域划分的结果,按照多层、深度防护的原则,安全域策略的实现从边界防护策略和内部防护策略两个方面入手,采用防火墙安全策略、路由器(或其他网络互联设备)的 ACL(访问控制列表)策略,实现安全域的边界、安全域内部的访问、通信控制。

4.1 交互网络域防护策略

4.1.1 互联网接入区防护策略

(1) 边界防护策略

对于安全域改造,其安全策略的实施是一个重要的内容,针对边界的防护策略有以下内容:部署并优化防火墙策略,优化出口防火墙的访问控制策略,只允许特定的业务数据流通过防火墙,通信流控制要细化到通信的 IP 地址和服务端口,并且除允许的业务通信外,严格禁止其他通信。

(2) 内部防护策略

网络域划分过后,其网络域的安全策略是一个重要的

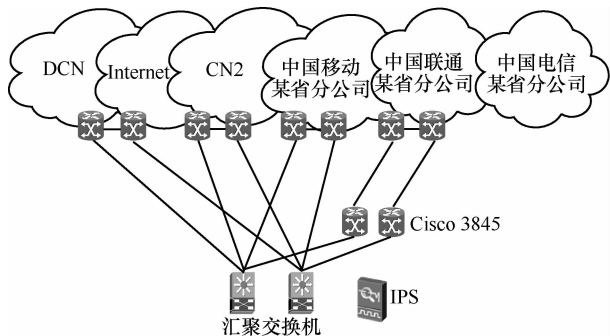


图3 短信平台目标网络部署一

(2) 部署防火墙并将业务系统割接至汇聚交换机,划分以下安全域,具体网络变更如图 4 所示。

(3) 调整各安全域的服务器与网络设备,部署相应的

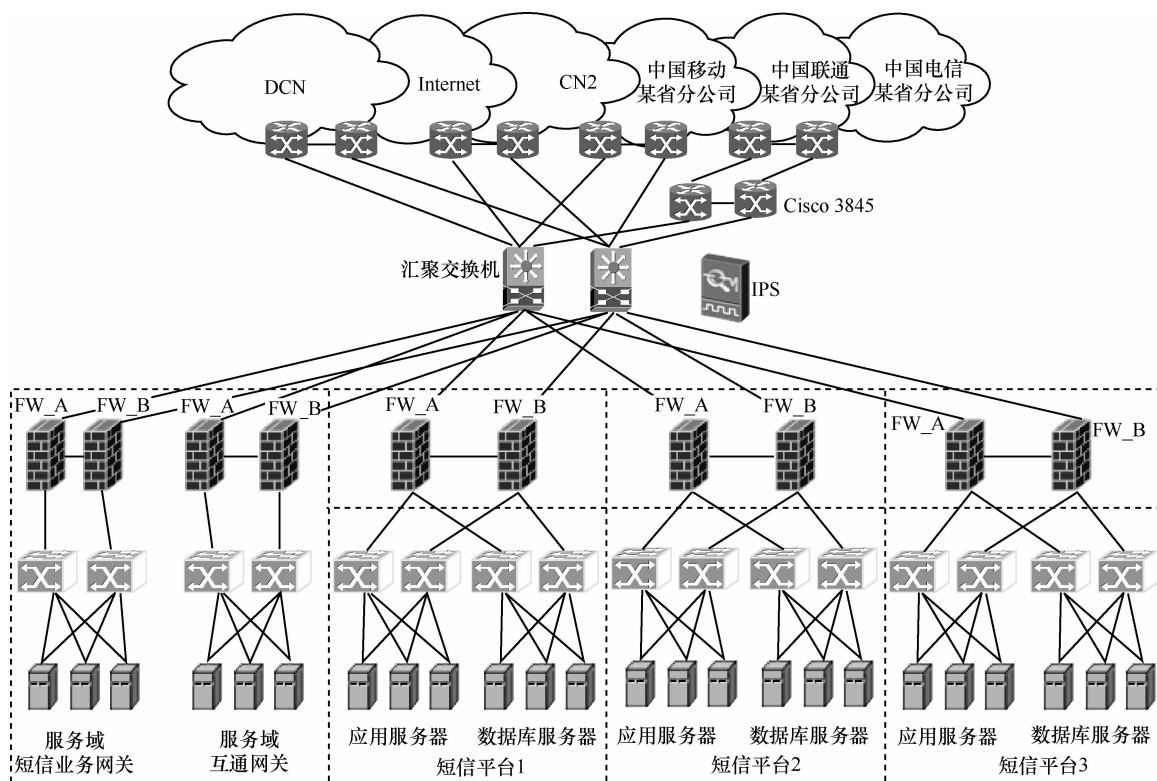


图 4 短信平台目标网络部署二

实施内容。针对区域的安全防护,除了边界保护策略外,也要考虑内部防护策略,内部保护的重点与边界有所不同,其内部防护策略主要有以下 3 方面。

部署日志审计系统:对所有核心路由器、交换设备、业务系统、数据库系统等日志进行统一集中审计分析,审计记录应包含网络系统中的网络设备流量、运行状况等,而事件审计记录应包括事件发生的日期和时间、事件类型、用户、事件成功情况以及其他与审计相关的情况。

部署行为审计系统:对所有核心路由器、交换设备、业务系统、数据库系统等管理员用户的管理操作行为进行记录。

对路由器、防火墙等网络设备进行安全加固服务,包括配置合理的访问策略,严格控制对设备的访问;对管理员登录地址进行限制,包括在待登录的目标网络设备中对用户的源 IP 地址进行设置,仅允许合法的 IP 地址登录、在用户端与目标设备通信之间的网络设备上设置相应的访问控制;启用网络登录链接超时功能,用户登录一段时间后未进行操作,将自动中断此用户的连接;启用登录次数

限制,通常设为 3~5 次,在尝试给定次数登录都未成功的情况下,将直接中止连接。

4.1.2 内网接入区防护策略

(1) 边界防护策略

针对内网接入区的边界保护策略与互联网接入区的防护策略基本类似,性质上都是边界防护,其防护策略有以下举措。

- 边界调整:将各业务系统边界调整为统一出口,并进行集中防护。
- 边界路由器策略优化:在边界路由器上启用 ACL 功能,对病毒蠕虫常用端口进行过滤。
- 防火墙策略优化:优化出口防火墙的访问控制策略,只允许特定的管理维护数据流通过防火墙,通信流控制要细化到通信的 IP 地址和服务端口,并且除允许的业务通信外,严格禁止其他通信。

(2) 内部防护策略

内网接入区的防护策略与互联网接入区的内部防护策略基本一致,安全防护手段相似,因为虽然区域不同,但在安全要求上基本一致,具体包括如下 3 个方面。



部署日志审计系统:对所有核心路由器、交换设备、业务系统、数据库系统等日志进行统一集中审计分析,审计记录应包含网络系统中的网络设备流量、运行状况等,其事件审计记录应该包括事件发生的日期和时间、事件类型、用户、事件成功情况以及其他与审计相关的情况。

部署行为审计系统:对所有核心路由器、交换设备、业务系统、数据库系统等管理员用户的管理操作行为进行记录。

对路由器、防火墙等网络设备进行安全加固服务,包括:应及时安装各种网络设备的补丁或升级程序;配置合理的访问策略,严格控制对设备的访问;对管理员登录地址进行限制,包括在待登录的目标网络设备中对用户的源 IP 地址进行设置,仅允许合法的 IP 地址登录、在用户端与目标设备通信之间的网络设备上设置相应的访问控制;启用网络登录连接超时功能,用户登录一段时间后未进行操作,将自动中断此用户的连接;在网络设备中设置登录失败处理机制,具体包括结束会话、停用账号、记录日志等;启用登录次数限制,通常设为 3~5 次,在尝试给定次数登录都未成功的情况下,将直接中止连接。

4.2 业务域防护策略

4.2.1 边界防护策略

业务域是保护的一个重点,因为提供的业务功能是在业务域的服务器上承载,如何保护业务域是本次研究的重点。根据业务域的特性,如何保护业务域的各种业务服务是策略保护的导向,具体策略如下:

- 合理划分 VLAN,对计算域、服务域、维护域通过 VLAN 进行隔离,只允许合法数据流通过;
- IP 地址、MAC 地址、交换机端口绑定;
- 对业务域的维护通过统一的边界跳板机(堡垒机)进行统一访问,并记录其操作等信息。

4.2.2 内部防护策略

由于业务域的重要性,其内部防护策略要重点考虑,重点是审计、系统防护策略、防病毒、认证、授权等一系列策略,具体如下。

部署日志审计系统:对所有核心路由器、交换设备、业务系统、数据库系统等系统日志进行统一集中审计分析,审计记录包含系统日志等,其事件审计记录应该包括事件发生的日期和时间、事件类型、用户、事件成功情况以及其他与审计相关的情况。

部署行为审计系统:对所有核心路由器、交换设备、业

务系统、数据库系统等管理员用户的管理操作行为进行记录。

对主机操作系统和数据库系统进行安全加固服务,包括:系统补丁修补、账号口令策略增强、端口服务最小化、启用日志审计功能、启用非法登录的次数限制功能、启用登录连接超时功能。严格进行业务域内部的访问控制,颗粒度达到端口级。通过部署网络防病毒产品,对整个短信平台系统进行防病毒工作。

4.3 系统安全策略部署

针对操作系统,根据国家、工业和信息化部以及中国电信集团的文件要求和业界安全最佳实践,对其进行安全配置加固,介绍如下。

- 关闭多余的系统服务,启动操作系统自带的软件防火墙,配置系统的安全策略,配置防止源路由攻击、防止源 IP 地址欺骗式攻击、SYN flood 保护、禁止重定向设置、防止 ping of death 攻击、禁止 ICMP 广播回应、忽略错误 ICMP 分组;
- 限制了远程登录只能使用 SSH,并且对 SSH 服务进行加固,修改默认的登录端口和能使用 SSH 登录的用户,只有特定的用户才能使用 SSH 登录;
- 删除多余的用户和组,限制有 SU 权限的用户;
- 对系统关键文件增加不可修改属性,防止被误删除或人为破坏;
- 保护系统启动引导配置文件;
- 抵御特洛伊木马病毒的攻击;
- 记录远程登录用户的行为,便于审核用户进行破坏操作。

4.4 网络设备安全加固

针对网络设备,根据国家、工业和信息化部以及中国电信集团的文件要求和业界安全最佳实践,对其进行安全配置加固:关闭或限制可能引起安全问题的服务,如 UDP 和 TCP 服务器、finger、NTP、CDP 服务、proxy ARP、SNMP 服务、HTTP 服务;启用备份和日志服务器;用 IOS 安全机制保护关键设备。

5 结束语

通过一系列的安全域改造研究后,进行安全域的改造实施工作,通过一系列安全防护手段,达到提高业务平台安全性的目的,具体可以达到以下效果,也可以为其他业务平台改造提供参考依据。

(下转第 113 页)

道传播过程中的路径损耗不一样,其传播距离不一样的特性,并结合载波聚合技术中不同频带内非连续载波聚合技术对高低频率进行聚合,以达到 UE 对大带宽的需求,同时运用“高频切换、低频辅助”的协作切换思想,使得 UE 在切换过程中切换中断时延相对降低,并且减小了切换中断概率。通过进一步的仿真得知,UE 的切换中断概率相较于传统的 LTE-Advanced 系统和 LTE-Advanced 中继系统有所降低,并且 UE 的吞吐量也得到了提升。

参考文献

- 1 郑毅,李中年,王亚峰等. LTE-A 系统中继技术的研究. 现代电信科技, 2009(6):45~49
- 2 Lee Y, Zhao J H, Qu H. A combined handover scheme for LTE-Advanced. Proceedings of IEEE ICAC, Seoul, Korea, 2012: 154~157
- 3 3GPP TS 36.300 V11.1.0. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2, 2012
- 4 Lee H K, Son H K, Lee S H. Semisoft handover gain analysis over OFDM-based broadband systems. IEEE Transactions on Vehicular Technology, 2009, 58(3):1443~1453
- 5 Chang J R, Li Y J, Feng S L, *et al.* A fractional soft handover scheme for 3GPP LTE-Advanced system. Proceedings of IEEE International Conference on ICC Workshops 2009, Piscataway, USA, 2009
- 6 Teyeb O, Phan V V, Raaf B, *et al.* Handover framework for relay enhanced LTE networks. Proceedings of IEEE International Conference on ICC Workshops 2009, Dresden, Germany, 2009:14~18
- 7 沈嘉,索士强,全海洋等. 3GPP 长期演进 (LTE) 技术原理与系统设计. 北京:人民邮电出版社, 2010
- 8 封彪. LTE-Advanced 无线中继网络切换算法研究. 北京邮电大学硕士学位论文, 2012, 3
- 9 3GPP TS 36.826 V0.13.0. Evolved Universal Terrestrial Radio Access (E-UTRA); Relay Radio Transmission and Reception, 2012
- 10 3GPP TS 36.942 V10.3.0. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) System Scenarios, 2012

[作者简介]



赵季红, 女, 博士, 西安邮电大学教授, 主要从事新一代无线宽带无线通信技术研究工作。



何炜扬, 男, 西安邮电大学硕士研究生, 主要从事宽带移动通信网的研究工作。



曲桦, 男, 博士, 西安交通大学教授, 主要从事新一代无线宽带无线通信技术研究工作。

(收稿日期 2013-04-25)

(上接第 68 页)

- 管理层: 区域之间维护界面清晰, 谁主管谁负责, 易于分析管理与维护界面。
- 数据层: 增强了数据及应用的安全性; 跨业务系统非授权互访易于监控和管理; 业务系统间的应用访问进行了安全域的隔离, 有效控制数据流, 保护信息安全。
- 系统层: 加强了域内系统的访问安全; 防范了安全域之外的威胁来源; 加强了安全事件的追根溯源。
- 网络层: 各业务域具有清晰、简洁的网络及系统架构; 明确安全域网络出口; 安全问题易控制、处理、

调查; 保证网络与系统间的安全互联; 业务系统间互连互通统一控制规范; 从边界进行安全防护, 从来源进行安全控制。

- 物理层: 边界互联清楚, 接口统一。

做好业务平台的安全域改造工作, 可以更好地保证电信业务平台的安全性, 保证业务正常连续地运行, 提高电信服务水平。中国电信的其他业务平台, 可以参考短信平台安全域改造的研究成果进行安全域改造, 以提高平台的安全性。

(收稿日期: 2013-08-01)