doi:10.3969/j.issn.1000-1247.2018.07.001

企业上云数据安全策略研究

付双胜　罗世雄
湖南省邮电规划设计院有限公司

摘要　先指出数据安全问题是我国企业上云进程中面临的最大障碍，然后研究分析企业上云面临的主要数据安全风险，并针对风险给出相应的数据安全策略，供相关企业参考，最后提出企业上云可先从“容灾备份上云”入手，然后逐步向“核心业务迁移”过渡的建议。

关键词　企业上云　数据安全　数据安全风险　数据安全策略

1 引言

目前，中国已经进入信息化3.0时代。云数据安全问题已成为企业上云的最大障碍，深入开展企业上云数据安全策略研究，为“上云”企业提供技术参考，对助推我国企业上云进程具有重要意义。

2 相关概念

2.1 企业上云与数据安全

(1)企业上云

2017年，《浙江省政府工作报告》出台“十万企业上云”行动计划，这是企业上云概念第一次被提出。企业上云也称企业云化，是指在互联网环境下，企业为降低信息化建设成本、优化运营管理流程、创新业务发展模式，以硬件、软件、数据等基础要素迁入云端为先导，快速获取数字化能力，不断变革原有体系架构和组织方式，有效运用云技术、云资源和云服务，逐步实现核心业务系统云端集成，促进跨企业云端协同，不断融入开放创新生态的转型变革过程。

(2)数据安全

数据安全是指通过采用一定的技术手段和管理措施，保障系统数据的机密性、完整性和可用性，并能对数据进行安全审计。数据安全通常包括两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护；二是数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护。

2.2 企业上云的内容

根据《浙江省深化推进企业上云三年行动计划（2018-2020年）》文件附件中的定义，企业上云内容按上云程度通常可分为资源上云、管理上云、业务上云、数据上云、整体云化5类。

(1)资源上云

企业租用云服务商提供的计算、存储、数据库、网络带宽等云化IT资源，以及相应的安全防护服务。

(2)管理上云

企业将行政办公管理、人力资源管理、财务税务管理等信息系统部署在云端，或直接应用云服务商提供的基于云计算的相应管理软件和服务。

(3)业务上云

指企业在云端协同开展设计和研发，部署ERP（企业资源计划系统）、MES（制造过程执行管理系统）、PLM（产品生命周期管理系统）、CRM（客户关系管理系统）等，以及采购、仓储、物流等供应链管理软件，电商、客服等营销管理软件，或直接使用云上相关的SaaS服务。

(4)数据上云

通过资源云化、管理云化、业务云化，促进企业高效采集生产经营数据，逐步实现数据集成打通，并从本地数据中心向云上迁移，支撑企业实现云端数据同步，及云上智能分析等数据开发利用。

(5)整体云化

企业IT基础资源、生产制造、经营管理等全面云化，实现资源融合、数据融合，驱动业务创新和价值重构，促进企业数字化、网络化、智能化发展。

总之，企业上云内容覆盖企业的方方面面，相互之间又有很多结合点。但无论企业上云的内容和程度如何，只要企业选择云服务，都需要进行数据安全防护与隐私保护。文中主要从云数据安全的维度，阐述企业上云面临的风险，并给出相应数据安全策略供上云的企业或咨询单位参考。

3 企业上云数据安全风险

数据资源是企业的命脉，云数据安全问题已成为企业“上云”的最大障碍。当前，企业上云主要面临身份认证、数据传输、数据存储和安全审计等数据安全风险。

3.1 认证与访问控制风险

企业上云后，系统和数据部署在云端，将面临身份认证和访问控制风险，云用户身份一旦被盗用或访问控制界限被突破，攻击者就可获取企业部署在云端的软硬件资源和相关数据资料，甚至可以利用云平台各种资源组织类似DDoS的大规模攻击行为。按照云计算根据实际使用资源付费的方式，受控客户将在不知情的情况下为黑客发起的资源连线偿付巨额费用，并且很难对此类攻击进行定位和追踪。

3.2 数据传输安全风险

企业上云后，经常需将企业内部基础数据通过网络传递到云端，由云计算系统进行加工处理，或者从云端调用和下载相关处理后的数据，数据在网络传输过程中存在被黑客截获的风险，如何保障数据在传输过程中不被窃取或数据即使被窃取也无法还原，成为企业上云数据安全关注的重点。

3.3 数据存储安全风险

基于云计算模式，云服务提供商在大容量集中存储空间，按需划分一定的存储空间给企业使用，企业并不清楚自己的数据存储在哪些物理设备，甚至不知道这些物理设备部署在哪些国家。因此，企业上云后，在数据存储资源共享的环境下，数据存储主要面临加密存储、数据隔离、数据残留等方面的威胁与挑战。

(1)数据的加密存储

在云计算环境中，数据云存储面临一个安全悖论，即：加密存储，数据不方便计算处理，甚至无法处理和加工；不加密存储，数据安全及隐私无法得到保障。在PaaS模式和SaaS模式中，现有的技术对加密数据的检索或运算操作是非常困难的，因此，云计算服务提供商一般不对数据进行加密存储，存在较大的数据安全风险。

(2)数据隔离

基于多租户技术的云计算架构中，多个租户或企业的数据会存放在同一个物理存储，甚至是同一数据表中，尽管云服务提供商采用数据标签和访问控制等数据隔离技术来防范对混合存储数据进行非授权访问，但是仍然存在非授权用户通过程序漏洞进行非法访问的安全风险。譬如，2009年3月，Google公司就发生过大批量的不同用户之间数据非授权交互访问的安全事件。

(3)数据残留

数据残留是数据在被以某种形式删除后所残留的形式，即在逻辑上已经被删除，但在物理存储介质中仍然存在或通过技术处理可实现数据恢复。在云计算环境中，数据残留可能会导致企业数据被无意泄露。到目前为止，还没有哪个云服务提供商可以完全解决数据残留问题。

3.4 数据安全审计风险

为确保上云的数据归企业所有，并且除企业和其授权用户外的任何人不能访问和更新数据，需要对数据进行安全审计。在云计算模式下，企业数据存储至云端后，云服务提供商很容易获得数据的优先访问权，因此，云服务提供商本身提供的数据安全审计服务是不在可信域中的。而企业对云端数据进行安全审计要比数据存放在本地或可信域中时要复杂得多，目前只能依靠概率分析手段进行审计，存在很多漏洞与风险。

4 企业上云数据安全策略

企业上云的数据安全保障是一项系统工程，涵盖云数据安全的全生命周期，包括数据的产生、存储、使用、分享、归档、销毁6个环节。上云企业应根据云数据生命周期各阶段的安全特点，制定相应安全策略，降低数据安全的风险，确保上云后企业可实现降成本、提效率和从数据中获得价值释放的目标。

4.1 身份认证与访问管理策略

企业采用云计算服务以后，机构的信任边界将变成动态的，并且在企业IT控制范围之外，因此身份认证与访问管理（IAM）变得非常重要。为弥补控制权的丢失，建议企业采用高级别的软件控制策略（譬如采用应用程序安全和用户访问控制），并优先选取已经建立统一集中认证和授权系统的云计算服务提供商，确保满足企业权限策略管理和访问认证管理的要求。

(1)集中用户认证

目前主流认证方式有LDAP、数字证书认证、令牌卡认证、硬件信息绑定认证、生物特征认证等，支持多因子认证。云计算服务提供商能针对企业的不同需求，提供相应安全与技术等级的一种或多种组合认证，满足企业上云的不同子系统安全等级、成本、易操作性等差异化需求。同时能提供企业用户访问日志记录，并记录用户登录信息，包括系统标识、用户名、登录时间、登录IP地址、登录终端等信息。

(2)集中用户授权

云计算服务提供商用应能根据用户、用户组、用户级别的定义对云计算系统资源的访问进行集中授权，具备集中授

权或分级授权机制，并支持细颗粒度的授权策略。

(3)访问授权策略管理

云计算服务提供商应能提供用户身份与终端绑定、完整性认证检查及口令等常用的身份认证策略，支持采用集中授权或分级授权策略。同时，云计算服务提供商应有完善的账号安全策略，包括口令连续错误锁定账号、长期不用导致账号失效、用户账号未退出时禁止重复登录等策略，并允许企业自定义个人用户账户权限，支持添加特定条件（如：时间、来源IP地址、是否使用 SSL等）。

另外，对上云企业而言，云计算服务提供商必须有完整的日志管理，支持对用户认证信息、授权信息等详细日志的集中存储和查询，同时须支持对认证、授权等敏感数据进行加密存储及传输。

4.2 数据传输与存储安全策略

(1)数据传输安全策略

数据在传输过程中可能遇到被中断、复制、篡改、伪造、窃听和监视等威胁，需要保证信息在网络传输过程的完整性、机密性和有效性。

通常使用数据传输通道加密的方法保障数据传输安全，具体策略如下：

- 采用VPN、专线加密方式和数据加密技术，实现从用户终端到云主机中心传输通道安全；
- 管理域与其他域之间的数据传输采用加密通道，保障管理控制信息的安全性；
- 用户访问虚拟机采用SSH、HTTPS等安全传输协议。

(2)数据存储加密策略

目前，尽管还没有办法完全解决数据云存储面临的安全悖论，但是数据加密仍是云数据存储安全最可信的解决方案，从密码理论上讲，只要用户的密码没有暴露，即使数据丢失也可以保障信息不外泄。

对上云企业而言，在当前的技术背景下，常用的数据加密策略有：

- 用对称加密算法对企业数据进行加密；
- 非对称加密算法应用于身份认证、数字签名及对称加密算法密钥的传送；
- 不可逆加密算法用于企业应用系统中的口令加密；
- 采用第三方加密机制，真正做到让企业放心，云服务商可自证清白。譬如，杭州安恒信息技术有限公司在阿里云“钉钉”的开发模板中引入了“密盾”，钉钉用户选用“密盾”对自己的数据加密后，密钥就只掌握在用户自己手里，包括阿里云服务商在内的其他个人或组织都没有办法获取到这些数据，而且，这个基于第三方加密机制的“密盾”产品的可靠性在2016年G20杭州峰会安保工作使用钉钉时得到了验证。

下面介绍一种常用的云计算虚拟磁盘加密系统（如图1所示），供上云企业选择数据存储加密策略参考。

该虚拟磁盘加密系统采用加密机、PKI证书、对称密钥三级密钥机制对虚拟磁盘进行高强度、高安全性的全盘加密。数据安全防护系统与第三方CA无缝对接，提供高安全、高可靠性的密钥管理服务。通过屏蔽云平台差异，兼容所有类型的Hypervisor，实现与云业务管理系统的松耦合关系以及数据安全防护系统的独立部署。

4.3 数据备份与数据销毁策略

(1)数据容灾备份策略

- 上云企业应要求云计算服务提供商做出承诺，对所托管数据进行容灾备份，以防止出现重大事故时，企业用户的数据无法迅速得到恢复。
- 企业上云可以通过考察、咨询等多种途径，了解云服务提供商的云存储系统容灾备份的建设模式，进而选择服务优良的云供应商。目前，云存储安全实践表明“两地三中心”系统容灾备份模式具有高可用性和容灾备份能力，如图2所示。“两地三中心”在同城建立两个可独立承担系统运行的云存储中心，双中心通过高速链路实时同步数据（RPO≈0）。通常情况下可同时分担业务及管理系统的运行，并可切换运行，发生灾难时可在基本不丢失数据的前提下进行容灾备份应急切换，保障业务连续运行。为提高应对地理和自然灾害的能力，在异地建立一个备份的容灾备份中心，采用异步复杂模式，无距离限制，当同城的双中心全部故障后，异地容灾备份中心可以对备份数据进行业务恢复。

(2)数据销毁策略

上云企业对数据进行删除操作后，云计算服务提供商要能保证彻底删除数据，确保无残留，防止数据被无意泄露。常用的数据销毁策略有：

- 重复使用磁盘前先做覆盖存储资源处理，确保之前的数据不可复原；
- 磁盘报废时进行消磁处理，消磁过程应全程视频监控。

4.4 数据安全审计策略

在当前技术条件下，企业上云数据安全审计策略有：

(1)选择具有完善的数据安全审计机制和高商业信誉度的云服务提供商；

(2)引入第三方数据安全审计机构进行数据审计，通过合同等机制和策略约束审计机构不泄露企业的数据，特别是敏感数据。

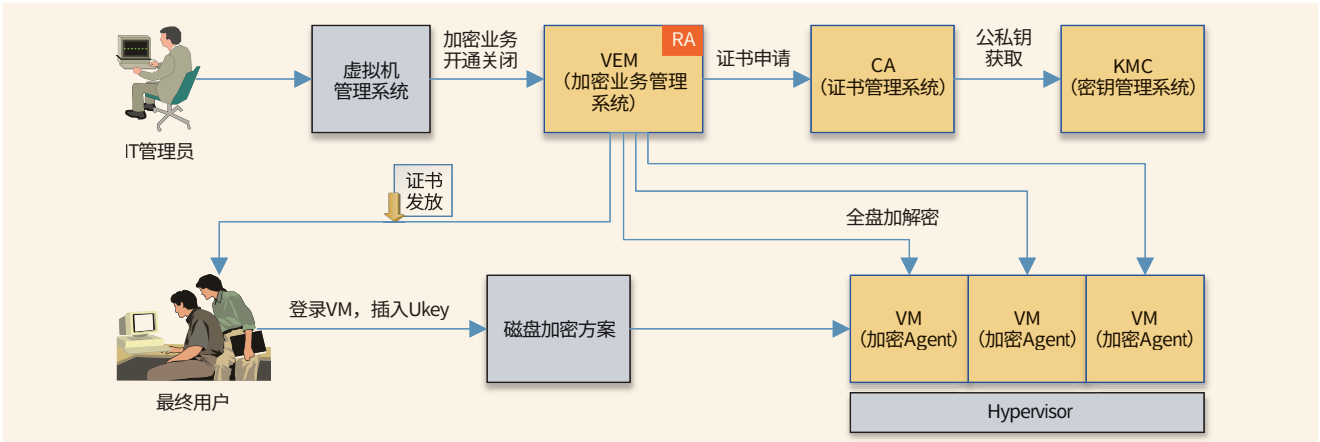


图1　云计算虚拟磁盘加密系统

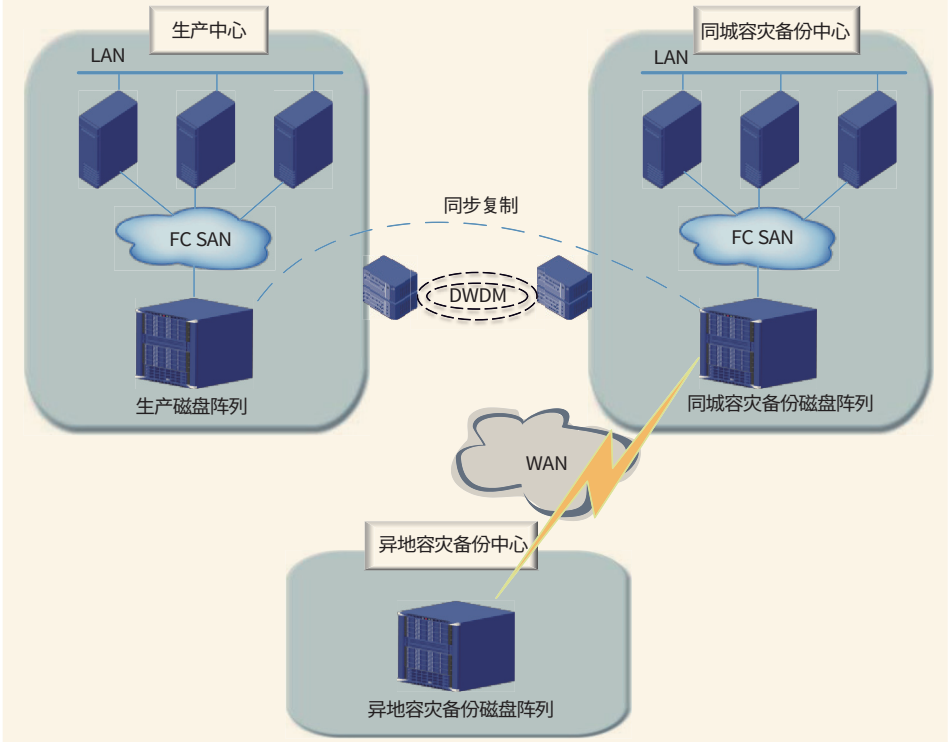


图2　云存储系统“两地三中心”容灾备份模式

5 结束语

企业上云要综合考虑企业IT现状、企业发展现状等因素，并结合对云的理解来确定上云的方式、内容及程度。目前，由于云计算的经济因素以及密码技术的限制，云计算服务提供商无法提供足够强大的数据安全保证，但企业不能因此延缓上云的进程，否则企业会逐渐被边缘化，失去市场竞争力。根据现有技术水平，加密数据在云计算中若只是用作简单存储，则安全是有保障的，因此无论企业IT基础如何薄弱，信息化人才如何缺乏，企业都可先从“容灾备份上云”入手，迈出企业上云的第一步，通过将数据容灾备份到公有云，用户可以实现与公有云的磨合，然后逐步向“核心业务迁移”过渡。

参考文献

[1] 中国电信网络安全实验室.云计算安全:技术与应用[M].北京:电子工业出版社,2012

[2] 刘文云,岳丽欣,马伍翠,等.政府数据开放保障机制在数据质量控制中的应用研究[J].情报理论与实践,2018(4)

[3] 党长青.云计算技术及信息安全性分析[J].技术与市场,2014(10)

[4] 顾炯炯.云计算架构技术与实践(第2版)[M].北京:清华大学出版社,2016

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

付双胜

硕士，工程师，现就职于湖南省邮电规划设计院有限公司，主要从事云计算、网络及安全规划设计工作。

罗世雄

硕士，工程师，现就职于湖南省邮电规划设计院有限公司，主要从事IT、云计算、资源池规划设计工作。

doi:10.3969/j.issn.1000-1247.2018.07.002

基于MPLA算法的NB-IoT网络覆盖评估

肖　亚　宋知明
中国电信浙江公司嘉兴分公司

摘要　分析利用LTE和NB-IoT共站共天线部署的特点，根据LTE网络的海量MR信息，通过MPLA算法进行路损折算处理来评估NB-IoT深度覆盖的方法，并通过现场测试对比进行验证。该方法解决了因NB-IoT终端不能上报测量报告而不能进行整网评估的问题，有助于网络运维人员及时了解当前NB-IoT网络的覆盖情况，精准助力网络建设进而支撑业务发展。

关键词　窄带物联网　LTE　测量报告　MPLA　深度覆盖

1 引言

在大数据、人工智能大展身手的今天，如果一味通过现场路测的手段了解网络的信号状况，不仅成本高、周期长、效率低，而且很多发生NB-IoT业务的场景点位通过路测不可能全面覆盖。基于成本、效率及全面的考虑，浙江电信提出利用共站共天馈部署的LTE和NB-IoT频段相近的特点，利用共站共天馈LTE的MR测量信息进行路损折算处理，解决NB-IoT终端不上报测量信息就不能进行整网评估，以及需要路测才能清楚网络信号状况的难题，为做好覆盖评估，指导建设优化进而支撑业务发展。

2 可行性分析

中国电信在重耕原CDMA 800MHz频段的基础上，开通全网的LTE 800MHz网络，并利用LTE 800MHz的射频设备、天馈线系统同站址按1:1开通NB-IoT网络。因此，NB-IoT网络在组网结构上与LTE 800MHz网络具备同站址同天馈、频段相近的特点，具备覆盖评估折算的基本条件。

2.1 同站址同天馈组网

根据中国电信相关规范，目前中国电信LTE 800MHz网络与NB-IoT网络采用1:1同站址组网。且由于共射频设备、天馈线系统，NB-IoT网络与LTE 800MHz网络在射频特性上（天线型号、天线挂高、俯仰角、方位角）保持完全一致。

2.2 同频段组网

LTE 800MHz网络部署于原CDMA 800MHz重耕后的空余频段，中心频点为2458；NB-IoT网络部署于CDMA网络的保护带宽上，中心频点为2506。二者同属于Band 5，在频带上相差4.8MHz。由于频段相同，二者理论上具有相同的无线传播特性。中国电信LTE 800MHz网络频点划分如图1所示。

2.3 LTE网络MR覆盖评估方法

MR数据是用户在执行业务过程中上报给网络的测量信息，能够准确反映网络的覆盖情况。MR定位是利用 MR中的主服务小区和邻小区电平信息结合主服务小区与邻区的经纬度及发射功率，确定MR发生的经纬度以及生成MR时用户所在位置；再将场强信息栅格化，即按照一定尺度将网络划分为若干正方形栅格（栅格为50m×50m），将MR发生的经纬度映射到栅格来实现。利用海量MR数据将LTE网络栅格化，以栅格为单位建立网络模型，将LTE网络覆盖情况可视化呈现出来，为射频精细优化和LTE工程规划提供重要支撑。以嘉兴城区为例，MR覆盖栅格如图2所示。

相比传统的DT/CQT采集数据的方法，MR评估方法具有采样全面、经济高效等优点，目前广泛应用于中国电信LTE网络的覆盖评估中，有效指导网络建设与优化工作。

3 基于LTE MR折算NB-IoT方案

基于现网数据，通过工程参数确定折算小区对，利用已有LTE 800MHz的MR、MDT等数据生成栅格数据构建目标网络的路损矩阵，借此来评估NB-IoT的网络覆盖。

3.1 覆盖折算公式

Forecast RSRP=NB-IoT Power+NB-IoT Antenna Gain-[(LTE Power+LTE Antenna Gain-LTE RSRP)]+MPLA Offset，

以LTE折算NB-IoT为例，重点考虑如下三个方面的折算。

NB-IoT Power+NB-IoT Antenna Gain：考虑目标网发射功率和对应天线增益。

LTE Power+LTE Antenna Gain-LTE RSRP：源网络栅格对应的源小区路损。

MPLA Offset：源小区和目标小区的路损差，包含频段不同引起的路损偏差和天线高度不同引起的路损偏差。

3.2 覆盖折算过程

整体折算流程见表1。

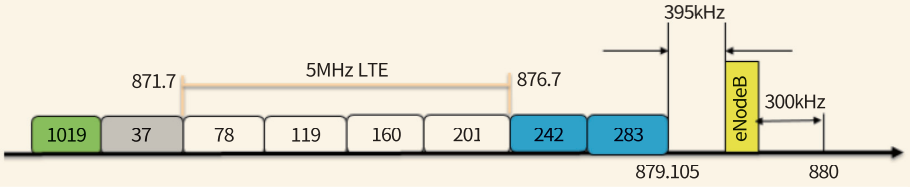


图1　中国电信LTE 800MHz网络频点划分

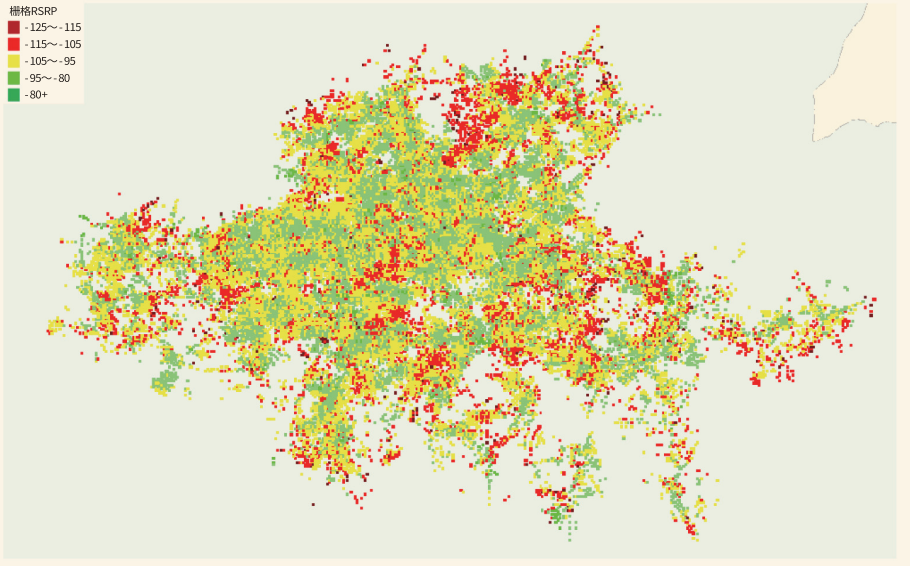


图2　嘉兴城区MR覆盖栅格

4 应用MPLA算法的LTE 路损折算方法

MPLA算法（Multi-band Propagation Path-Loss Adaptive，多频段路损折算算法）是本次折算方法的关键。借助LTE 800MHz计算出的栅格路损差值，通过MPLA算法计算出相同位置NB-IoT的路损差值。

4.1 Freq_PathLoss折算

对于Freq_PathLoss，采用Okumura-Hata传播模型，适用频率：150～1500MHz。路损公式如下。

$$PL=69.55+26.16\times\lg F-13.82\times\lg(Hb)-a(Hm)+[44.9-6.55\times\lg(Hb)]\times\lg D+C$$

F：频率，单位MHz。

H：基站天线有效高度，单位m。

D：发射天线和接收天线之间的水平距离，单位km。

C：环境校正因子，根据现场环境不同而取值不同。

不同频率引起的路损差异可以简化为传播模型计算的路损差异Freq Offset_PathLoss。

Freq Offset_PathLoss=目标小区Freq_PathLoss-源小区Freq_PathLoss

4.2 Height_PathLoss折算

对于Height_PathLoss估算，采取SPM传播模型，适用频率：150～2000MHz。路损公式如下。

$$PL=K1+K2\times\lg(d)+K3\times\lg(Htx)+K4\times Diff+K5\lg(d)\times\lg(Htx)+K6\times Hrx+K7\times f(clutter)$$

表1　整体折算流程

覆盖折算步骤	步骤一	步骤二	步骤三	步骤四
步骤名称	确定折算小区对	对折算小区进行优先级排序	折算小区对过滤	目标小区路损构建
输入	NB-IoT网络工程参数/LTE 800MHz工程参数	上一步匹配好的折算小区对	A：上一步排序好的折算小区对； B：现网MR、MDT数据	A：上一步选取折算小区对； B：现网MR、MDT数据； C：传播模型
处理过程	A：根据工程参数确定小区对，小区对必须是共站、共天馈小区； B：遍历目标网（NB-IoT）每个小区，寻找源网络匹配条件的小区	A：首先判断是否有频段相同的小区对，根据天线挂高、方位角、频段、制式接近的程度对小区对排序； B：排序时频段差异小的小区对有更高的优先级	A：选取源网有现网数据导入的现网小区及其对应的目标小区作为折算小区对； B：根据折算小区对优先级选取优先级最高的小区对做折算小区对，如果有多个相同的优先级小区对，则都选取	根据上述折算公式折算目标网络NB-IoT的RSRP值

*K*1：常数，其值与频率有关，单位dB。

*K*2：lg(*d*)的乘数因子（距离因子），该值表明场强随距离变化而变化的快慢。

D：发射天线和接收天线之间的水平距离，单位m。

*K*3：lg(*Htx*)的乘数因子，该值表明场强随发射天线高度变化的情况。

Htx：发射天线的有效高度，单位m。

*K*4：衍射衰耗的乘数因子，该值表明衍射的强弱。

Diff：经过有障碍路径引起的衍射损耗，单位dB。

*K*5：lg(*d*)×lg(*Htx*)的乘数因子。

*K*6：*Hrx*的乘数因子，该值表明场强随接收天线高度变化的情况。

Hrx：接收天线的有效高度，单位m。

*K*7：*f*(*clutter*)的乘数因子，该值表示地物损耗的权重。

f(*clutter*)：因地物所引起的平均加权损耗。

不同站高引起的路损差异可以简化为传播模型计算的路损差异Height Offset_PathLoss。

Height Offset_PathLoss=目标小区Height_PathLoss−源小区Height_PathLoss

表2为这两种传播模型的简单介绍及对比。

4.3 MPLA Offset算法

MPLA算法使用的前提是源小区和NB-IoT小区共站共天馈，每次计算的源小区和目标小区的路损差，包含频率不同引起的Freq_PathLoss和天线高度不同引起的Height_PathLoss。所以MPLA Offset计算时还会考虑NB-IoT和LTE 800MHz的下倾角及站高差异所带来的影响（主要考虑到后续技术演进可能会存在NB-IoT和LTE 800MHz不共设备的场景）。MPLA算法示意如图3所示。

5 成果应用验证

根据上述方案在杭州拱墅区域选取试点评估区域，该区域涵盖新小区、老小区、商业楼宇、学校、商场等常见典型场景。由于NB-IoT关注的重点在深度覆盖上，故本次验证的是室内的折算场景。

步骤1：采集该区域LTE MR数据，分析得到该区域内LTE 800MHz的室内覆盖结果，再将LTE 800MHz室内覆盖结果导入覆盖折算工具，输出折算后NB-IoT的室内覆盖结果。将上述折算前后的室内覆盖结果结合卫星地图进行建筑物匹配，得到折算前后LTE 800MHz和NB-IoT室内分布的感知地图，具体如图4所示。

说明：考虑到NB-IoT测试终端相比普通手机有2～3dB的接收天线增益；同时NB-IoT终端实际商用时是部署在行业终端内部且布放在较隐蔽的地方，NB-IoT相比LTE 800MHz手机又存在5～8dB损耗。实际验证时，LTE 800MHz用的是手机，NB-IoT用的是测试终端，那么可以将NB-IoT这部分7～11dB的增益折算到小工具的额外损耗中。

步骤2：为减少采样点数量带来的误差，在区域内选择31幢楼宇（每栋楼测4层，每层楼3个点，最后按照楼宇对RSRP取平均值）进行现场验证测试，统计发现折算后预测的电平和现场实测电平吻合度较高，87%的点位偏差在4dB以内，5个点位偏差超过4dB。偏差较大的点和现场测试的位置存在一定的关系。通过实验测试验证，此方案评估准确率

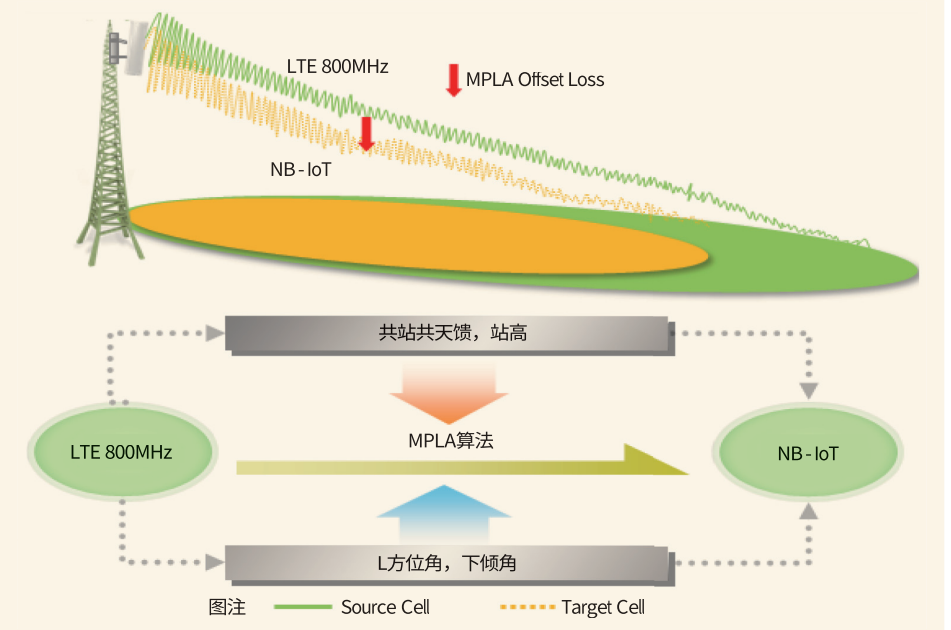
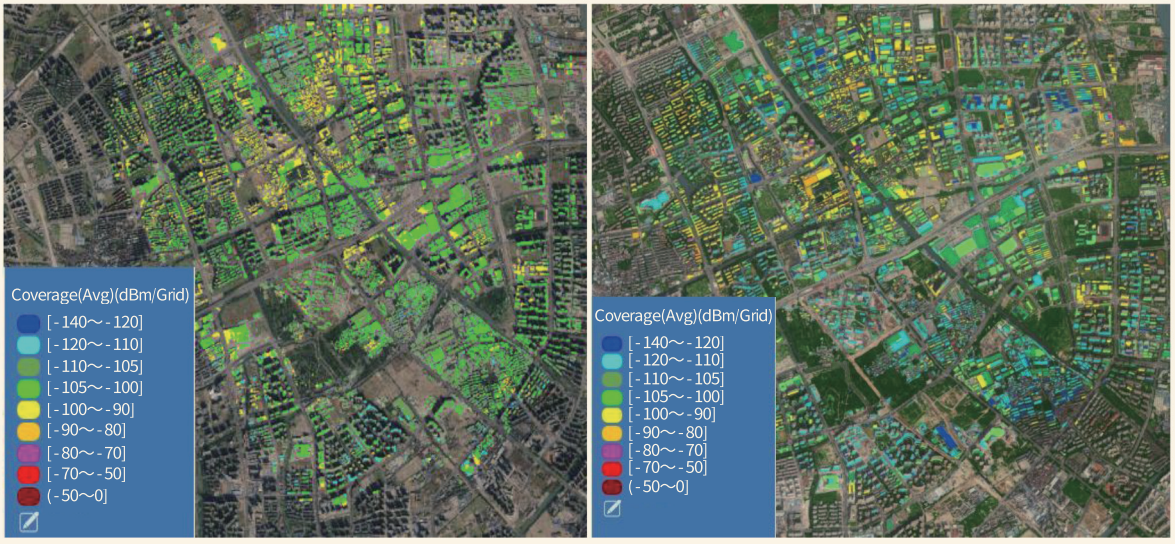


图3 MPLA算法示意

表2 两种传播模型对比

模型	适用频段	适合小区类型	适用场景	备注
Okumura-Hata	150～1500MHz	宏蜂窝；半径1～20km	普通城区、郊区、乡村，基站天线高于周围屋顶	对Okumura模型中的曲线进行拟合得到
SPM	150～2000MHz	宏蜂窝	适合各种室外宏蜂窝场景	一个通用的模型，根据实测结果进行模型校正



（a）LTE 800MHz室内分布感知地图　　（b）折算后NB-IoT室内分布感知地图

图4　室内分布感知地图

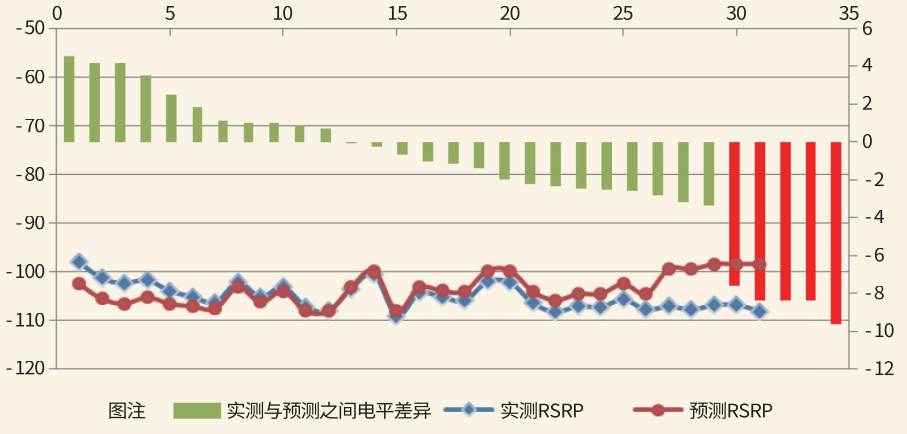


图5　NB-IoT折算电平与实际测试RSRP比较

较高，可以进行推广和应用。NB-IoT折算电平与实际测试RSRP比较如图5所示。

6 结束语

相比传统DT/CQT评估方法，LTE MR覆盖折算NB-IoT覆盖方法节省了大量外场测试的队伍和车辆，所有的过程都是基于后台人员提取的LTE MR数据在工具上实现，不仅节省成本也提高效率。若后期NB-IoT部署在LTE 1800MHz上，依据MPLA算法（多频段折算算法）依然可以用此方法来评估，不需要重新开发，减少后期额外的开发成本。

根据LTE MR折算NB-IoT网络覆盖评估技术有助于运维人员及时了解覆盖情况，精准助力政企部门对潜在的用户进行售前牵引，对在网的用户做好监控管理，真正成为业务收入的看护抓手，并在业务服务上进行主动呵护。有助于行业用户上下游依托于电信运营商的专业性和保障能力，能够将更多的精力着眼于日常运营、安全管理和服务升级，将业务和服务做专、做精，形成优势互补，提高用户满意度。

参考文献

[1] 戴博，袁戈非，余媛芳. 窄带物联网(NB-IoT)标准与关键技术[M]. 北京：人民邮电出版社，2017

[2] 中国电信集团公司. 中国电信NB-IoT无线网络系统优化指导书(试行)[Z]. 2018

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

肖亚

本科，毕业于浙江大学，长期从事移动通信规划与优化工作，现主要研究方向为CDMA/LTE无线网络规划与优化。

宋知明

硕士，毕业于浙江工业大学，长期从事移动通信维护与优化工作，现主要研究方向为CDMA/LTE无线网络维护与优化。

doi:10.3969/j.issn.1000-1247.2018.07.003

基于机器学习的客户信息安全防护研究

林玉广　张　恒
中国移动通信集团福建有限公司

摘要　针对电信运营商在客户信息识别和人员操作审计方面存在的效率低、不够系统全面等难题，首先自动化实现客户信息快速识别与定级，接着构建基于大数据的行为审计分析平台，通过聚类分析、决策树等算法，智能高效地实现对人员操作行为画像、行为轨迹分析和异常行为检测及预警，有效防止客户信息泄露，确保客户信息的安全。

关键词　信息安全　机器学习　大数据　运营商

1 引言

近年来，诈骗事件频发，各种信息安全泄露事件纷纷曝光，引起大众对客户信息的广泛关注。“大数据”时代，各类信息、数据已成为不同利益群体争相挖掘的宝贵资源，由此导致客户信息泄露问题，成为信息安全领域的“重灾区”。不管是国家政策、行业监管层面，还是运营商企业战略层面，都在不断加强对信息安全的管控要求，特别是随着2017年6月《网络安全法》的颁布实施，对数据安全的要求上升到法律层面，需要对数据安全更加重视，客户信息安全的保护已经成为电信运营商核心竞争力和品牌价值的有机组成部分。

客户信息集中存储在电信运营商业务支撑系统的BOSS、CRM、BASS及大数据平台中，因此电信运营商对大数据平台等系统的客户信息安全防护能力进行提升，加强客户信息安全管理，规范客户信息访问流程、用户访问权限以及承载客户信息的环境，防范客户信息被违规、违法使用和传播的风险迫在眉睫且极其必要。

2 客户信息安全现状及存在的问题

随着国家、社会的高度重视，以及上级主管部门的严格要求，运营商高度重视客户信息安全，但在日常信息安全工作中，客户敏感信息保护工作仍然存在不少盲点，主要集中在如下方面。

(1)客户信息识别较难、效率低。客户信息包括用户身份和鉴权信息、用户数据及服务内容信息、用户服务相关信息等。而在这三类信息中，又包含身份标识、基本资料、鉴权信息、使用数据、消费信息等诸多不同类型的数据。这就导致在实际工作落地中，电信运营商往往很难进行全量的识别，导致对这些客户信息进行管理时，无法进行全部监控，不能在第一时间发现风险。此外，客户敏感信息的识别，目前基本还是靠人工定期梳理，依赖于风险评估人员的个人经验，评判标准不统一，在面对海量数据等场景时识别速度慢、周期长、覆盖不全面。

(2)缺乏全景化的客户信息态势感知。电信运营商业务支撑系统经过长期的持续建设，涉及管理人员、运维人员、开发人员的不断更替，此类涉及客户敏感信息的业务系统中，哪些地方、以什么形式存储敏感信息，敏感信息的安全保护是否符合要求，基本没人能够全面掌握。

(3)人员对客户信息操作访问的监控和审计缺乏有效手段。国家法律法规和运营商企业管理办法对规范各类人员对客户信息的访问和使用，以及降低客户信息泄露风险起到相应的作用。然而运营商营业厅网点比较多，客户终端量比较大，服务人员流动性也较大，需要从不同层级对客户信息的使用和流转进行监控。但目前缺乏有效的技术措施和产品能做到全过程的监控和信息泄露事件的有效定位，及时定责和追查违规人员，及时通告相关主管，形成管理信息防护的闭环。

3 客户信息安全防护对策与实践

为了更好地做好客户信息的安全防护，解决运营商在客户敏感信息识别和人员操作审计方面存在的效率低、不够系统全面等长期未能有效解决的难题，基于多年的客户信息安全防护能力建设研究和实践，根据运营商客户信息访问总体架构（如图1所示），以前后台人员操作、用户行为轨迹等应用场景为切入点，利用自动化工具快速识别敏感信息，

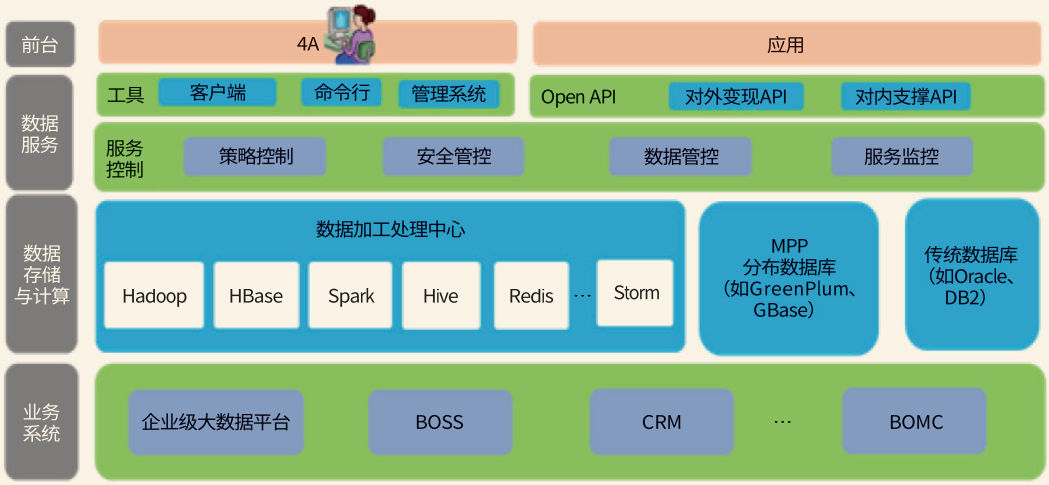


图1　客户信息访问系统架构

可视化展示敏感数据的态势感知。同时，利用流处理、大数据等技术搭建前后台人员操作行为审计分析平台，通过聚类分析、决策树等机器学习算法进行数据流转监控、用户操作实时分析、异常行为检测和预警，并对疑似异常行为核实确认，形成闭环的解决方案。

该方案实现事前客户敏感信息生成自动发现与定级、事中敏感数据使用实时监控与预警、事后智能高效安全审计分析及异常行为核实确认的全流程安全管控，最大限度保护系统中的敏感数据，确保客户信息的安全。

3.1 客户信息定义及分类分级

对客户信息的定义与分类是客户信息安全防护体系建设的基础。客户信息是指电信运营商在提供服务过程中收集的、能够单独或者与其他信息结合识别客户个人身份和涉及客户个人隐私的信息，包括但不限于客户姓名、出生日期、身份证件号码、住址等个人身份信息，以及使用服务的号码、账号、密码、时间、地点等信息，具体包括用户身份和鉴权信息、用户数据及服务内容信息、用户服务相关信息等三大类。

用户身份和鉴权信息：包括但不限于用户自然人身份及标识信息、用户虚拟身份、用户鉴权信息等。

用户数据及服务内容信息：包括但不限于用户的服务内容信息、联系人信息、用户私有数据资料、私密社交内容等。

用户服务相关信息：包括但不限于业务订购关系、服务记录和日志、消费信息和账单、位置数据、违规记录数据、终端设备信息等。

基于《电信和互联网服务用户个人信息保护分级指南》等，结合电信行业的业务特点，典型的电信运营商客户信息定义与分级标准见表1。按照客户信息的敏感程度划分为极敏感级、敏感级、较敏感级和低敏感级4个等级，并根据分类分级管控原则，确定不同敏感数据的安全管控要求及相应的涉敏人员范围。

3.2 敏感数据自动识别与感知

在复杂、全面的海量数据中识别出敏感数据，是客户信息安全防护的第一步。只有知道敏感数据的存放位置、存放形态、应用场景，才能帮助管理员配置合适的授权策略和保护措施。

传统基于人工识别客户敏感信息的方式主要依赖于风险评估师的个人经验进行。这种方式首先在面对大量数据时梳理速度周期较长、识别速度慢、不够系统全面；其次主要依赖人的主观判断，评判标准不统一。基于敏感信息定义与分级分类标准，开发自动化工具和界面，通过规则配置、模糊匹配和自然语言分析等手段，实现对客户敏感数据的自动快速、全面识别与定级，并可视化全景展示敏感数据的态势感知。

3.2.1 敏感数据识别与定级

敏感数据自动化工具主要基于元数据的关键字匹配、数据内容的正则表达式匹配和自然语言分析等方式实现客户敏感数据自动发现与定级。

(1)基于元数据的敏感数据识别

首先定义敏感数据的关键字匹配式，通过精确或模糊匹配表字段名称、注释等信息，利用元数据信息对数据库表、文件进行逐个字段匹配，当发现字段满足关键字匹配式时，判断为敏感数据并自动定级。这种匹配方式成本低、见效

表1　敏感信息定义与分级分类标准

级别定位	子类及范围	对应数据	安全管控原则
极敏感级	实体身份证明	身份证、护照、驾照、营业执照等证件影印件等；指纹、声纹、虹膜等	实施严格的技术和管理措施，保护数据的机密性和完整性，确保数据访问控制安全，建立严格的数据安全管理规范以及数据实时监控机制
	用户私密资料	揭示与个人种族、家属信息、居住地址、宗教信仰、基因、个人健康、私人生活等有关的用户私密信息以及《征信业管理条例》等法律、行政法规规定禁止公开的用户其他信息	
	用户密码及关联信息	用户网络身份密码及关联信息，如手机客服密码、139邮箱密码、飞信密码、移动WLAN密码、和包等交易密码，以及这些密码关联的密码保护答案等	
敏感级	自然人身份标识	客户姓名、证件类型及号码、驾照编号、银行账户、客户实体编号、集团客户编号、集团客户名称、集团客户负责人/联系人信息等可以精确标识定位具体实体客户的信息	实施较严格的技术和管理措施，保护数据的机密性和完整性，确保数据访问控制安全，建立数据安全管理规范以及数据准实时监控机制
	网络身份标识	联系电话、邮箱地址、网络客户编号、即时通信账号、网络社交用户账号等可以精确标识网络用户或通信用户的信息	
	用户基本资料	客户职业、工作单位、年龄、性别、籍贯、兴趣爱好等；集团客户所在省市、所在行业、集团签约时间及协议到期时间、单位成员个人、用户社会化生活实体编号（如水表号、社保号等）基本资料等	
	服务内容数据	电信网服务内容数据：短信、彩信、话音等通信内容； 移动互联网服务内容信息：包括飞信、融合通信、139邮箱等移动互联网服务所涉及的通话内容、即时通信内容、群内发布内容、数据文件、邮件内容、用户上网访问内容等； 用户云存储、SDN、IDC等存储或缓存的非公开的私有文字、多媒体等资料数据信息	
	联系人信息	用户通讯录、好友列表、群组列表等用户资料数据	
	服务记录和日志	服务详单及信令：包括语音、短信、彩信和GPRS详单、2G/3G/LTE用户面XDR及信令面XDR等，内含主叫号码、主叫归属地、被叫号码、开始通信时间、时长、流量等信息； 移动互联网服务记录：包括Cookie内容、上网日志、连接APP等，内含主叫号码、网址、网购记录等	
	位置数据	精确位置信息(如小区代码、基站号、基站经纬度坐标等)、大致位置信息(如地区代码等)	
较敏感级	消费信息和账单	消费信息：停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度、缴费情况、付费方式、余额、交易历史记录； 账单：每月出账的固定费用、通信费用、欠费信息、数据费用、代收费用	实施必要的技术和管理措施，确保数据生命周期安全，建立数据安全管理规范
	终端设备标识	唯一设备识别码IMEI、设备MAC地址、SIM卡IMSI信息等可以精确标识定位具体设备的信息	
	终端设备资料	终端型号、品牌、厂商、OS类型、预置/安装软件应用、使用时长等	
低敏感级	业务订购关系	基本业务订购关系：品牌、套餐定制等情况； 增值业务订购关系：139邮箱、飞信、通信录、来显、彩铃、和包等增值业务的注册、修改、注销	实施基本的技术和管理措施，确保数据生命周期安全
	违规记录数据	用户违规记录，包括垃圾短信、骚扰电话等记录、黑名单、灰名单等； 业务违规记录，包括端口滥用、违规渠道、不良网站域名等记录、黑名单、灰名单等	

快，可识别全网50%以上的客户敏感数据。

(2)基于数据内容的敏感数据识别

有些临时表或历史上开发的未按照规范建立的敏感表，根据元数据无法判断是否为敏感数据，这种情况更多是靠分析数据内容来判断。自动化工具通过扫描获取这些表，将系统中大量数值型、英文型的敏感信息（如手机号、身份证号、邮箱等）通过预先定义正则表达式的方式进行匹配，做出敏感数据及其级别的判定。

(3)基于自然语言处理技术的中文模糊识别

前面两种方式可以发现系统中大部分的客户敏感数据，但系统中还保存了部分中文信息，无法通过上述两种方式很好地发现。因此引入NLP自然语言处理技术加中文近似词比对的方式进行识别。首先，根据数据内容整理输出一份常用敏感词，该敏感词列表需具备一定的学习能力，可以动态添加敏感词；其次，通过NLP对中文内容进行分词，通过中文近似词比对算法计算分词内容和敏感词的相似度，若相似度超过某个阈值，则认为内容符合敏感词所属的分类分级。

3.2.2 敏感数据态势感知

识别出敏感数据后，可以通过敏感数据的态势感知、血缘追踪等方式帮助管理员对整个系统的敏感数据有全局认识，并通过机器学习等技术实现用户/应用行为实时监控预警功能，进而降低客户信息泄露、核心数据恶意破坏的风险危害。

图2　客户敏感数据的态势感知

根据客户信息的敏感等级、敏感字段数、记录数、访问频次等参数构建数据敏感等级评估模型，评测出主机文件目录、主机及数据库表、数据库的整体敏感等级，并在安全态

势感知平台集中可视化展现，通过图标大小展示不同主机及其目录、不同数据库及其表的敏感信息数量，实现系统敏感数据全景态势感知，如图2所示。

3.3 行为审计分析平台构建

通过对用户操作的日志等数据进行分析，可以发现不同的异常行为操作，如用户非工作时间登录、异常IP登录等。基于大数据技术构建行为审计分析平台，通过日志数据标签化的方法建立灵活自定义的审计模型，快速支撑人员操作行为画像、行为轨迹分析等应用场景的分析。

3.3.1 行为审计分析平台

用户行为审计分析平台系统架构如图3所示。该平台基于Hadoop分布式架构，将各系统用户操作日志基于实时数据流与数据模型进行匹配，通过日志集中存储、大数据建模分析、快

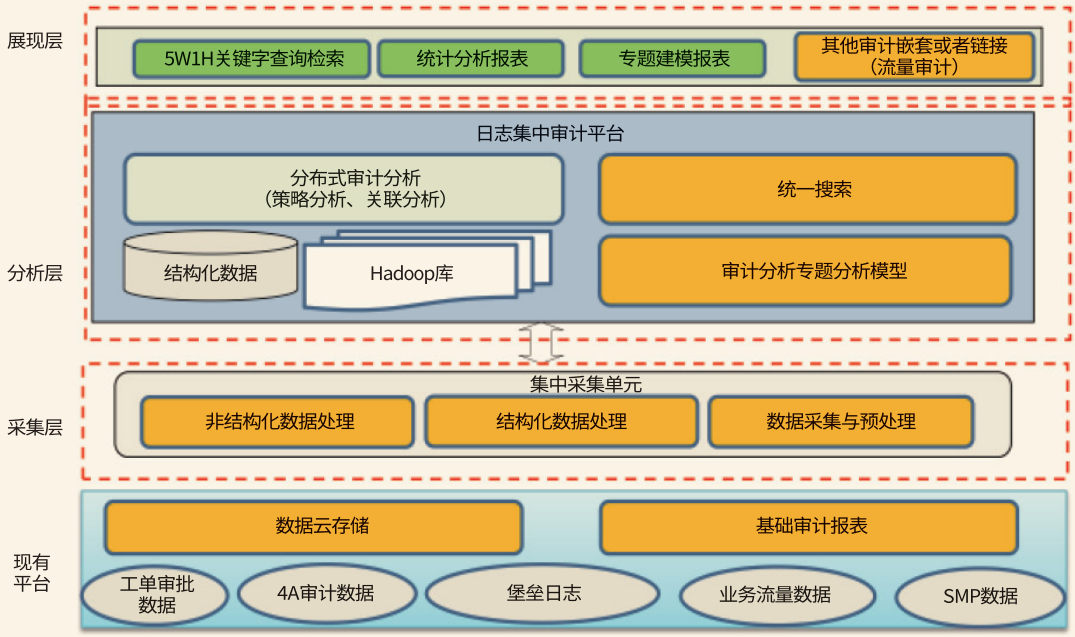


图3　用户行为审计分析平台

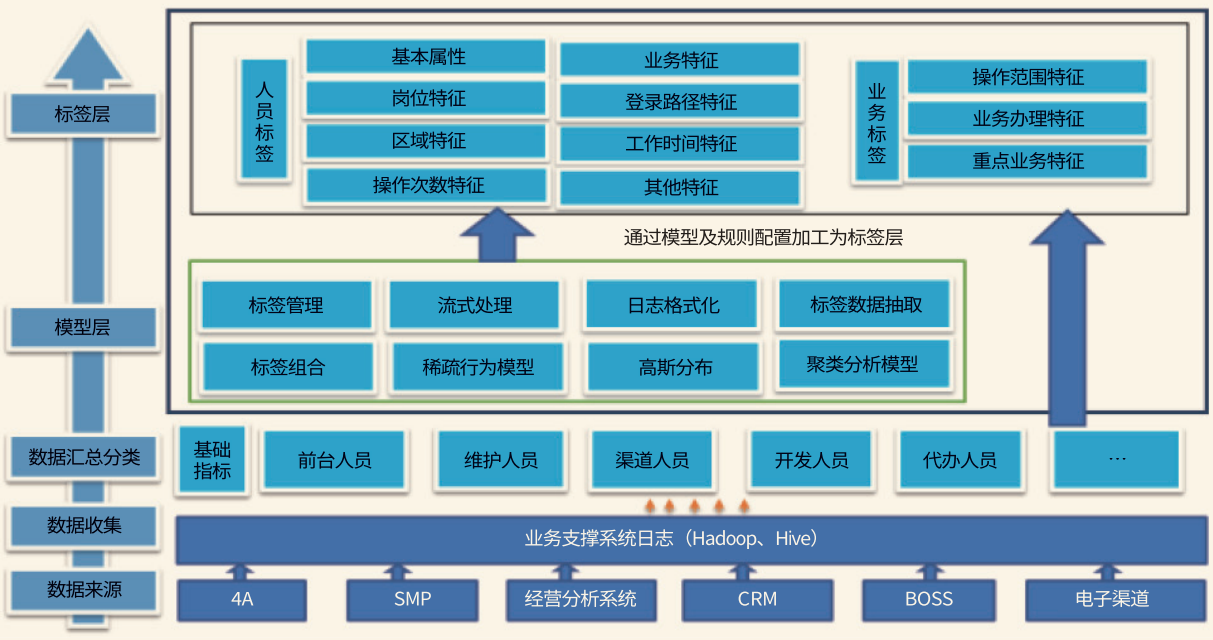


图4　日志数据标签处理模型

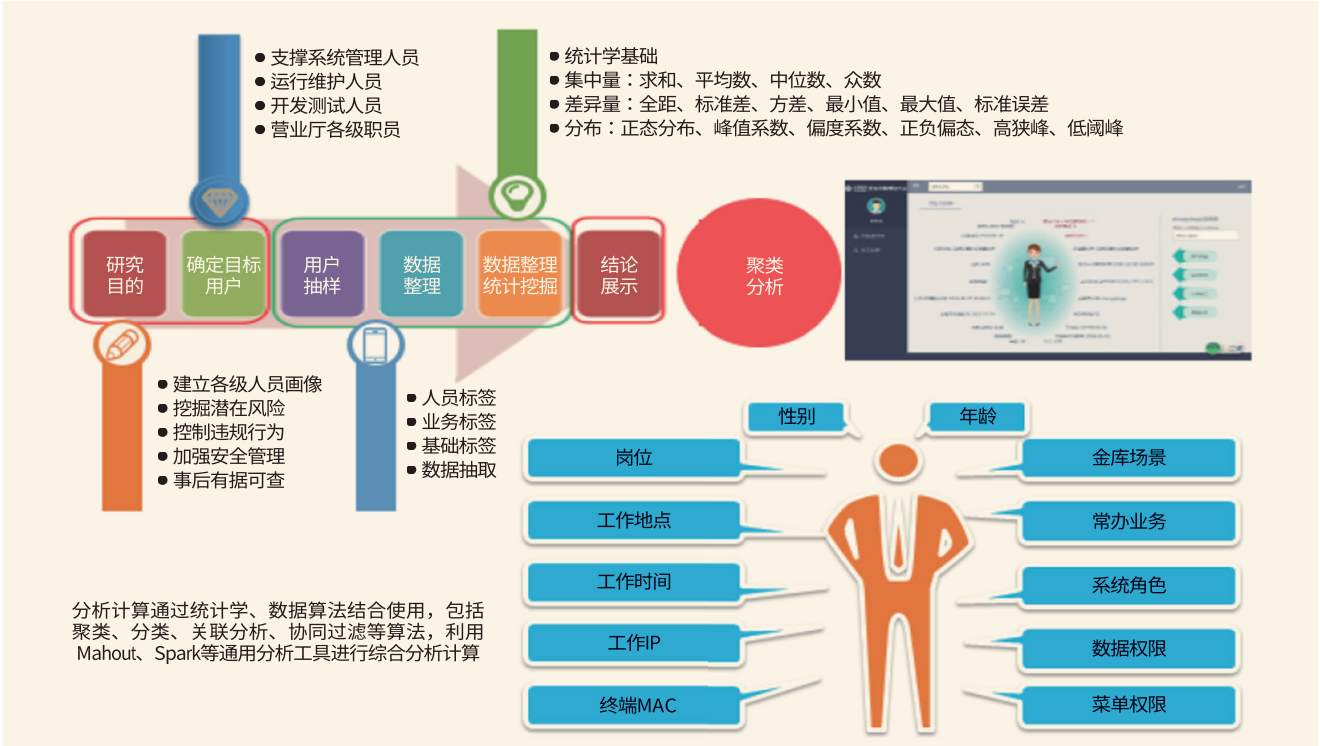


图5　人员画像模型

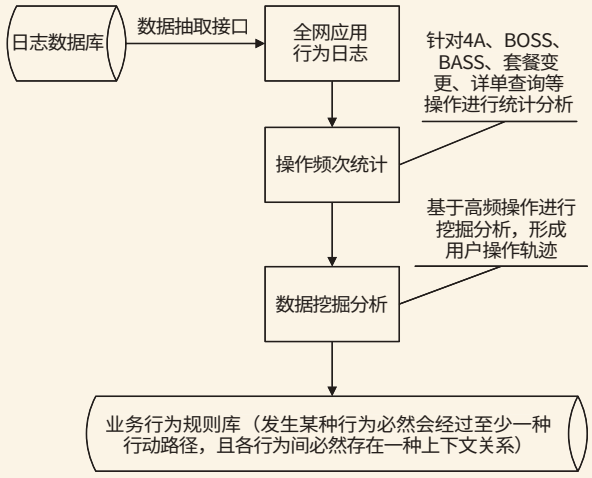


图6　全网用户行为轨迹分析

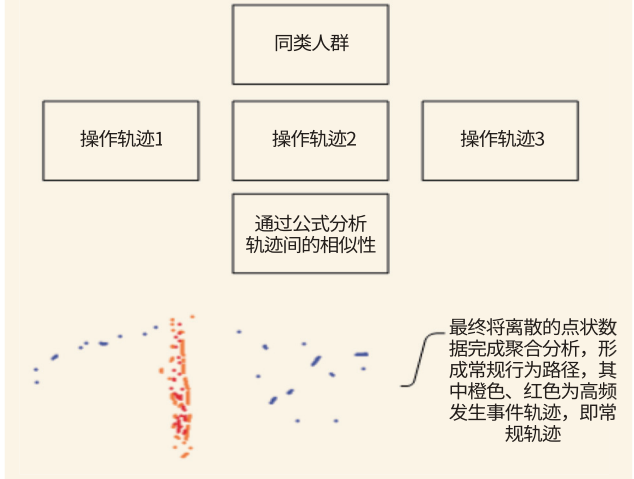


图7　单个用户行为异常检测

速检索等手段，实现对用户操作日志的集中审计分析。

3.3.2 数据标签处理模型

基于数据标签化的用户操作日志处理方法实现灵活自定义的专题审计模型（如图4所示），支持通过日志类型、日志标签的组合叠加，归纳形成审计日志决策树挖掘分析策略，并应用于前后台人员操作画像、用户行为轨迹分析等场景，极大提高安全审计覆盖场景和效率。

3.4 操作人员行为画像

构建用户行为画像的核心是给用户贴“标签”，而标签的选择是通过对用户信息分析而来的高度精炼的特征标识。通过构建人员画像模型（如图5所示），建立用户特征画像图谱，基于聚类分析等机器学习算法，支持对前台操作人员（自有渠道人员、社会渠道人员）、后台操作人员（包括系统管理人员、运维人员、开发测试人员）等各类人员的操作

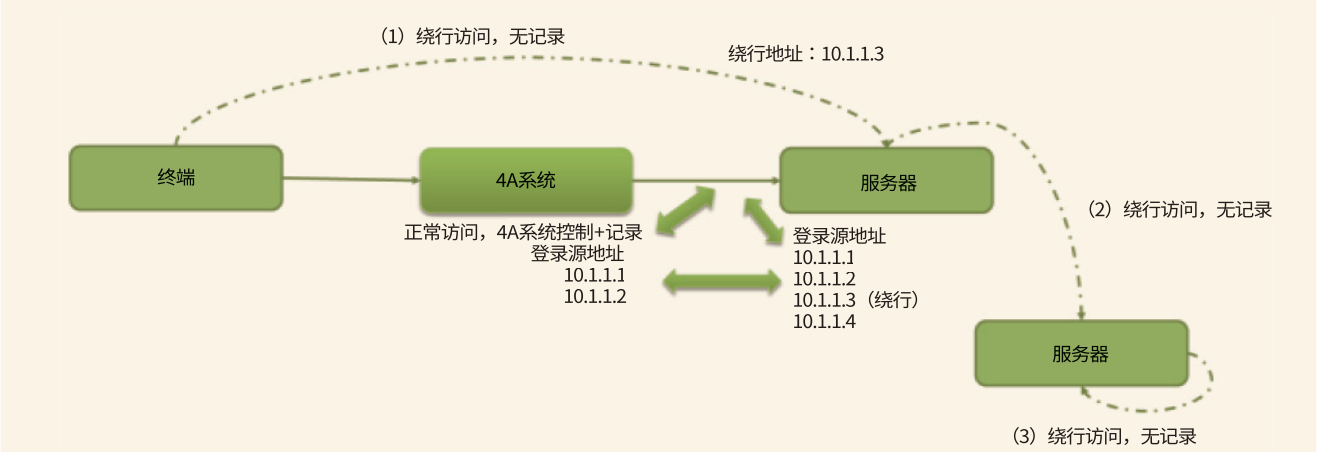


图8　用户绕行访问分析

行为进行数据标签和画像分析。

3.4.1 前台人员画像

将4A系统和BOSS/CRM/大数据平台等系统的操作日志采集到行为审计分析平台中，通过数据同步、数据解析和标准化保存到Hive中，按照如下步骤实现前台人员客户画像并分析异常行为。

(1)分析系统中各类前台人员的业务操作情况，刻画出人员操作行为画像。

(2)根据生产实际情况，建立分析模型，通过一段时间的数据学习，形成操作基线数据。

(3)根据各类型人员的操作行为画像与单个人员的操作日志进行自动分析，发现前台人员业务操作的异常情况。

3.4.2 后台人员画像

将4A审计系统采集的后台人员操作日志，包括数据库和主机操作日志，按照如下步骤实现后台人员客户画像并分析异常行为。

(1)按人员基本信息、人员操作类型、操作地址（网段）、资源类型、操作对象等属性对人员进行标签化处理。

(2)对标签化后的人员信息进行聚类分析，得出人员实际的归属类别和群体特征。

(3)对聚类后群体的操作特征进行分析，观察群体内的人员是否有偏离本群体的异常操作行为。

3.5 用户行为轨迹分析

基于系统资源日志数据、应用资源数据等信息进行深度数据挖掘，从用户访问行为中遍历用户频繁使用的路径，通过准实时分析用户的行为轨迹，预先发现用户的一些操作异动，并通过这些异动和既有知识库中的标准访问路径进行比对匹配，预示风险发生的可能性。

用户行为轨迹分析包括全网用户操作行为分析、单个用户行为异常检测两个步骤，分别如图6、图7所示。

以上述分析为基础，可建立完整的用户操作行为轨迹，从而实现对“人”“来源终端”“访问通道”“访问资源”“何种操作”的完整事件表述，有效支撑绕行访问敏感数据等异常行为监控，提升客户信息安全防控水平。同时，用户行为轨迹分析改变了以往的审计从一些预先设定的异常场景中去发现安全风险，无法将用户的正常操作事件串联起来发现有可能出现异常的问题，极大地提高审计系统的事前预知性。用户绕行访问分析如图8所示。

4 结束语

客户信息的安全防护是一项系统性工程，涉及到管理、流程和技术等多个方面。针对客户信息识别和人员操作审计方面存在的效率低、覆盖不全面等难题，基于机器学习、大数据等技术提出相应的安全防护对策和实践经验，以期为我国电信运营商实现客户信息全天候全方位感知和有效防护做出有益的探索。

参考文献

[1] 张琳，刘佳，张宏坤.通信运营商的客户信息安全保护研究[J].数据通信，2015(3)

[2] 王飞.基于大数据环境下的电信运营商客户信息安全保护研究[J].中国新通信，2017(18)

[3] 陈龙.基于行为监测的客户信息防护探讨[J].网络安全技术与应用，2017(10)

[4] YD/T 2782—2014，电信和互联网服务用户个人信息保护分级指南[S]

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

doi:10.3969/j.issn.1000-1247.2018.07.004

应对大流量分组核心网优化的研究与实践

武俊芹
中国联合网络通信有限公司河南省分公司

摘要 目前，以视频业务、在线手游为代表的移动数据流量爆发式增长，对分组核心网带来极大的冲击，在网络建设及扩容工作不能实时到位的情况下，通过修改分组核心网相关软件或参数来降低信令负荷、系统负荷，使分组核心网能承担更大流量的业务、更多的在线用户显得尤为重要。本文提出了应对大流量分组核心网优化的方案及实施步骤，有效提升了用户满意度。

关键词 智能寻呼 TA List SGSN/MME Pool 均衡用户

1 前言

目前，随着“冰淇淋”套餐、腾讯“大小王卡”等移动数据流量套餐的推广，河南的移动数据流量呈现几何式增长。4G扁平式的网络架构使得信令消息从数量巨多的4G基站（eNodeB）直接汇聚到4G分组核心网（EPC）,目前的4G语音解决方案（CSFB和VoLTE）都必须通过分组核心网。

2 实施背景

自2016年以来，河南联通使用移动数据上网的用户增加约3倍，流量增加约10倍。尤其是4G上网用户增加显著，月均用户和流量的增长率约为12%和25%。由于工程建设预估不充分，新建及硬件扩容工作不能及时实施，造成分组核心网即将处于高负荷运行状态，这样对其提供的服务能力、对设备自身的良好运行都带来极大的挑战。

3 优化研究及实施

3.1 MME开启智能寻呼，降低S1接口信令开销

3.1.1 核心网MME信令开销分析

EPS（4G通信网络）采用扁平的网络架构，由4G无线（LTE）和4G核心网EPC组成。其特点是4G基站直接与4G分组核心网EPC对接，优点是减少网络节点，缩短时延。4G是提供高速上网的纯数据业务的网络，没有语音业务。因此目前提供的语音解决方案都必须借助于4G分组核心网。这些都造成S1与其他接口的信令及其他信息量开销巨大，给核心网的CPU负荷、系统负荷、单板处理能力都带来巨大的冲击，使核心网网络不堪重负。

在EPS中，用户的位置信息主要通过TA（Tracking Area）表示；每个TA由一到多个eNodeB组成，TA之间没有重叠区域。4G的注册区域由一系列TA组成，即TA List；TA List由MME生成，在附着过程中带给UE，当手机在同一个TA List移动时不会发生TAU。MME能知道的UE当前准确的位置信息为TA List，所以通常情况下MME对UE注册的TA List中的全部eNodeB发起寻呼。河南联通4G语音方案采用的是CSFB方式，其主要实现方式就是4G的TAI（TAI=MCC+MNC+TAC）与3G的LAI做一个绑定，通过SGs接口进行，为了保证4G语音的时延及接通率，TAI的设置一定要合理，一般要求TAI的大小要小于等于LAI。通常情况下4G用户的TAU及寻呼都是基于TA List，因此TA List的设置就尤为重要，TA List不能过大（寻呼量会增加），也不能过小（会造成频繁的TAU）。在无线网络合理规划TA的基础上，MME通过合理地分配TA List，实现寻呼负荷和TAU的平衡。现网采用的是一个TA List包含一个TA的配置方法。

3.1.2 核心网优化寻呼策略及成效

EPC话务模型如图1所示。

从图1可以看出，EPC话务模型中，消息量最大的就是寻呼，因此对寻呼的优化就成为核心网优化中重中之重的工作。随着中国联通4G用户的快速发展，语音业务主要使用CSFB。目前发现MME的S1_MME接口利用率较高，主要原因是大量的寻呼消息占用了S1_MME的带宽。与此同时，MME设备的AP板卡负荷较高。一般来说寻呼策略包含如下因素：寻呼范围、寻呼次数、寻呼标识，因此优化寻呼策略要从三个方面下手，具体见表1。

经研究发现，90%的4G用户在使用语音业务时都驻留在Latest eNodeB下，因此河南联通决定在一个MME上修改现网的寻呼策略，即把默认对一个TA List做4次×3s的寻呼策略，修改为首次基于对Lastest eNodeB进行寻呼，二次及以后

对TA List做三次寻呼。

开启智能寻呼之前配置：

create_paging_profile -id 1 -enb 0 -ta 0 -talist 4 -ptpt NULL -enbl 0

开启智能寻呼之后配置：

create_paging_profile -id 7 -enb 1 -ta 0 -talist 3 -ptpt NULL -enbl 0

对修改过寻呼策略的MME进行一周的观察，发现该局的寻呼次数下降显著，S1-MME的带宽利用率、系统负荷也都有大幅度的降低，整个MME运行良好稳定，因此将爱立信所有的MME都开启智能寻呼的操作。

实施前后寻呼次数变化情况如图2所示。

智能寻呼开启前，MME的寻呼策略为对整个TA_LIST下发寻呼消息。智能寻呼开启后，MME对用户驻留的LAST_eNodeB下发寻呼消息。对TA_LIST的寻呼下降85%以上，极大地降低寻呼量。实施前后S1-MME链路流量变化情况如图3所示。

智能寻呼开启前，4台MME的S1_MME接口链路速率为700Mbit/s左右；智能寻呼开启后，4台MME的S1_MME接口速率下降到150Mbit/s，因为S1_MME链路90%为寻呼消息。

实施前后相关板卡负荷变化情况如图4所示。

智能寻呼开启前，4台MME01/13的AP板卡负荷平均值在70%以上；MME02/14的AP板卡负荷在50%以上。智能寻呼开启后，MME01/13的AP板卡负荷降低到50%以下；MME02/14的AP板卡负荷降低到40%以下；整体负荷降低40%以上。

综上，MME开启智能寻呼后对整体网络资源的利用进行了较大的优化，减少了核心网额外开销。其中对MME的AP板卡负荷降低30%；对S1_MME的链路利用率降低80%；由首次寻呼基于TA_LIST的寻呼改为对Latest eNodeB的寻呼，寻呼量降低85%，缩小寻呼范围，对无线侧亦减轻负荷。

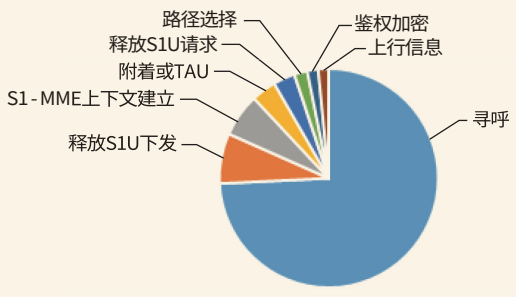


图1　EPC话务模型

表1　EPC寻呼策略优化研究方向：寻呼策略的设置因素

寻呼可选范围	寻呼次数设定	寻呼间隔	寻呼可采取的标识
Latest eNodeB	首次寻呼		S-TMSI（GUTI的一部分）
最近活动的eNodeB（列表）	二次寻呼		IMSI
最近活动的TA（列表）	三次寻呼		
UE当前的TA List	四次寻呼		
MME范围			

3.2 开启NNSF功能解决Pool内4G用户不均衡

目前现网中SGSN&MME为物理合设局，因此在2G/3G/4G互操作过程中首选合设的SGSN或MME，这样可

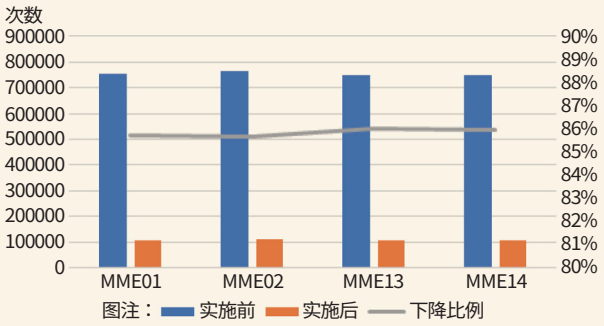


图2　实施前后寻呼次数变化情况

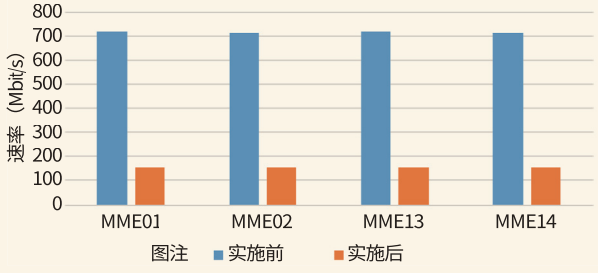


图3　实施前后S1-MME链路速率变化情况

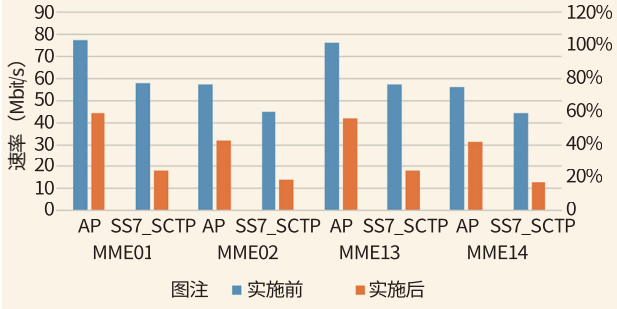


图4　实施前后相关板卡负荷变化情况

表2　SAEGW08 GTP echo每秒消息量统计

目的地址	基站侧故障时的SAEGW每秒收发的echo量	基站侧故障恢复后SAEGW每秒收发的echo量
	消息数	消息数
10.100.33.7（S1-U）	24285	23659
116.79.207.216（GnSGW-S5/S8-u）	26	23
220.206.141.242（GnPGW-S2b-u）	849	799

表3　SAEGW08 GTP echo优化后每秒消息量统计

目的地址	基站侧故障时的SAEGW每秒收发的echo量	基站侧故障恢复后SAEGW每秒收发的echo量	优化后基站侧故障时的SAEGW收发的echo量	优化后基站侧故障恢复后SAEGW收发的echo量
	消息数	消息数	消息数	消息数
10.100.33.7（S1-U）	24285	23659	12120	11723
116.79.207.216（GnSGW-S5/S8-u）	26	23	5	2
220.206.141.242（GnPGW-S2b-u）	849	799	166	157

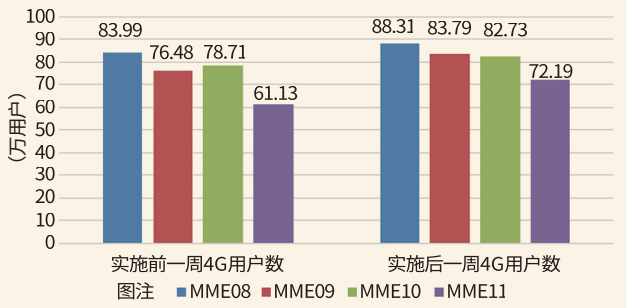


图5　开启NNSF前后4G附着用户变化情况

以减少局间信令开销，缩短时延，提高用户感知。但河南2G BSC因故没有组Pool，BSC在SGSN Pool中是单挂在某一个SGSN下的。中兴MME&SGSN Pool下的用户优先选择2G所在的SGSN&MME，日积月累之下就造成该Pool下的4G用户越来越不均衡，Pool内SGSN&MME间的设备利用率、系统负荷等指标差距明显，Pool的优势得不到体现。通过卸载高负荷SGSN&MME的方法解决4G用户不均衡的问题，其成本与收效差距较大且不能彻底解决问题。

经协商，采用开启NNSF功能解决该问题，具体做法为SGSN打开支持NNSF功能，指令如下。

SET SOFTWARE PARAMETER:PARAID=65582,PARAVALUE=1;

//Support NNSF Function

开启支持NNSF之后，用户从非FLEX区域进入FLEX区域，SGSN会将NULL NRI和非广播路由器给用户，用户重新接入时携带NULL NRI，FLEX RNC/BSC根据负荷分担关系选择SGSN，从而实现Pool中各个SGSN用户均衡。SGSN用户均衡后，根据选择合适局的原则，4G的用户也得到均衡。为了防止某些特殊场景下跨SGSN RAU没鉴权而造成PS的安全模式流程失败，进而影响RNC语音掉话率指标，还需要开启局间RAU强制鉴权，指令如下。

SET SOFTWARE PARAMETER:PARAID=327828,PARAVALUE=1

开启NNSF前后4G附着用户变化情况如图5所示。

综上，开启NNSF后基本解决MME Pool内4G用户不均衡的问题，这样Pool内的MME都能处于均衡的稳定运行状态，发挥出Pool的优势，使该MME可以接纳更多的4G用户，提供更优的服务能力。

3.3 优化GTP echo发送周期解决设备通信队列拥塞

河南联通ZZSAEGW07/08硬件是老平台设备，CPU处理能力弱，S1-U的路径检测消息（GTP echo）量处于较高水平，容易触发拥塞告警，引起单板负荷过高告警，影响这两个设备的良好运行。SAEGW08 GTP echo每秒消息量统计见表2。

从统计上可以看出，SAEGW每秒要处理的Echo Request消息负荷处于非常高的水平，其主动发出的Echo Request消息只有接收到的十分之一左右。无线侧告警恢复后，消息数量只有轻微的降低，也就是说目前只要有一些基站工作异常就会导致echo消息集中发送，造成ZZSAEGW07/08队列拥塞，因此无线侧优化GTP echo定时器才是解决SAE GW队列拥塞的关键。

GTP echo用来检测eNodeB和SGW之间业务路径的连通性，当路径不通的时候，会释放该路径上的所有承载。无线侧GTP echo定时器参数的修改会影响GTPU路径检查的灵敏度，和S1用户名路径告警上报有关，设置太小就会有大量的echo消息，但上报的灵敏性就更强；设置过大，GTPU保活请求发送周期检测会变长，周期配的越长，检测越慢。如果eNodeB与SGW之间的业务出现故障，会导致故障承载较长时间挂着。无线侧经过研究、测试验证，最后将基站上的GTP echo定时器参数由默认的1min发一次调整为2min发一次。

核心网侧经研究决定对ZZSAEGW07/08进行优化echo的操作，配置指令如下：

zte(config-xgw-pgw)#echo-request-send control 300 5

//间隔从60s修改为最大的300s。

SAEGW08 GTP echo优化后每秒消息量统计见表3。

综上，经过无线侧、核心网侧同时对GTP echo进行优化，ZZSAEGW07/08收发的GTP echo消息量大幅度下降，解决频繁出现队列拥塞告警、CPU负荷过高、影响设备良好运行的隐患。

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

doi:10.3969/j.issn.1000-1247.2018.07.005

移动互联网出口容灾分析和研究

孔令义　郭　威　时利鹏
中国联合网络通信有限公司河南省分公司

摘要　4G业务的飞速发展带来移动数据流量的激增，给运营商的网络承载带来巨大压力，尤其是网络的业务汇聚出口节点，一旦出现全阻故障，将产生恶劣的影响。通过对移动业务出口的业务容灾分析，给出相应的应急机制方案，使得发生节点级故障时，能够快速安全地疏通流量，保障业务安全。

关键词　移动互联网　容灾　流量　疏导

1 概述

当前组网架构中，用户流量到移动互联网采用的是回传到核心局点出口的模式，相比网络中其他节点，业务汇聚的出口节点承载业务量集中，一旦出现全阻故障，对用户感知影响巨大。

2 研究背景

2.1 移动互联网业务出口网络架构

河南移动分组核心网部署在郑州和洛阳两个大区的4个核心网局址，结合上网通信机制，用户上网流量出口相应汇聚到两大区移动分组核心网所在局址。在每个局址里，移动用户上网流量通过移动分组核心网SAE GW、SR路由器、Gi防火墙、Gi CE，接入城域网Internet出口，Gi CE和城域网设备之间部署EBGP，Gi CE通过EBGP接收缺省路由并通过OSPF非强制下发缺省路由引导SAE GW上行流量。整个网络业务出口组网拓扑采取“口”字型组网方式，具体如图1所示。SR路由器、防火墙、Gi CE此类集中汇聚节点设备，都采取了双冗余的配置部署。

2.2 当前业务出口面临的网络问题

根据移动上网通信的过程，移动数据流量最终通过分组核心网PGW（物理实体为SAE GW）的Gi出口接入公网或特定网络。现有网络中，分组核心网设备多采用集中设置的部署方式，相应的业务出口伴随设备也是集中部署。这种集中部署方式有方便管理维护，节省机房、传输等物理资源等优点，但在流量急剧增加的趋势下，单个局址承载的业务量压力逐步增大，过于集中的方式带来的潜在业务故障风险显著放大。虽然网络设备及组网设计上都采取了冗余的方式，但是一旦出现极端的全面阻断故障，则面临着怎样在短时内大业务量疏导的棘手问题，如果处理不及时或效果不佳，将引发严重的用户投诉，影响网络业务及口碑。在此类极端故障下，如何做好移动业务出口所承载大流量业务的有效疏导是网络维护人员需要认真思索的问题。

3 移动业务出口容灾方案研究

针对移动数据业务出口的极端全阻情况下的业务疏导，可采用SAE GW重选、增加备份链路和两种方式叠加使用这三种容灾方式，下面就每种方式做详细的阐述。

3.1 基于SAE GW重定向选择的容灾方式

当SR、防火墙及其以上汇聚节点的全阻故障后，局址内的SAE GW是无法感知业务阻断的，将继续向该业务流方向的数据转发。在此情况下，应当将用户数据业务流量导流到其他SAE GW承载，基于2G/3G业务量占比很小的情况，主要考虑4G用户的业务流量的导流。

4G用户上网流量经过哪台SAE GW是MME通过EPC核心网中DNS的解析来实现的，即根据实际的移动网络拓扑设计。在DNS中按局址、权重、优先级等参数配置解析数据，可实现将业务选择分流输出到网络中不同的SAE GW设备，限于篇幅，在这里对DNS的机制不再做详细描述。当业务全阻后，调整SAE GW的业务承载布局，通过修改DNS配置，删除故障业务流方向的SAE GW数据，不再承载业务。在实施过程中需要注意以下几个方面。

(1)此举措针对准备建立连接的新用户有效，对于已建

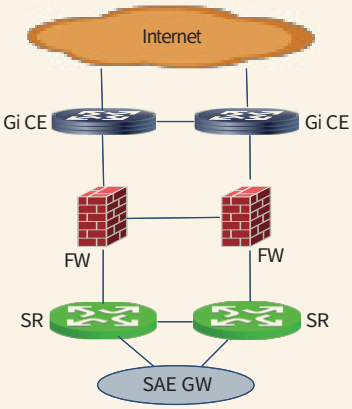


图1　业务出口网络拓扑

立连接的用户无法实现疏导，需要在SAE GW上将已建立连接的用户手工强制卸载下来，用户重新上线时将被疏导到其他SAE GW上。

(2)DNS调整配置生效后，需要在MME上清理原有DNS缓存信息，如果不清理，MME将根据缓存的地址信息，将新用户业务继续送往原SAE GW。

(3)业务流量疏导到其他局址之前，需要提前评估其他局址SAE GW设备业务负荷和链路负荷，以及当前SAE GW卸载业务的频率，防止业务量的突增产生“雪崩”效应。

(4)在日常维护中提前准备好相应调整的DNS应急脚本配置和PGW卸载脚本配置。

此方案的优点是只需通过修改配置即可实现业务流量的疏导，实施简便；缺点是故障后需要人工手动干预，根据业务量的整体变化情况，日常要不断地及时调整脚本配置，操作过程中配置的生效及卸载均需要花费一定的时间，业务疏导时效性稍差。

3.2 基于业务局址间链路备份的容灾方式

此方式是在业务出口的局址间增加冗余备份迂回链路，形成局址间备份。当某一局址的业务出口全阻时，通过冗余备份链路将流量迂回到备份局址（如图2所示）。该方案适用于防火墙之上业务汇聚节点全阻的情况。具体做法是在本局址SR和异局址FW之间增加备用双平面的物理链路，备用链路配置的cost值远大于本局SR和FW之间的主用链路cost值。

采取这种方案时，主要考虑异局址的承载能力，包括带宽和处理能力，防止出现“雪崩”效应，尤其是Gi防火墙，除了承载流量外，还承担用户终端上网过程中私网地址转公网地址的NAT功能，需要评估防火墙的会话处理能力。另外，该方案对于在同一城市的不同局址较为合适，对跨地区的局址不建议采用。在当前移动数据业务量居高不下的情况

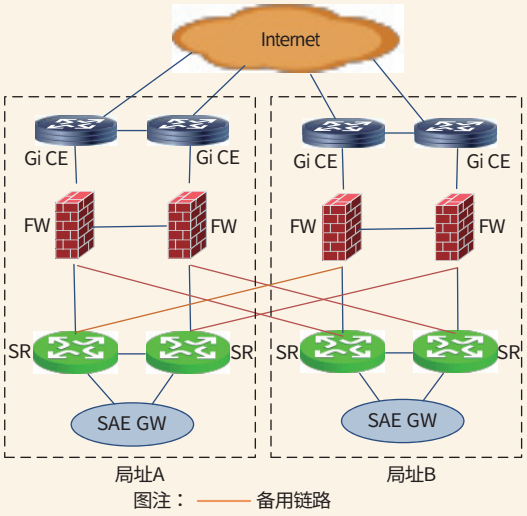


图2　局址间容灾示意

下，让TB级的大流量快速迂回到另一个地区，需要经过多个节点，将会对网络承载带来巨大冲击。

该方案的优点在于出现故障后，数据流根据路由cost值自动迂回到备份局址进行疏导，时效性高；缺点是带来了额外的物理开销，设备的物理端口和传输资源都要增加，增加了网络投资。

3.3 基于以上两种方式叠加的容灾方式

该方案是将上述两种方式同时部署。对于业务流量规模特别集中的大节点，安全平稳的疏导流量是放在第一位的，需要多措并举，在局间备份链路自动迂回的同时，通过DNS数据配置的调整，将部分流量引流到其他业务区域的SAE GW上，这样能够最大程度上做到及时、安全、平稳的疏导，保护用户业务安全的同时保证网络的安全。

4 现网容灾方案实例

现网中洛阳大区共有A局和B局两个核心业务出口局址，局址内业务承载采用负荷分担方式，各局址当前的设计承载能力和利用率见表1、表2。

表1中当前各局址的带宽利用率均没有超过40%，防火墙NAT会话利用率不超过20%，单局承载全部洛阳流量不会超过75%的安全阈值。从表2中可以看出每个局址SAE GW承载的业务量都超过了100万，利用率超过60%，业务集中度高。洛阳业务区整体呈现带宽利用率不高，单SAE GW设备利用率高的特点。当出现业务出口全阻时，采用SAE GW重定向选择的方式，A局址SAE GW是无法承载B局址业务量的，B局址虽然能承载A局址业务，但会造成每台SAE GW

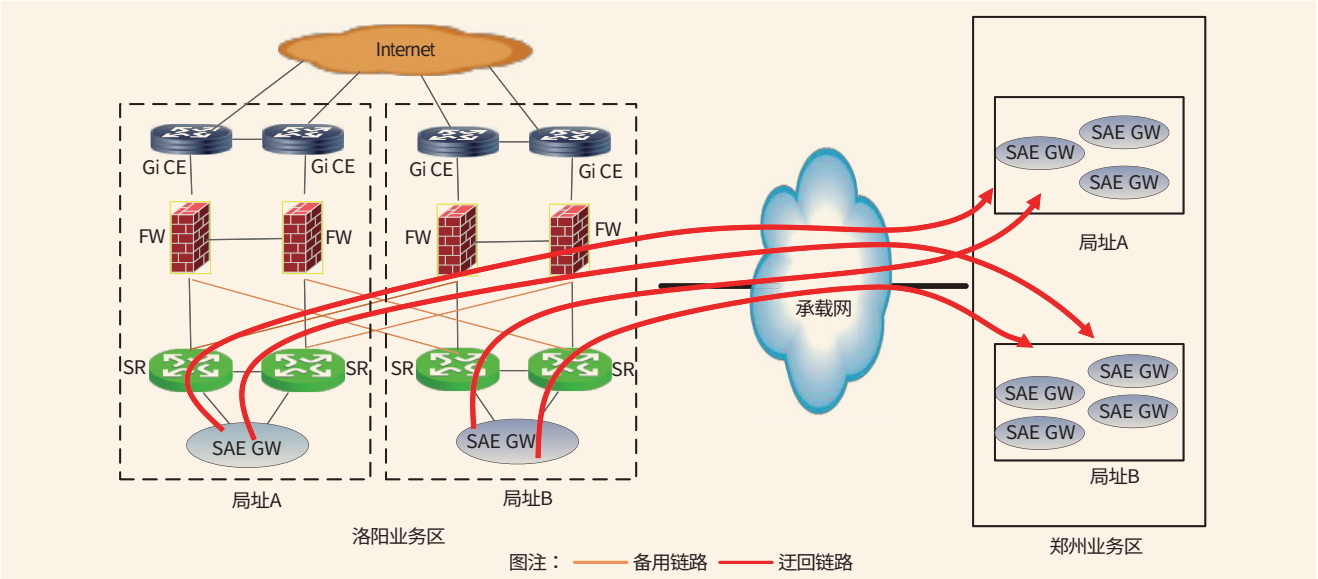


图3　容灾改造示意

表1　链路和NAT利用率

局址	FW—出局链路带宽（GHz）	忙时带宽利用率	NAT会话处理能力（亿）	忙时NAT会话利用率
A	400	21.60%	2	10.2%
B	400	39.70%	2	18.5%

表2　SAEGW利用率

局址	网元	4G 承载（万）	容量（万）	利用率
A	HA_LY_SAEGW14_ZX	122.67	200	61.34%
B	HA_LY_SAEGW15_ZX	125.86	200	62.93%
	HA_LY_SAEGW16_ZX	126.67	200	63.34%

利用率过高（平均利用率将接近90%）的风险。如出现FW以上汇聚节点业务全阻，通过增加局址间备份链路的方式疏导流量效果最好。考虑到业务量的持续增长，综合当前网络的承载，决定采取两种方式叠加使用的容灾方式（如图3所示），具体措施如下。

(1)在局址间各自增加本局SR到备份局FW双平面400GB的备份链路，路由采用P2P模式的OSPF协议，运行区域为area 0。本局SR到FW之间的cost值设为10，本局SR到备份局FW之间的cost值设为50000，根据cost值，无故障时在本局承载，全阻时流量自动选择备份链路疏导到备份局。

(2)准备各局SAE GW流量疏导的DNS脚本，按照流量平均分担的模式，配置中每个SAE GW的权重一样，单局址全阻后洛阳业务引导至郑州大区两个核心局址的7台SAE GW上，由其共同承载；洛阳局址内的每台SAE GW在线用户的卸载频率按照2000户/s执行，基本上在10min内可完成卸载。

5 结束语

移动流量规模增长态势给现有网络容灾能力带来了严峻考验，当前移动上网采用的流量回传到业务出口核心局址的模式造成了业务流量过于集中，文中给出的容灾方案是基于现有的网络架构进行容灾部署。长远来看，集中式的业务部署方式难以满足业务安全的需求，必须通过网络重构，将业务流量分散，比如采用C/U分离，将业务出口下沉到地市级业务出口；采用SDN和NFV技术部署网络，实现业务故障的自动隔离和恢复等，通过新技术的运用提高网络的抗风险能力，实现网络容灾的自动高效实施。

参考文献

[1] 张乐，马洪源，卜忠贵.VoLTE业务中EPC网络容灾方案优化研究[J].电信工程技术与标准化 2018(01)

[2] 郑圣，潘浩.分组域承载网4G回传承载优化[J].电信技术，2017(07)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

孔令义

本科，毕业于西安邮电大学，工程师，从事移动分组网维护优化工作。

郭威

硕士，毕业于解放军信息工程大学，高级工程师，从事移动分组网维护优化工作。

时利鹏

本科，毕业于郑州大学，工程师，从事移动分组网维护与优化工作。

doi:10.3969/j.issn.1000-1247.2018.07.006

对HTTPS加密通信技术的信息安全监管研究

钱　康

中国信息通信研究院安全研究所

摘要　针对采用HTTPS技术进行加密数据传输过程中可能出现的不良信息违规传输问题，文中分析HTTPS通信加密技术的广泛应用给信息安全监管带来的挑战，从技术和管理两个方面提出可行性方案，并阐述技术和管理结合处理不良信息的方案及流程。

关键词　HTTPS　安全监管　技术　管理

1 引言

随着互联网技术的不断发展与广泛应用，用户暴露在互联网上的信息越来越多，为避免信息被窃取，很多网站开始采用HTTPS技术进行加密数据传输，以保障用户的数据安全。这一技术是把双刃剑，同时给不良信息的违规传输带来可乘之机。对此，目前还存在技术瓶颈，无法破解掌握其传输内容，进而给互联网信息安全监管带来难题，必须从技术与管理两个方面研究解决。

2 HTTPS通信加密技术的广泛应用给信息安全监管带来挑战

2.1 HTTPS通信加密技术原理

HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer），是一种加密通信技术，是以安全为目标的HTTP通道，是HTTP的安全版。HTTPS通信加密技术原理如图1所示。

使用HTTPS进行传播，在加密方面具有三个特点:一是数据保密性，保证内容在传输过程中不会被第三方查看到或者窃取；二是数据完整性，及时发现被第三方篡改的传输内容；三是身份校验，保证数据到达用户期望的目的地。采用HTTPS加密通信，在整个传输过程中，数据都是以密文形式传输，第三方即便截取了数据包，也无法破解或掌握其内容，这能够在绝大部分情况下保证互联网访问数据传输的安全。HTTPS通信加密技术过程如图2所示。

2.2 HTTPS加密通信的广泛应用使信息安全监管面临难题

为保护用户数据安全和隐私，国内外各大网站纷纷使用HTTPS加密技术，在国外已经比较普及，全站HTTPS化已成为一种必然的趋势。Google、Facebook、Twitter等公司早已经实现全站HTTPS。浏览器开发商Mozilla、Google准备将所有HTTP网站标记为不安全。在国内，一些大的网站，如百度、淘宝等也全站使用了HTTPS来进行数据信息保护。

然而，技术向来就是一把双刃剑，可以服务社会，也可以被一些人利用来危害社会，HTTPS加密通信技术也是如此。通过HTTPS加密传输通信，用户的数据安全在很大程度上得以保障，但同样也给不良信息的传输带来可乘之机。一些不良信息采取HTTPS加密传输的技术手段，使得监管部门无法解析掌握其传输内容，进而给互联网信息安全监管带来难题。传统的HTTP网页由于是明文传输，遇到问题网页，可以通过相关技术手段处理，防止不良信息在互联网上蔓延传播，但当遇到采用HTTPS加密技术通信的问题，就目前而言，破解还存在技术瓶颈。随着HTTPS全站化在国内外的日益普及，这一问题给信息安全带来的挑战日益严峻。

3 对HTTPS加密通信进行信息安全监管的技术手段研究

加密通信可以通过加密算法极大增加破解所需要的成本，通过外部技术手段破解SSL/TLS握手过程获得密钥进行监管的方法是无法实现的。因此，需要研究在直接得到企业服务器的非对称密钥前提下，是否可以不破坏通信过程而破解加密通信的信息，从而实现利用技术手段监管。这就需要通过对当前主流加密方式进行实验和对比，找出可依循的路径。

3.1 加密方式的选择

通过对HTTPS握手协议过程的研究发现，目前有两种主流的加密方式，分别为ECDHE（前向安全性）与RSA。

ECDHE：满足Forward secrecy或者forward security的公钥环境下的（签名、密钥交换或加密）方案，其公钥是固定的，而密钥则随着时间进行更新。这个更新过程是单向的，因此也就保证了即使拿到当前的密钥，也无法恢复以前的密钥，从而保证了“前向安全”。

RSA：是目前最有影响力和最常用的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被国际标准化组织（ISO）推荐为公钥数据加密标准。但在分布式计算和量子计算机理论日趋成熟的今天，RSA加密安全性受到了挑战和质疑。

与RSA比较，ECDHE的加密方式具有前向安全性，安全级别更高，是将来HTTP服务器选择加密方式的趋势。

因此，分别对这两种加密方式进行实验并对比。实验设计流程如图3所示。

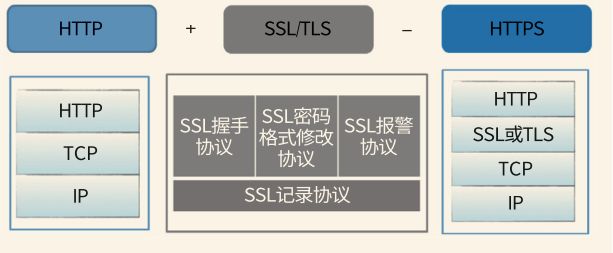


图1　HTTPS通信加密技术原理

3.2 选择RSA加密方式实验

访问测试网址，确定能访问，则该网址已经具备HTTPS条件。

解密SSL流量。

(1)导出私钥，将证书导出。

(2)进行wireshark设置，打开wireshark，edit→preferences→protocols→ssl，选择RSA keys list Edit，选择NEW，将服务器IP地址等输入，并将导出的server.pfx导入。

录包并解密流量，还原得到全部明文信息。

3.3 选择ECDHE加密方式实验

修改/etc/nginx/nginx.conf文件，将ssl_ciphers "AES128-SHA"替换为ssl_ciphers HIGH:!aNULL:!MD5；再使用wireshark录制访问测试网址的流量。

经follow TCP显示，依然是加密内容，无法解密。

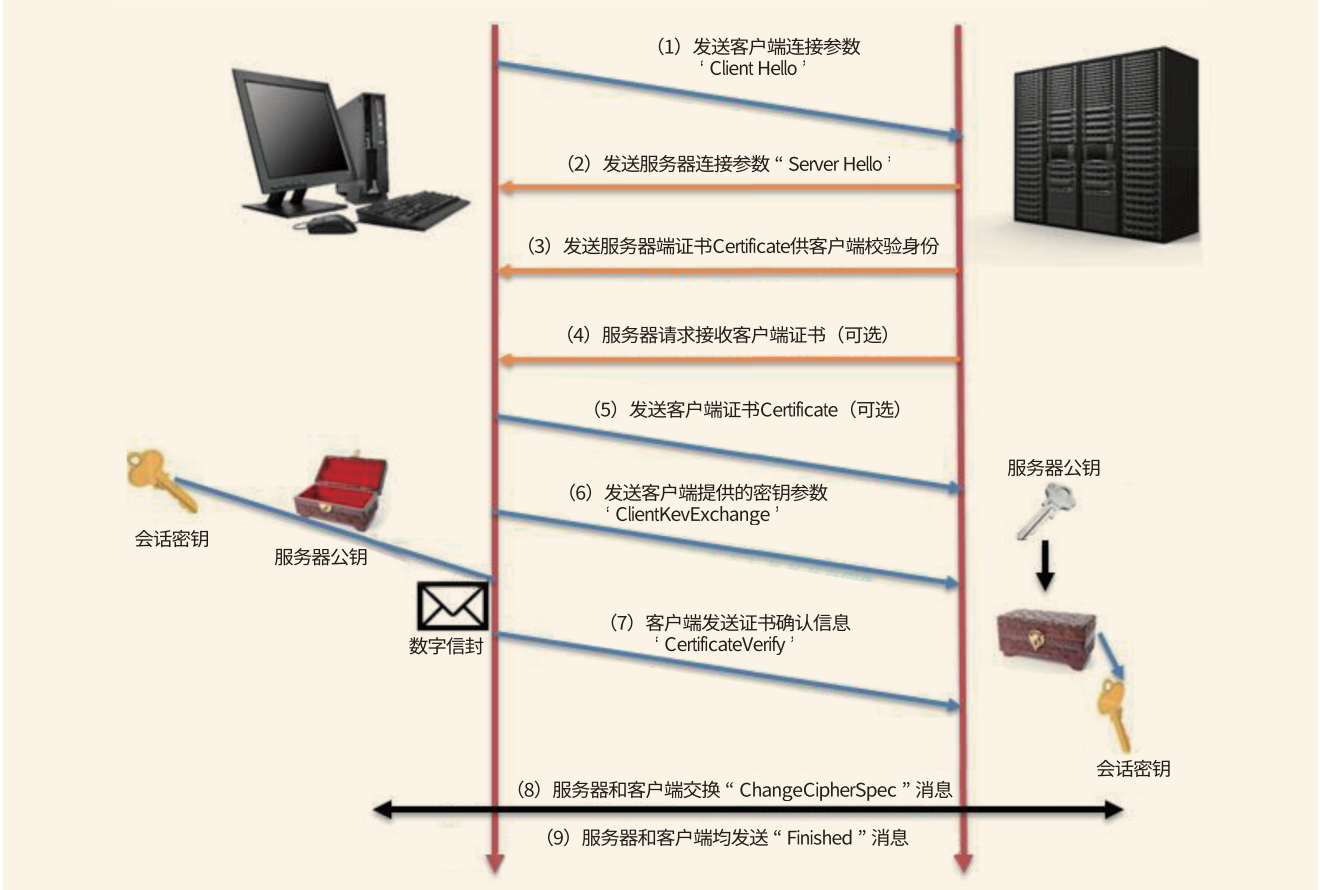


图2　HTTPS通信加密技术过程

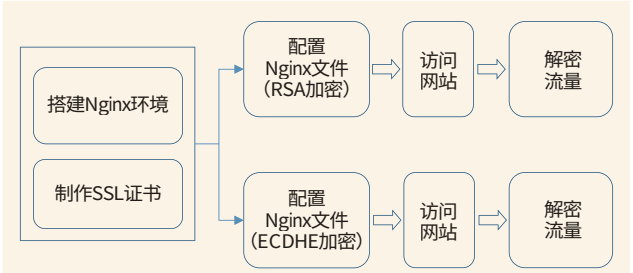


图3　实验设计流程

3.4 实验结果

对比两次捕包，会发现第一次服务器选择的加密方式是RSA，这种类型的加密方式，在掌握服务器私钥的情况下能够实时解密SSL的流量，并还原得到全部明文信息。第二次服务器选择的加密方式是ECDHE，这种加密方式有前向安全性，即使拥有服务器私钥也无法解开。而目前nginx这些主流的HTTP服务程序均默认打开ECDHE这种加密方式。

4 对HTTPS加密通信信息安全监管的分析与对策

4.1 加密通信信息安全监管的路径分析

通过以上研究，可以得出加密通信信息安全监管需要具备如下两个前提。

前提一：采取与企业协商等方式，得到企业网站与用户通信时使用的非对称密钥，之后通过截获HTTPS网站的握手协议得到加密密钥。

前提二：假设企业网站未使用前向安全性加密算法。

若要解密在加密通信传递的信息内容，以上两个前提条件缺一不可。但是在实际情况中，以上两个前提都很难满足。首先，企业采用HTTPS是为了保护用户隐私安全和通信数据安全，一旦密钥泄露，信息安全无从谈起，实际工作中企业不可能提供非对称密钥。其次，目前主流HTTPS服务程序均默认打开ECDHE加密方式，且是今后HTTPS发展趋势。所以，即便获得非对称密钥，对ECDHE加密也无法解密。

由上可见，在实际应用中，解密的两个前提条件都很难满足。因此，HTTPS加密通信时，无法以第三方单纯通过数据解密技术手段进行信息安全监管，对其进行信息安全监管的路径，除了极端情况外，只能通过与企业/网站合作的联合处置的方式。

4.2 加密通信信息安全监管的可行路径

目前，互联网、移动互联网越来越是一个服务交易的闭环链，这意味着用户对技术的依赖度日益提升，需要一个更安全的网络承载环境，因此，HTTPS加密通信不仅应用越来越广泛，而且技术也在不断升级。这就要求在信息安全监管中，加强技术手段与协调管理，实行技管结合，联合处置。可行的信息安全监管手段包括两个：一是应急情况下，直接对使用HTTPS的网站停止域名解析，实现全站应急处理；二是日常情况下，通过与企业建立互信管理机制，采用技管结合的方式处理不良信息。技管结合处理不良信息流程如图4所示。

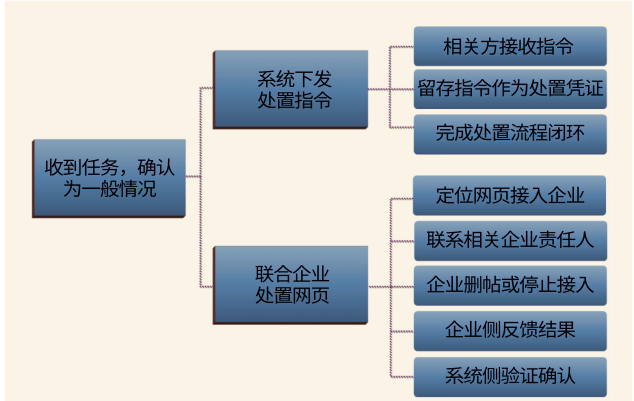


图4　技管结合处理不良信息流程

(1)应急情况。应急情况的全站处理适用于以下情况：展示不良信息的恶意网站，包含涉政类、邪教类、色情类网站，以及内容被篡改的小型网站，包含部分政府网站、企业网站等。

(2)日常情况。技管结合的方式适用于如下情况：监测发现存在违规网页的大型网站，例如百度贴吧、新浪微博等。接入企业/网站本身具备信息安全监管和处置能力的，可根据通过技术手段接收到的指令，按行业主管部门要求及时处置不良信息网页。

HTTPS技术与应用的特殊性，决定了HTTPS加密通信监管必须与企业及网站联合实施，因此，要建立信息安全技管结合管理机制。要加强沟通、协调与管理，建立监管部门与接入企业及网站的信息安全互信管理机制和制度规范，联合处理不良信息，使HTTPS加密通信信息安全管理有效、规范和制度化。

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

doi:10.3969/j.issn.1000-1247.2018.07.007

视频业务暴增对中国联通分组域的影响研究

周新荣　何力毅　徐大伟
中讯邮电咨询设计院有限公司

摘要　随着4G业务的快速发展，尤其是近期中国联通大力发展2I2C、冰激凌套餐、畅视等业务，数据流量爆发性增长，导致现有的分组域承载网络出现瓶颈，严重制约业务的发展。文中分析现有网络的结构及存在的弊端，提出网络扁平化、简约化的方案，为未来中国联通网络结构的调整提供技术支持。

关键词　4G　数据流量　分组域　扁平化

1 引言

2018年上半年，中国联通大力推广2I2C业务，与互联网企业腾讯、阿里分别合作推出腾讯大王卡、蚂蚁宝卡，对定向流量给予优惠；全国正在推广的冰激凌套餐，对所有业务不限流量。还有近期推出的畅视业务，对沃视频、乐视、优酷等签约视频客户端观看标清视频免流量费。这些业务的开展带来的结果就是流量爆发性增长，尤其以视频业务为主，对网络的冲击非常大，现有承载网络的结构已经严重影响业务的发展。

因此，针对目前中国联通市场对于流量经营的策略，有必要重新构建分组域承载网络的架构，为后期业务的发展奠定基础。

2 现有承载网络结构及业务分析

以某运营商分组承载网络为例进行分析，分组域承载网分为接入层、汇聚层和骨干层。目前分组域核心网设备主要集中设置在省会的几个机房，省会设置一对汇聚DCE，每个机房设置一对接入Gn ACE，汇聚DCE与IP承载B网AR对接。接入层主要传输IP RAN设备，对接无线设备；汇聚层主要是各地市的本地承载网，每个机房设置一对接入ACE，同时每个本地网设置一对汇聚DCE，DCE上行与IP承载B网对接，下行与IP RAN对接；骨干层主要是指IP承载B网，每个地市设置有一对AR设备，全省一对BR，连接本地和省会。

对于2G/3G网络，各本地网设置在本地核心机房的BSC/RNC经本地承载ACE，通过汇聚DCE经IP承载B网送至省会；对于4G网络，本地接入层无线网eNodeB通过分组传送网到地市核心机房的IP RAN汇聚设备RSG，通过本地承载网的汇聚DCE经IP承载B网送到省会分组域核心层；分组域的出口均设置在省会，通过169网访问互联网。

现有承载网架构如图1所示。从目前的网络架构来看，2G/3G/4G流量的回传均需要通过本地承载网和IP承载B网，在单用户流量模型小时，对承载网的压力不明显。对于2G网络用户来说，由于本身速率的原因，流量不大，而且模型比较稳定，单用户基本保持在0.5～0.7kbit/s。对于3G网络用户来说，速率要快于2G，但很有限，单用户基本在5～8kbit/s。对于4G网络用户来说，速率最快，流量占比最高，单用户流量基本在12～15kbit/s。但随着2I2C业务、不限流量业务的开展，4G由于速率优势，流量增长迅猛，单用户模型不断提高，导致承载网络压力越来越大，主要问题在于网络层级过多，投资浪费，效率低下。因此承载网络架构的调整势在必行，否则承载网络将影响业务的发展。

2B2I用户对4G流量贡献明显，以月均5%增幅攀升，2017年6月在4G中流量占比已接近60%，其中腾讯王卡用户属于2B2I主力，用户占比及流量占比均突破80%。

统计近一年单用户数据流量和用户速率情况，整体趋势是不断增长。

单用户模型增长和流量增长基本是从2I2C业务和不限流量业务推出后开始的，而且增长速度很快。其中4G单用户模型一年时间增长1.9倍，4G流量增长4.45倍，流量增长的倍数要远大于单用户模型增长，主要是因为网络侧对4G业务的开放，只要终端支持4G，就能用4G网络。因此随着后续市场策略的调整，如2G网络退网，势必造成大量的用户向4G网络迁移，增加对承载网络的压力。

3 承载网络调整方案

目前承载网络存在的问题如下。

端到端层级多，端到端业务流多自治域且多跳，业务承载效率较低：4个自治域，每个自治域至少2层，最多达到10

跳（UTN 3层3跳+本地CE 2层2跳+B网骨干2层3跳+本地CE 2层2跳）；如果是漫游用户会更甚之。

背靠背端口资源浪费：UTN核心、地市AR、本地汇聚CE端口都需要扩容，投资浪费。

承载网络的演进目标是扁平化，其中IP承载B网只保留核心汇聚设备，原有的本地AR融入本地承载网/UTN。承载网演进目标如图2所示。

本地：UTN、本地汇聚CE及原IP承载B网AR，融合成一张本地承载网/UTN三层架构（接入+汇聚+核心）。

调整后的网络优点如下。

端到端层级减少：3个自治域，5跳（本地承载网3跳+B网骨干1跳+本地承载网1跳）。

背靠背端口资源减少：原UTN核心、地市AR、本地汇聚CE融为1对出口设备。

调整后端到端的网络结构如图3所示。

考虑到骨干网采购周期长，调整比较缓慢，本地承载网络融合也非一蹴而就，涉及多专业、多部门，整合力度大。因此流量回传可以采用过渡方案，即为了满足目前流量爆发性增长的需要，可以通过本地网IP RAN的汇聚设备RSG，通过传输直连省会分组域汇聚DCE。这样既解决IP承载网带宽受限的瓶颈，同时能缓解IP承载B网扩容压力，节省投资。4G回传过渡方案如图4所示。

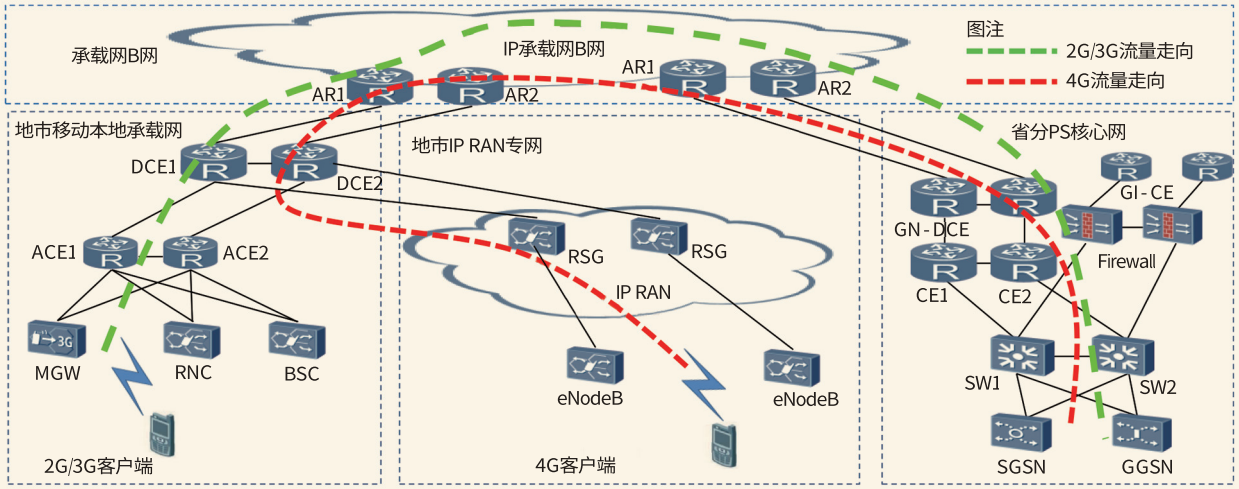


图1　现有承载网网络架构

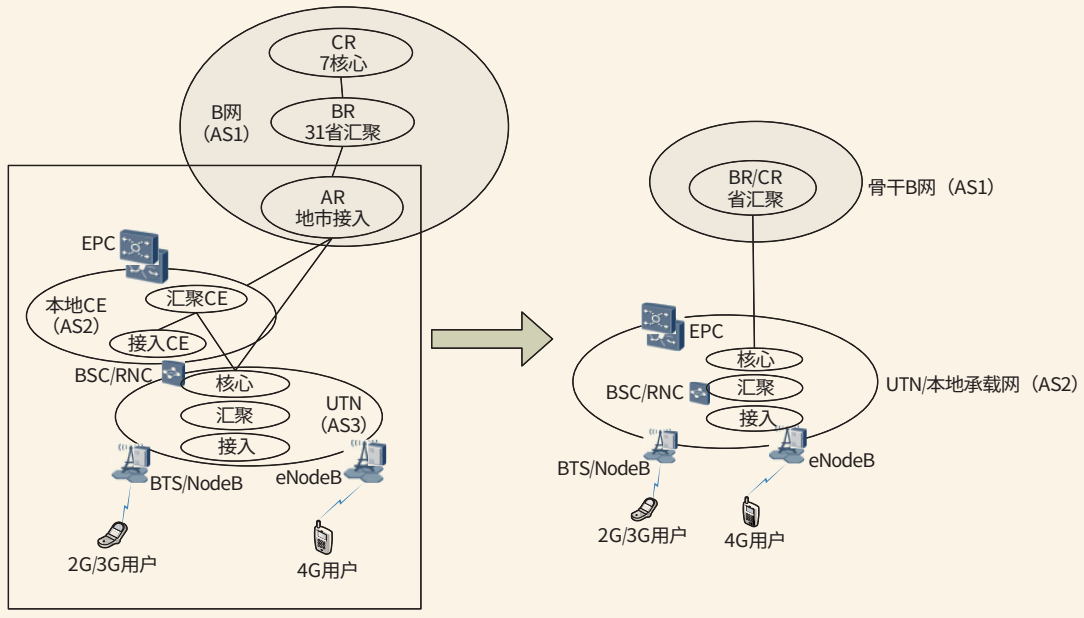


图2　承载网演进目标

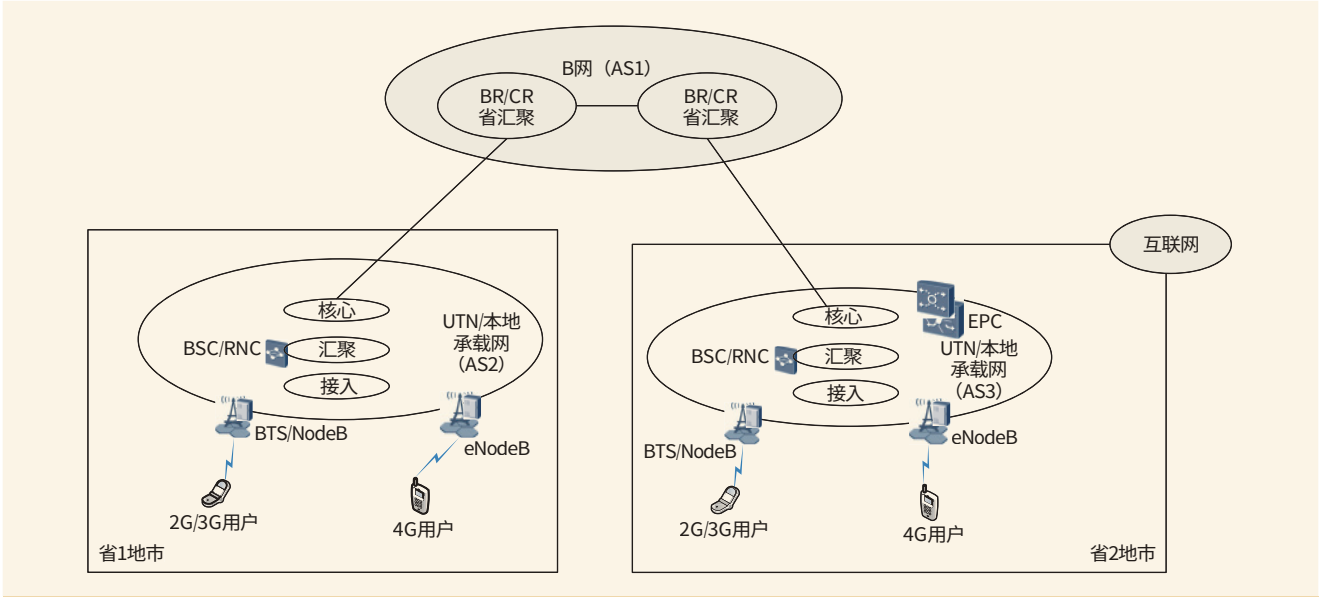


图3　端到端的网络结构

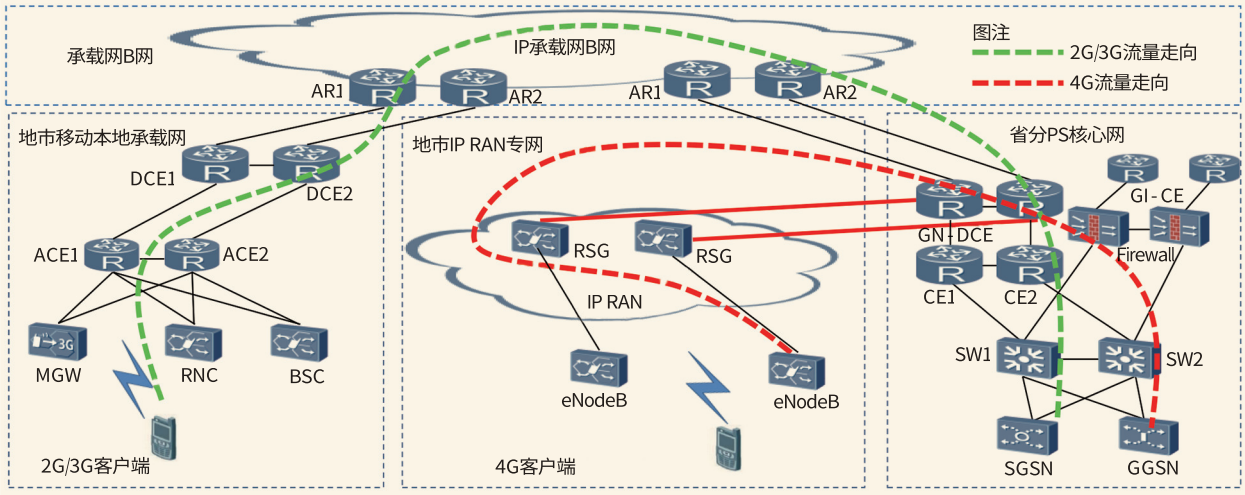


图4　4G回传过渡方案

4　分组域设备调整方案

目前分组域核心设备均集中在省会城市，所有流量均需回传到省会，再从省会去访问互联网。流量小时，对承载网和出口带宽需求也小，这时网络结构看起来是合理的。但当流量大到一定程度时，承载网就会成为业务发展的瓶颈，同时由于流量迂回比较严重，会影响用户的使用感知。

因此当某些用户规模比较大的城市的流量达到某个值时，就可以考虑用户面GGSN下沉，而这个值的取定要综合考虑多方面的因素，如承载网的扩容投资、传输的扩容投资、下沉的投资（包括机房相关配套、数据通信设备等）。如果下沉明显能够节省投资，同时也能更好地满足业务发展，则GGSN下沉是很有必要的。GGSN下沉至169骨干节点与非169骨干节点拓扑分别如图5、图6所示。

对于169骨干节点城市，用户流量出口经GGSN可以从本地直接访问互联网，这对用户的使用体验很有帮助，尤其是对一些时延要求比较高的业务。

GGSN的下沉能够有效缩短用户到互联网的距离，提升用户数据使用感知，可节省承载网的投资。同时GGSN的下沉使视频CDN也要考虑下沉，这可以缓解城域网和169网络的扩容压力。

随着网络的演进，分组域的发展目标是虚拟化并CU分离。因此，随着产品的成熟，分组域GW可以考虑采用CU分离的架构进行建设，C面集中部署的省会或大区，U面下沉地

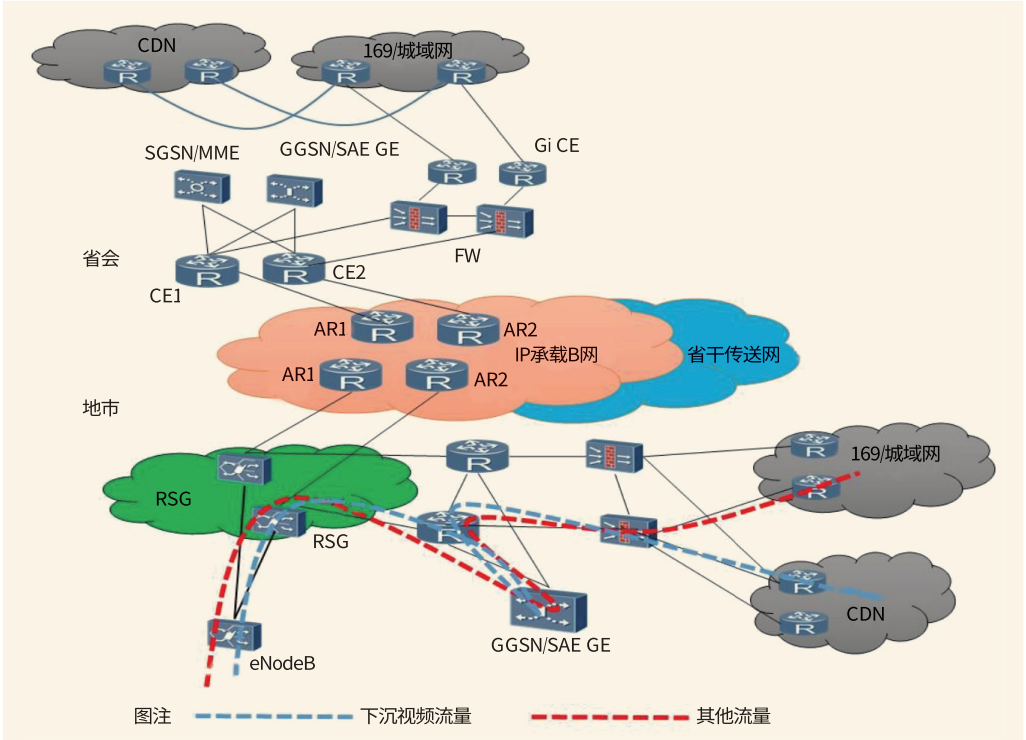


图5　GGSN下沉至169骨干节点拓扑

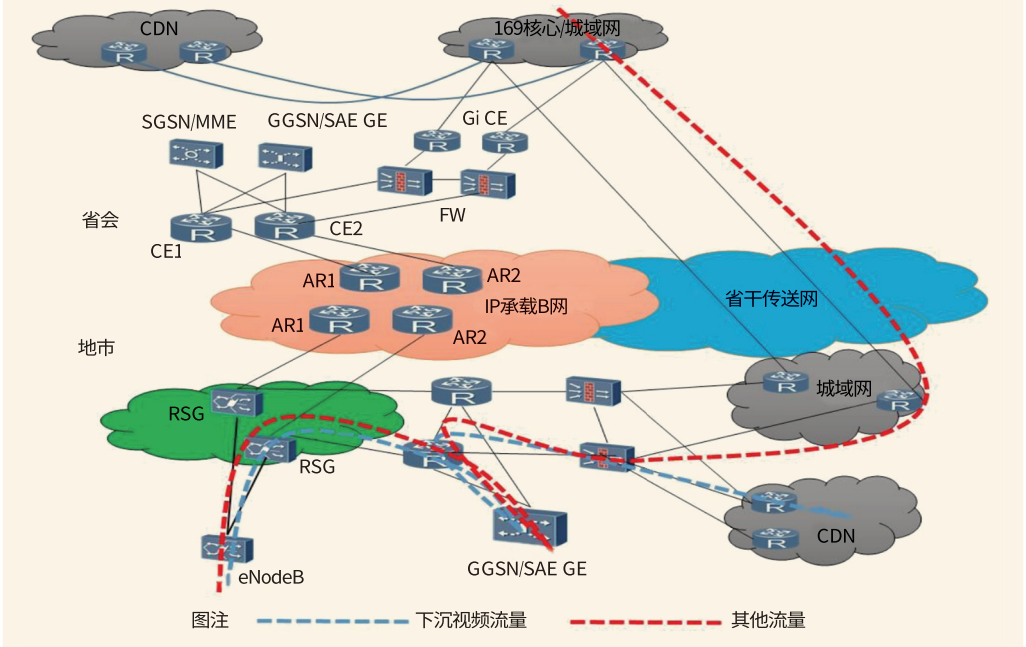


图6　GGSN下沉至非169骨干节点拓扑

市，与GGSN下沉的思路基本一致。

(1)按照网关的控制面和用户面分离原则：SGW拆分成SGW-C和SGW-U，PGW拆分成PGW-C和PGW-U。

(2)S5/S8逻辑接口按照控制面和用户面分离的原则，拆分成S5/8-C和S5/8-U接口。

(3)SGW-C和PGW-C合一部署呈现控制面网关，SGW-U和PGW-U合一部署呈现用户面网关。

(4)控制面网关统一信令接口，简化网络部署。

(5)用户面网关部署到城域，甚至更低，缩短业务访问路径，提升用户业务体验。

虚拟化并CU分离架构未来是可以向5G演进的，既可以满足目前业务发展的需求，同时也可以通过简单升级支持5G，符合网络的发展目标。

5　结束语

分组域是运营商未来网络的发展重点，尤其是视频等大数据流量业务，对网络的冲击很大。提前做好网络规划，适当调整网络结构，对业务的发展以及未来网络的演进是非常有必要的。

因此，不管是承载网络的调整还是GW的下沉，都是为业务服务，同时也能节省投资，提升用户使用感知，增强企业的竞争力。ttm

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

周新荣

硕士，毕业于南京邮电大学，工程师，现就职于中讯邮电咨询设计院有限公司，主要从事核心网规划设计工作。

doi:10.3969/j.issn.1000-1247.2018.07.008

基于电信级5G URLLC短时延平台的车联网应用研究

董　涛　张志华
中国电信股份有限公司江苏分公司

摘要　对毫秒级时延保障、网络安全问题、硬切换问题及车辆对于未来几秒路况预判得不到保障等车联网现状进行分析，从多维度提出5G URLLC车联网应用具体解决方案，降低时延，提高安全性与可靠性。

关键词　5G　URLLC　车联网

1 前言

车联网为了实现低时延与高可靠性，需要将时延控制在10ms以内，在实现车联网业务时，发现需要解决毫秒级时延保障性、网络安全问题、硬切换问题及路况预判保障这4大技术问题，而利用URLLC（Ultra Reliable & Low Latency Communication，超高可靠超低时延通信）短时延平台来进行调度与控制，可以很好地解决车联网的需求，因此，URLLC与短时延平台结合是未来URLLC走向成熟的必然趋势。

2 现状问题分析

(1)毫秒级时延保障：网络层级增加，耗费宝贵的时间，增加时延

现有网络属于多级网络架构，多级串行节点造成信息延迟增加，难以满足车联网对于时延的苛刻要求。以苏州电信为例，全市共设4个IDC（Internet Data Center，互联网数据中心）机房，而BBU节点（1~3个基站的汇聚节点）超过2000个，从IDC机房到汇聚节点机房传输路由会经过很多迂回，信息传递需要数十毫秒的时延，无法满足低时延业务要求。多级串行节点示意如图1所示。

(2)网路安全问题

网络安全性风险主要来源于网络故障和黑客攻击两个方面。

网络故障：一旦网络核心节点（包括核心网、车联网云平台）发生故障，将造成非常大的安全事故。

黑客攻击：对车联网的攻击，可以让车辆变成自杀工具；对车辆APP的攻击，使自动驾驶服务得不到保障。

(3)硬切换的问题

目前4G网络以及R15中定义的5G网络切换策略是硬切换，切换特点是先断开后连接，在基站边缘会引入时延抖动，甚至引起不确定的大时延，降低稳定性，增加时延，甚至失败。如果此时系统恰好对车辆做出刹车或拐弯等紧要指令，则网络可能无法满足要求，对行车安全造成隐患。

(4)车辆对于未来几秒路况预判得不到保障

在无人驾驶场景中，需要对未来几秒的路况进行准确判断识别，确保行车的安全与准确性。虽然无人驾驶车辆配有3D雷达，但在拐弯、天气恶劣的情况下，雷达可能出现失效情况，而且当前面车辆突然刹车时，后面几排车辆雷达可能出现探测不到的情况。因此，利用广覆盖的车联系统，通过V2V（Vehicle-to-Vehicle communication，车与车通信）、V2X（Vehicle-to-X communication，车与其他通信），可以大大提高预判的准确性。

但在现有车联网方案设计当中，高清地图及路况信息需要车辆直接与云平台进行获取。以苏州为例，如有5000辆网联汽车同时运行，每辆车并发进行高清地图增量实时更新，空中接口速率需达到100Mbit/s/辆，云平台服务器出口带宽将达到500Gbit/s；若使用5台云平台服务器，那么，每个服务器出口带宽将达到100Gbit/s，这将会导致网络拥塞，时延增大；而且如处于BBU边界，时延将更大，无法及时下载所需高清地图。未来几秒路况预判问题如图2所示。

3 5G URLLC车联网应用具体解决方案

为了推进R16协议的完善，针对车联网应用存在的4大问题，江苏电信在苏州建设了11个基站的外场试验网络，与设备厂商、行业应用专家一起，反复探讨最终具体的针对性的解决方案。

(1)利用IDC机房的扁平化充分实现毫秒级时延保障性。

(2)建立电信级URLLC低时延平台解决网络安全性问题。

(3)将切换方式从硬切换改为软切换解决硬切换中断的问题。

(4)信息源从中心化到区块化实现未来路况的预判保障。

3.1 彻底扁平化的低时延云平台架构

仍以苏州电信为例，利用5G无线基站虚拟化，即CU（Centralized Unit，集中单元）、DU（Distributed Unit，分布单元）分离，将BBU（1～3个基站汇聚点）的CU部分作为URLLC低时延云平台硬件。基于BBU通用的x86服务器形成微型IDC机房，将4个IDC机房的低时延业务客户端充分下沉至2000多个BBU汇聚点组成微型IDC机房，使得低时延云平台变成IDC机房中的“云”和BBU机房中“雾”的结合体，让每个低时延终端充分得到“雨露”的滋润。

IDC服务器充分下沉，使得传输的层级一步到位，终端和BBU之间只存在空中传播距离，毫秒级时延可以真正得到保障。低时延平台和BBU合二为一，维护工作量和机房的空间都可以大大节省。各种应用的服务器端可以放在4个IDC机房内，各种应用的APP/客户端放在微型IDC内。由于IDC充分下沉，使得客户端本地计算和决策成为可能，90%决策链不通过传统IDC的服务器端，而是直接在BBU客户端完成，从而保障毫秒级低时延。BBU机房变身微型IDC机房示意如图3所示。

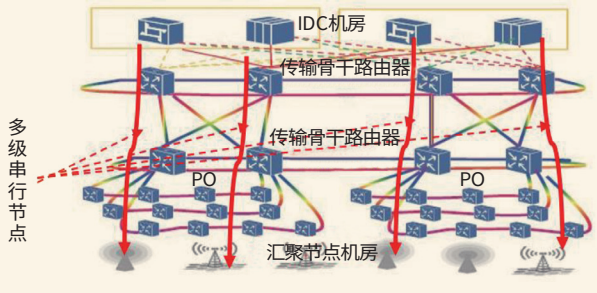


图1　多级串行节点示意

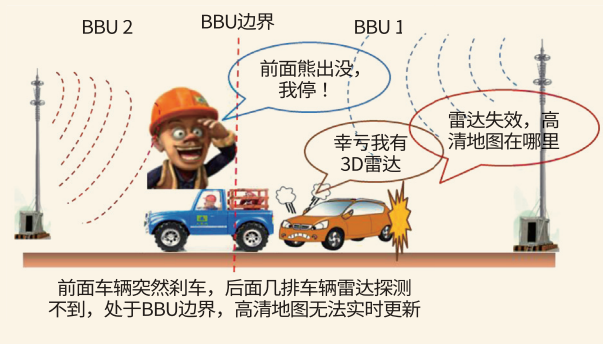


图2　未来几秒路况预判问题

3.2 提供电信级URLLC低时延平台

将传统基站的设备变为IDC的服务器，然后对第三方应用开放，由于基站设备CU是电信级的网元，网络攻击的安全性由运营商来保障。

本地鉴权：充分利用低时延业务客户端存储在BBU机房的特点，核心网或云端服务宕机时，能够在本地客户端上进行鉴权或者通过存储在其他BBU机房的客户端获取用户的鉴权信息，使之能够正常工作。

黑客问题：URLLC低时延云是由运营商提供的私有云，不是在传统的IDC机房内，而是附着在下层BBU网元上，不对外部公众开放，黑客很难通过外网攻击控制客户端的操作。

同时，CU变为未来的低时延云平台，对第三方应用开放接口，类似于淘宝平台对接各种低时延业务的客户端，节省了硬件资源。

3.3 硬切换中断问题解决

5G切换空中接口时延为毫秒级，硬切换时若存在干扰将导致误码率增大，从而引起切换失败，网络可靠性降低。因此对于车联网此类URLLC应用，硬切换方式无法满足毫秒级业务时延及高可靠性要求。

在基站侧采用软切换方式，当车辆进入两个基站覆盖交界位置处时，可同时接收两个站点的信号，实现基站间的联合传输，改善时延，同时提高可靠性。手机可以通过使用不同的码同时对两个小区的下行信号进行解码，故在与新小区建链的过程中还可同时接收原小区的下行信号，建议联合3GPP成员单位在R16中对移动性做进一步增强，提升切换过程的可靠性并且缩短切换导致的中断。软切换实现机制示意及软切换信令流程如图4所示。

3.4 未来路况信息预判问题解决

为了解决前面提到的网络拥塞问题，建议引入Xn接口，共享邻近基站数据。同时，对于同一基站内的数据，实

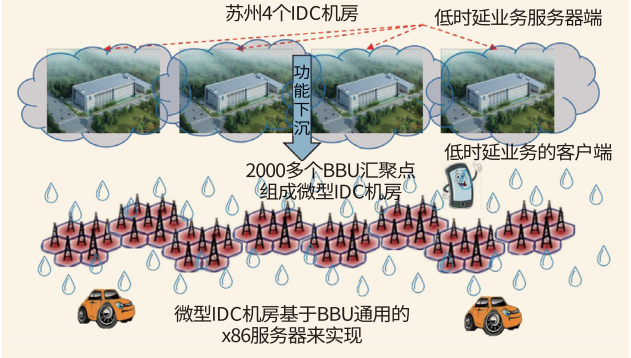


图3　BBU机房变身微型IDC机房示意

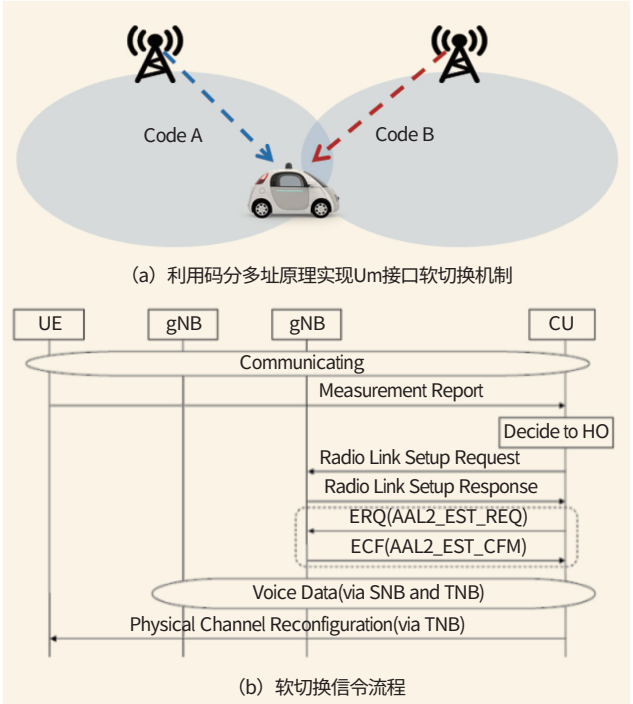


图4　软切换实现机制及软切换信令流程

现在本地BBU内进行车辆间的交互。以上功能基于车联网客户端APP应用功能实现，网络仅提供数据交互路由。

即使BBU的本地客户端可以存储BBU内部车辆的高清地图，在BBU的切换边界，如果两辆车分属不同的BBU，地图的共享需要在云平台进行中转，增加很大的时延。

为了降低车联网云平台服务瓶颈，创新性提出利用Xn接口传输高清地图数据，并联合3GPP成员单位推动Xn接口标准化，从而使得两个或多个BBU间通道可以数据共享，降低获取邻近路况高清地图的时延。

基于Xn接口打通BBU间数据通道如图5所示。BBU1通过向BBU2发送Xn Data Transfer Request消息发起该流程，BBU2用Xn Data Transfer Response消息应答。Xn接口建立后，BBU1和BBU2之间建立数据通道，低时延APP客户端可以完成高清地图数据共享。

本地基站可以提供车联网APP接口，使得车联网APP通过Xn接口在多个基站间进行数据共享，增量同步。对于同一个BBU内的车辆间地图数据共享，可由BBU内低时延APP客户端进行地图信息关联，无需云平台参与。基于Xn接口的BBU资源共享示意如图6所示。

4　结束语

通过构建统一的电信级低时延云平台，应用客户端直接部署在BBU侧的CU（BBU的x86通用硬件部分）上，使得

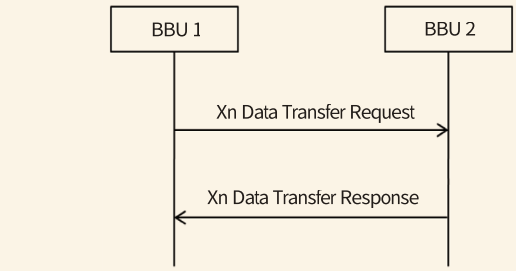


图5　基于Xn接口打通BBU间数据通道

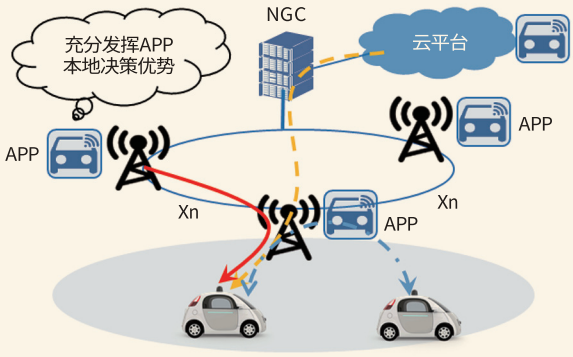


图6　基于Xn接口的BBU资源共享示意

用户与客户端之间的距离最近，本地决策、本地计算成为可能，数据业务路由效率更高，毫秒级低时延得以保障。同时提供电信级网络安全保障，防止黑客攻击及网络故障带来的业务无法使用的风险，可靠性更高。

通过打造开放、开源的平台，为企业提供统一的API，企业用户可以将客户端APP部署在该平台上，除了车联网，还可广泛应用于无人挖掘机、远程机器人排爆及远程AR/VR手术操作等低时延业务，减少行业用户低时延业务平台搭建的软硬件及维护成本。

参考文献

[1] 朱红梅,林奕琳,刘洁.5G URLLC标准、关键技术及网络架构的研究[J].移动通信,2017(17)

[2] Afif Osseiran,Jose F.Monserrat,Patrick Marsch.5G移动无线通信技术[M].陈明,缪庆育,刘愔译.北京:人民邮电出版社,2017

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

董涛

硕士，现就职于中国电信股份有限公司江苏分公司。

张志华

博士，现就职于中国电信股份有限公司江苏分公司。

doi:10.3969/j.issn.1000-1247.2018.07.009

基于垃圾短信发往方向、频次及流量的大数据相关性分析

秦保根[1]　秦　政[2]
1.中国联合网络通信有限公司江西省分公司
2.华南理工大学

摘要　垃圾短信纷繁多样，给电信运营商的拦截带来极大的困扰，通过基于短信发往的所属本地网方向、频次及流量的垃圾短信大数据相关性分析，可解决这一难题。

关键词　垃圾短信　大数据　相关性分析

1 前言

相关资料显示，仅有0.7%以下的用户表示没有收到过垃圾短信，用户每周平均收到的垃圾短信数量为12条。此外，电信运营商每月退网用户中垃圾短信用户占近一半，并造成大量欠费，尤其是后付费用户漫游异地后，其话单记录需要经过一定时间，方能向其归属地发回账单，造成欠费。因此，依法治理垃圾短信，是促进社会主义政治文明及精神文明建设、构建和谐社会、净化社会环境、打击违法犯罪的必然需要，是保障人民群众合法权益的根本。

垃圾短信诈骗和传播违法短信等活动日益猖獗，主要表现如下：

- 假借银行或银联名义发送手机违法短信进行诈骗或者敲诈勒索公私财物；
- 散布淫秽、色情、赌博、暴力、凶杀、恐怖内容或者教唆犯罪、传授犯罪方法；
- 非法销售枪支、弹药、爆炸物、走私车、毒品、迷魂药、淫秽物品、假钞、假发票或者犯罪所得赃物；
- 发布假中奖、假婚介、假招聘，或者引诱、介绍他人卖淫嫖娼的内容；
- 多次发送干扰他人正常生活的，以及含有其他违反宪法、法律、行政法规禁止性规定的内容；
- 极少数境内外敌对势力、敌对分子和对社会心怀不满的人，编造、传播一些明显带有诽谤、煽动性内容的手机违法短信，企图破坏社会稳定。

2 建议的技术方案

2.1 原有垃圾短信防范系统存在的缺点

原有垃圾短信防范系统存在的缺点如下：

- 仅通过对短信关键字进行匹配识别拦截；
- 仅对某一时段超频发送短信的用户进行识别拦截。

以上方式易造成对正常用户的误判，且对垃圾短信的识别量非常有限。

2.2 实施的组网及处理流程

为在公众通信网上，提高垃圾短信判别的准确率，大幅减少垃圾短信的传送，使经济诈骗、垃圾广告、不法短信传播得到及时的甄别堵截，提出如下垃圾短信拦截方案。

垃圾短信判别系统组网示意如图1所示，判断可疑垃圾短信的流程如图2所示。

3 实施的主要步骤

首先定义“可疑短信接收方向”是指：在某一时间段内，A地某一电信运营商发往异地本地网（Bn地）的短信数量X，若大于或接近其发往所在地（A地）的本地网短信数量Y，则该异地本地网（Bn地）称为“可疑短信接收方向”，“可疑短信接收方向”（Bn地）可能同时存在不止一个，即$n \geq 1$。比如：假设南昌联通（A）发往长沙（B1）、海口（B2）、东莞（B3）所有运营商（中国联通、中国电信及中国移动）的短信数量，大于或接近其发往南昌本地三个

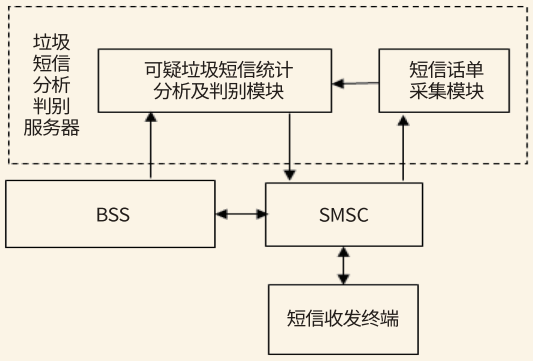


图1　垃圾短信判别系统组网示意

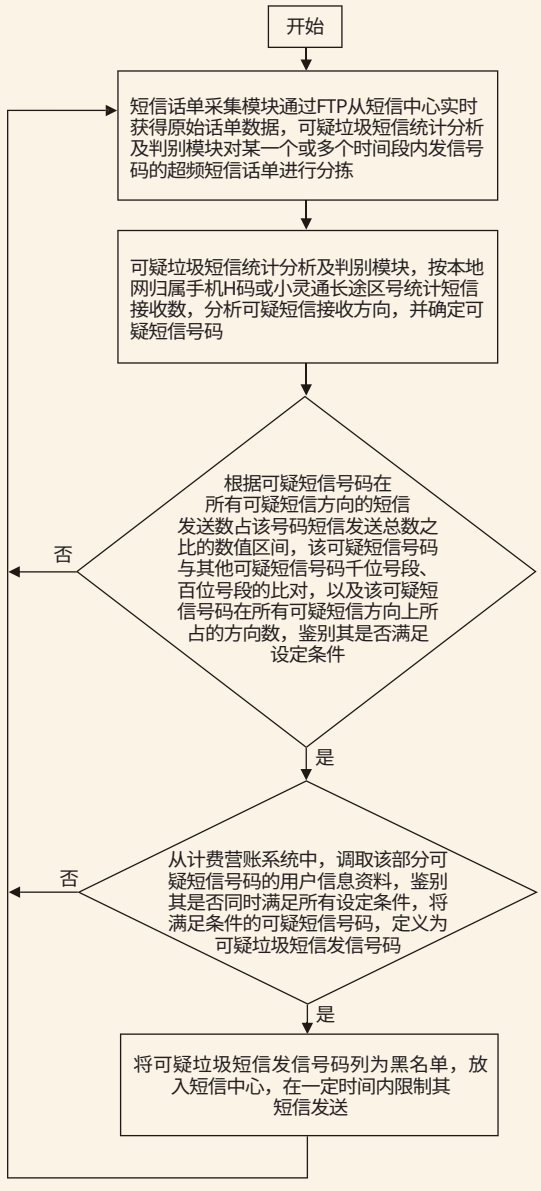


图2　判断可疑垃圾短信的流程

运营商（中国联通、中国电信及中国移动）的短信数量，则长沙、海口、东莞称为“可疑短信接收方向”，具体见表1。

“可疑短信号码”是指可疑短信接收方向的所有发信号码中，剔除电信运营商设定的白名单号码和吉祥号码后的发信号码。

具体来说：参照图1所示的可疑短信判别系统组网示意，按照图2所示的判断可疑垃圾短信的流程，除重大节日：如春节、元宵、端午、中秋、国庆、元旦、五一、圣诞平安、情人节、父亲节、母亲节等外，垃圾短信分析判别服务器的短信话单采集模块，从短信中心采集短信话单，统计分析及判别模块分析某一个或多个时间段内超频发信号码的可疑短信接收方向及其可疑短信号码，对可疑垃圾短信方向发信号码的关联情况进行统计分析，再从计费账务系统中提取该部分发信号码的用户信息资料并进行鉴别，将判定为垃圾短信的号码列为黑名单，放入短信中心限制其短信发送。具体步骤如下。

步骤1：短信话单采集模块通过FTP从短信中心实时获得原始话单数据，对某一或多个时间段内（如每日8:00−12:00、13:00−17:00、19:00−23:00或按天等）发信号码的超频短信话单（如在设定的某个时间段内超频发送100条以上短信，其他时间段超频发送短信数可以设定为150条等）进行分拣。

步骤2：可疑垃圾短信统计分析及判别模块按本地网归属手机H码或小灵通长途区号统计短信接收数，将短信接收数大于或接近（如：50%以上）发信号码所在本地网的异地本地网（城市）列为可疑短信接收方向。在可疑短信接收方向的发信号码库中，剔除电信运营商设定的白名单号码和吉

表1　可疑短信接收方向分析

主叫→被叫号码	发送数（条）	(A→Bn发送数)/(A→A发送数)
A→B1方向	15644	299%
A→B2方向	6864	131%
A→A方向	5238	100%
A→B3方向	4101	78%
A→B4方向	2382	45%
A→B5方向	1083	21%
A→B6方向	421	8%
A→B7方向	341	7%
A→B8方向	297	6%
A→B9方向	284	5%
A→B10方向	252	5%
A→B11方向	202	4%
A→B12方向	174	3%
…		

表2　垃圾短信发送方向上超频100次以上且占比大于50%的部分号码

垃圾短信发送号码	发送方向	该方向次数	总次数	占比
132****4496	A→B1	156	156	100.00%
132****6304	A→B1	151	151	100.00%
132****7584	A→B1	151	151	100.00%
132****1704	A→B1	150	150	100.00%
132****4919	A→B1	149	149	100.00%
132****7520	A→B1	149	149	100.00%
155****3137	A→B2	190	196	96.94%
155****2867	A→B2	176	182	96.70%
155****2908	A→B2	183	191	95.81%
155****2353	A→B2	181	189	95.77%
155****2835	A→B2	173	181	95.58%
155****2501	A→B2	189	198	95.45%
132****5894	A→B3	125	190	65.79%
132****2140	A→B3	116	177	65.54%
132****5084	A→B3	116	177	65.54%
132****3650	A→B3	124	190	65.26%
132****2644	A→B3	119	183	65.03%
132****0141	A→B3	120	185	64.86%

祥号码后，将剩余部分列为可疑短信号码。

步骤3：分析可疑短信号码在所有可疑短信方向的短信发送数占该号码短信发送总数之比的数值，如该数值大于50%（见表2），则继续步骤4，否则返回到步骤1。

步骤4：从计费营账系统中，调取该部分可疑短信号码的用户信息资料，并进行鉴别，若同时所有设定条件：信用度为0、近期入网（如当月入网）、入网后极少接收短信（如接收短信少于三条）且通话记录极少（剔除电信运营商免费客户号码的通话记录后，通话记录少于三条），则将可疑短信号码定义为可疑垃圾短信号码，并继续步骤5，否则返回到步骤1。

步骤5：将可疑垃圾短信号码列为黑名单，放入短信中心，在一定时间内（如7天或三个月等，根据具体规定设定）限制其短信发送，返回到步骤1。

鉴于部分垃圾短信发送方式越来越隐蔽和狡猾，对于实施以上规则后，仍没有截停的垃圾短信号码，可按照以下规则，予以二次过滤，提高拦截效果。

- 统计用户入网时间至6个月，以捕捉部分开卡时间和开始使用时间差较长的准预付费的“养卡”号码。
- 增加总量控制，加长统计时间，如按4h、6h等区段统计，其累计发送总数量≥电信运营商设定的超频数量，如200条、300条、500条等，按上述步骤3判断分析。
- 对于个别真实的正常新入网用户，在入网后，会以短信方式告知亲朋好友，有可能被识别为垃圾短信用户，可采取对个别已错列黑名单的用户结合营账系统中取得的通话、流量等正常使用行为情况进行复核，一旦出现正常通话和流量，则立即将该号码从黑名单中剔除。
- 电信运营商应将垃圾短信黑名单用户拦截记录提供给客服，便于投诉处理时的查询和解释。

通过以上二次过滤，再次提高垃圾短信的拦截质量和效率，有效率超过99%，目前拦截效果很好。

4 结束语

基于发送方向、频次及流量的垃圾短信大数据相关性分析，通过采集某一个或多个时间段内超频发信号码的可疑短信接收方向、可疑短信号码，对可疑垃圾短信方向发信号码的关联情况进行统计分析，再从计费账务系统中提取该部分发信号码的用户信息资料并进行鉴别，将判定为垃圾短信的号码列为黑名单，放入短信中心限制其短信发送。该方法极大地提高垃圾短信判别的准确率，大幅减少垃圾短信的传送，使经济诈骗、垃圾广告、不法短信传播得到及时的甄别堵截。

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

秦保根

毕业于南京邮电学院，高级工程师，享受国务院特殊津贴，中国联通科技成果评审专家、结算专家、评标专家，现任江西联通高级经理。

秦政

硕士，毕业于华南理工大学。

doi:10.3969/j.issn.1000-1247.2018.07.010

自动重合闸剩余电流保护器在通信电源防雷中的应用

刘裕城[1]　陈荣斌[2]
1.中国电信股份有限公司广东研究院
2.厦门大恒科技有限公司

摘要　分析雷电造成剩余电流保护器误动作的原因和自动重合闸剩余电流保护器的工作原理、性能要求和安全问题，并提出具体的数值要求，通过自动重合闸剩余电流保护器自动重合剩余电流保护器以恢复供电，提高通信系统抵抗雷击的能力，解决无人值守站不能及时恢复设备工作的弊端。

关键词　通信　防雷　通信电源　自动重合闸

1　雷击造成RCD误动作致使电源中断问题

一般的通信电源电路如图1所示，在供电进线端安装剩余电流保护器（RCD），剩余电流保护器主要针对电气设备漏电，对人身安全进行保护，在电源支路安装浪涌保护器，针对雷电侵害进行防护。当雷击发生时，传感器线路会感应出不平衡干扰雷电脉冲电流及差模干扰电流，当差模电流超过RCD动作电流值时，误动就会发生。另外，若通信设备漏电流处在动作临近边界，在雨季容易导致不均衡磁通引起的RCD误动。

雷电流是瞬态电流，可能产生一个脉冲，也可能产生多个脉冲。雷电流通过浪涌保护器F1和F2的电流分别为I1和I2，I1往往不等于I2，会出现差模干扰。当差模干扰值大于RCD剩余电流动作值时，保护器动作，电路断开，通信设备中断工作，需要人工恢复供电。通信局站主要为无人值守，一个地区发生雷击，会造成有的通信局站停电，无法短时恢复通信，因此必须解决这个问题。

2　自动重合闸剩余电流保护器工作原理

自动重合闸是解决RCD误动作造成电源中断问题的有效方法。自动重合闸一般用在高压电力系统，而且取得了非常好的效果。但出于安全考虑，现在还没有在低压民用电力系统中推广使用，中国通信系统近几年开始使用，并且制定了标准：YD/T 2346-2011《通信用自动重合闸剩余电流保护器技术条件》，使用效果明显。

当雷击造成RCD误动作使电路断开时，自动重合闸剩余电流保护器会自动合上开关。由于雷击电流是短暂的，雷击过去后I1≈I2，合闸成功，电路恢复供电，通信恢复。

自动重合闸是有条件的，必须考虑安全等因素。自动重合有两种方法，一种是检测漏电流情况，决定是否重合；另一种是不检测，自动重合。

自动检测L-PE漏电故障的重合装置（以下简称检测重合闸）由电动操作机构、控制电路、检测电路、输出接口组成，检测电路与重合闸配合使用，在重合闸控制电路操作下完成检测，根据检测结果决定是否重合闸。检测电路分别接在RCD相线、PE线、接地电阻Re1和Re2、变压器中性N线，通过相线、PE线、接地电阻Re1和Re2、变压器中性N线、检测电路构成回路，检测电路PE线无需连接设备外壳，具体如图2所示；也可以通过相线、设备外壳、PE线构成回路，重合闸检测电路PE线需要连接设备外壳，具体如图3所示。RCD脱扣，重合闸检漏电电路分别是a-PE、b-PE、c-PE。检测电路信号既可以是直流也可以是交流，电压不超过24V。

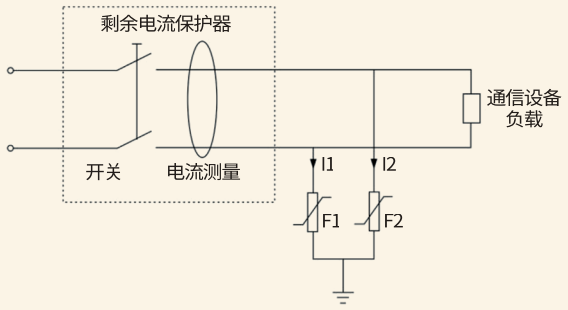
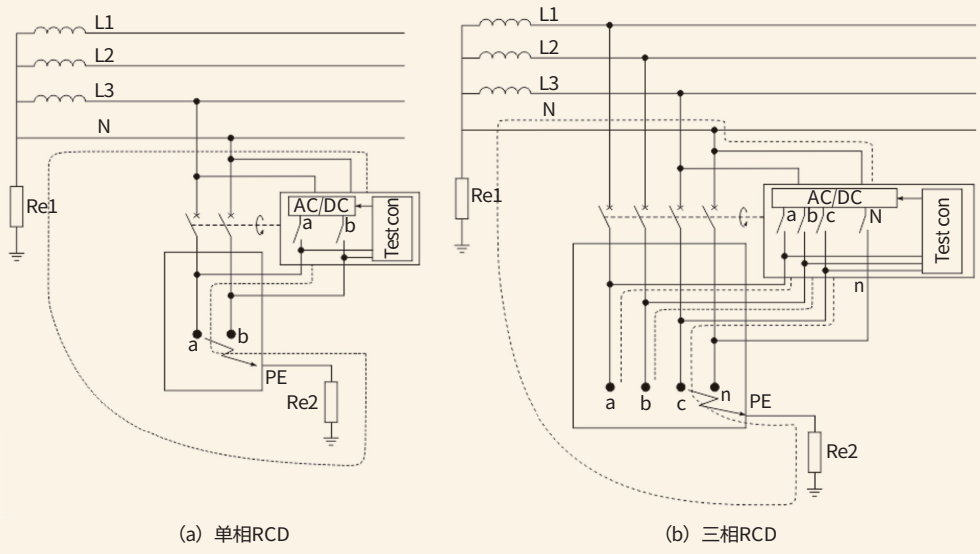
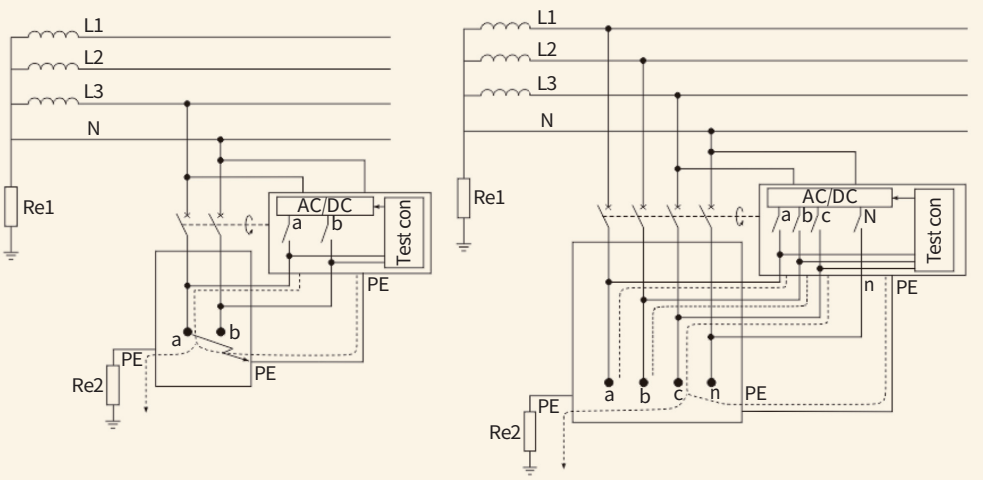


图1　通信电源电路原理



(a) 单相RCD　　(b) 三相RCD

图2　无需连接设备外壳



(a) 单相RCD　　(b) 三相RCD

图3　需要连接设备外壳

3 主要性能要求

剩余电流保护功能解决了安全问题，自动重合闸解决了电源雷击中断问题。YD/T 2346-2011《通信用自动重合闸剩余电流保护器技术条件》对一些参数的考虑如下。

自动重合闸功能需要兼顾供电和安全这两个因素。

(1)重合闸次数

从用户使用角度看，重合次数多好；但从安全角度看，重合次数少好。对于不检测漏电流即自动重合的重合闸产品，标准允许自动重合三次。

(2)重合闸时间间隔

从用电角度看，时间间隔最好是零；但从安全角度看，却必须足够长。

标准规定：如果保护器不具备断开后线路漏电检测功能，剩余电流保护器动作断开后20～60s自动重合闸一次；如果不成功，延时15min进行第二次重合闸；若第二次重合闸不成功，延时15min进行第三次重合闸；如果第三次不成功，则禁止再重合闸。

(3)检测电压

检测电压也是一个很重要的安全参数，不能太高。

标准规定：如果保护器具备断开后线路漏电检测功能，要求如下。

- 1min内如果三次合闸不成功，则不能再重合闸。
- 检测电压≤24V。

(4)耐雷能力

保护器可能有一定的电子电路，需具有一定的耐雷能力，否则无法使用。

标准规定：剩余电流保护器对通过设备的电容负载流过的对地浪涌电流和设备闪络而流过的对地浪涌电流均应有足够的耐受能力。延时型剩余电流保护器对设备闪络而流过的对地浪涌电流应具有足够的耐误脱扣能力。

电源线间（L-N）施加1.2/50μs（8/20μs）组合波、2kV冲击电压，应不发生误动作。电源线间（L-N）施加1.2/50μs、4kV冲击电压，样品工作正常不损坏。

电源线L对N流过8/20μs、20kA雷电流，附加安装电涌保护器时，样品工作正常不损坏。

4 结论和建议

自动重合闸剩余电流保护器可以有效解决雷击造成的电源中断问题，提高通信系统抵抗雷击的能力，而且安全可靠，是一种提高通信系统防雷能力的有效手段。

（下转42页）

doi:10.3969/j.issn.1000-1247.2018.07.011

移动网用户投诉处理精准分析与定位

康宏建

中国联合网络通信有限公司呼和浩特市分公司

摘要 从移动网络发展趋势与用户投诉诉求考虑，以投诉常见类型分类介入，重点阐述巧用系统工具进行精准分析与定位的两种方法，最后通过典型案例应用证明其实施后的效果，为处理错综复杂的各种类型投诉提供基本方法。

关键词 移动网 投诉处理 精准分析 定位

1 引言

随着移动网络各项技术标准和组网建设的逐步成熟与实施，移动网的业务也是内容丰富、包罗万象。移动网用户量飞速递增，接踵而来的用户投诉情况五花八门，途径众多。投诉用户是移动网络运行情况最直接的发现者和最有权力的发言者。运营商NPS、KPI、KQI、QoE等考核指标的最终落脚点都是为了不断提升用户服务感知。为了挽留用户，逐步提升用户感知度，必须要准确快速地处理与回复用户诉求，此项工作中对用户投诉原因的精准分析与问题定位尤为重要。

2 用户投诉常见类型分类与对应处理方案

首先对来自于各个渠道的投诉，必需采取有效分类与分解。通过事先与用户通话沟通，根据用户的投诉内容及范围，制定一个简单的分类与分解基本思路。用户投诉的基本类型情况及相对应的处理方案细分如下。

(1)覆盖率

- 弱覆盖，处理建议：建站或者天馈调整。
- 越区覆盖，处理建议：调整天馈，压缩覆盖范围。
- 室内分布系统外泄，处理建议：调整主服务小区。

(2)故障类

可大致分为宏基站和室内分布故障（此类故障可以直接由网管中心日报故障记录表获取）。

- 传输故障，处理建议：恢复传输故障。
- 软件故障，处理建议：恢复软件故障。
- 硬件故障，处理建议：恢复硬件故障。
- 天馈故障，处理建议：恢复天馈故障。
- 室内分布系统故障，处理建议：恢复室内分布系统故障。

(3)优化类

- 资源利用率高，处理建议：小区扩容。
- RF调整，处理建议：调整射频。
- 弱覆盖，处理建议：调整天馈。
- 各种干扰，处理建议：排除干扰。
- 载波不均衡，处理建议：平衡载波。
- 小区拥塞，处理建议：小区扩容。
- 容量受限，处理建议：小区扩容。
- 切换频繁，处理建议：调整主服务小区。

(4)终端类

- 异网终端定制，处理建议：更换终端。
- 双卡双待终端，处理建议：设置卡槽1为主卡槽位置。
- 终端本身故障，包括终端自身的软硬件故障以及程序、系统故障等，处理建议：咨询售后服务部门。

3 巧用系统工具精准分析与定位

针对投诉内容繁杂、区域广泛的问题，必需采取多手段、多方法去应对。巧用多个分析判断系统，达到反应快速、问题与位置定位精准、处理准确与回复及时的效果。例如某运营商投诉处理中的核心网博瑞德系统与厂商网管系统相结合的精准定位分析方法，以及MapInfo基站覆盖图与百度拾取坐标系统和基站故障通报记录表相结合的分析方法，这两种方法通过多个案例验证都能达到预期理想的效果。两种方法可以根据投诉工单内容与用户沟通情况，相互配合或者单独使用。两种方法合理使用，基本可以精准判断与处理

大多数用户的投诉。

博瑞德系统与厂商网管系统相结合的精准定位分析方法主要针对覆盖类、优化类、终端类的投诉类型。该系统通过输入用户投诉手机号码与相应时间段，不但可以获取用户使用过程的相关信息，还可以对上述各类问题进行精准判断。然后促进投诉处理人员能及时果断地对用户所投诉的问题做出分析定位，及时拿出处理解决方案。该系统分为两个子系统：一个是核心网网优监测系统（主要针对处理CS域问题），另一个是核心网分组域优化系统（主要针对处理PS域问题）。通过博瑞德系统可以获取用户相关的信息：用户使用终端类型，用户基站占用情况，用户接入切换过程，为无线资源利用率使用情况提供必要的时间段参考数据，数据业务使用情况等重要用户的使用与占用信息。获取到相关重要信息后，根据需要与厂商网管配合查询所占用基站的运行情况是否正常，并拿出相对应的有效处理措施。核心网博瑞德两个子系统界面分别如图1、图2所示。

MapInfo基站覆盖图与百度拾取坐标系统和基站故障通报记录表相结合的分析方法主要针对故障类的投诉类型。通过预先对用户投诉情况进行了解掌握，可以使用此方法判断出用户投诉所在地理范围和基站占用情况。若正好落在基站故障表通报的故障区域，则在基站维护时限考核期范围内尽快修复基站，使其尽快恢复正常运行。反之，则再回到博瑞德系统方法，继续查找其真实原因。

4 典型案例分析

虽然对投诉类型与分类进行了归纳与分类总结，但是具体投诉情况还是千奇百态，只能以大多数按照规律处理，个别案例特殊对待的基本工作模式应对。下面列举几个大类中的典型案例，作为具体分析案例。

4.1 覆盖类投诉典型案例

投诉内容：呼和浩特176****3209用户通过内蒙古联通网优助手反映在赛罕区内蒙古农业大学东校区宿舍楼内网络不好，上网慢而且频繁卡顿，要求赶快处理解决，尽快回复用户本机。

图1　核心网网优监测系统基站占用切换界面

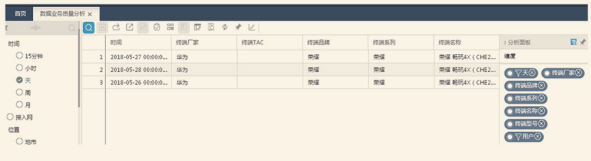


图2　核心网分组域优化系统终端查询界面

深度分析：回访用户具体位置在赛罕区内蒙古农业大学东校区12号楼4层，反映20:00−23:00上网卡顿比较严重。通过博瑞德网优监测系统分析用户占用FHH林学院CA2、FHH林学院CA5的均为两个小区的一二载波。一周忙时PRB利用率均在90%左右，下行单用户平均感知速率3Mbit/s。由于资源利用率高导致用户上网卡顿，经过对基站后台核实分析，由于该小区容量已经达到极限，无优化空间，所以考虑通过增加室内分布系统吸收话务的手段解决此投诉。

解决方案：经与网建部规划人员核实，内蒙古农业大学东校区12号宿舍楼已经列入规划，正在扩容室内分布系统实施。

效果验证：回访用户，告知处理过程与解决方案，用户表示满意与期待中。

4.2 优化类投诉典型案例

投诉内容：包头186****5839用户通过内蒙古联通10010平台反映，网络状态不好已经有一个月，周围其他联通用户都一样，无法正常使用，且不认可平台客服人员解释，要求尽快处理并及时回复本机。

深度分析：经核实，该用户投诉地点主要占用W望隆宾馆2小区、W鑫厦2小区、WUL正翔国际二期住宅室内分布三个基站的信号，经过后台查询，三个基站运行情况均为正常。通过博瑞德网优监测系统分析用户通话使用过程，整个过程是在三个基站中频繁切换而且起呼失败次数较多的情况下进行的，查其原因是属于弱覆盖无主服务区，而且还处在LAC边界上，导致该用户以及周围用户无法正常使用语言业务。

解决方案：通过优化手段调整主服务小区，控制室内分布信号外泄，达到用户感知度改善的效果。

效果验证：回访用户，用户表示网络已经恢复正常使用，表示对处理时效与结果非常满意。

4.3 终端类投诉典型案例

投诉内容：鄂尔多斯185****0322用户通过网络反映，手机无法上网，还是4G手机，需要查询原因，并尽快回复本机。

深度分析：经查询核实该用户个人后台数据与占用基站运行情况均为正常。通过博瑞德网优监测子系统分析用户使用过程是一直占用2G网络，再次通过博瑞德核心网分组域优化子系统查询用户终端类型是金立GIONEE GN5001S双卡双待手机，因此投诉处理人员怀疑该用户还使用着其他运营商SIM卡，并且未把中国联通SIM卡设置在主卡槽。

图3　用户当时基站占用示意

解决方案：再次与用户沟通后，得知卡槽1是中国移动卡，建议用户重新设置主卡槽1为中国联通卡，问题立马得以解决。

效果验证：回访用户，表示困扰多时的问题快而准地得到解决，非常满意。

以上三个案例都是通过核心网博瑞德系统精准定位与分析判断，可以看出巧借系统工具的重要性与时效性。

4.4 故障类投诉典型案例

投诉内容：呼和浩特186****0689用户通过微博反映，手机在诚信数码广场突然出现无法上网情况，其他地方都正常，急需回复本机。

深度分析：通过用户反映的情况分析，利用MapInfo基站覆盖图与百度拾取坐标系统和基站故障通报记录表方法，确定用户占用基站的情况。查询当日网管基站故障记录表后发现，该用户正好占用的诚信数码广场室内分布基站现正处于传输故障状态，基站与传输维护人员正在处理和修复。该用户当时基站占用情况如图3所示。

解决方案：通知基站维护人员，及时恢复基站正常运行，随后回访时用户前期发现的上网问题已消除，用户感知恢复。

效果验证：回访用户，表示问题已经得到解决，而且处理时间比较短，基本没有影响到正常使用，很满意。

通过上述4个经典案例的分析，发现原有规律性的投诉处理4步骤是；投诉内容、网优回复（内容是模板式环节）、深度分析、解决方案。现在建议完全可以把网优回复与深度分析合并，增加效果验证环节。处理环节的压缩与增加需要与时俱进。既压缩了处理流程步骤，又提升了处理时效，运营商与用户沟通过程中不但增加了亲和力，而且还改善了用户感知度。

5 应用效果验证

通过合理有效地利用上述两种处理方法，及时对用户回访和阶段性使用观察验证。无论在用户反映问题处理的时限上，还是处理的精准度上，各项效率都在迅速提升。实现从投诉数量的缩减到处理质量的提升式本质飞跃过程，可以从企业NPS值的改善和用户感知度提升的反馈得以证明。

参考文献

[1] 贺聪贤.移动网用户投诉分析[J].信息通信,2013(10)

[2] 张梅.客户投诉管理[M].北京:人民邮电出版社,2006

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

康宏建

毕业于北京邮电大学，高级工程师，现就职于中国联通呼和浩特分公司，主要从事移动网络优化、移动网络质量投诉分析、处理方案等工作，在多种刊物发表过论文。

（上接39页）

参考文献

[1] YD/T 2346—2011,通信用自动重合闸剩余电流保护器技术条件[S]

[2] IEC/TR 60755—2008,General requirements for residual current operated protective devices[S]

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

刘裕城

本科，高级工程师，现就职于中国电信股份有限公司广东研究院，长期从事通信防雷技术、工程设计和标准制定工作，主持多个防雷技术研究项目，编写了10多项国家和通信行业防雷标准，是YD/T 2346-2011《通信用自动重合闸剩余电流保护器技术条件》的编制负责人。

陈荣斌

本科，工程师，现就职于厦门大恒科技有限公司，从事自动重合闸剩余电流保护器的设计和生产工作。

doi:10.3969/j.issn.1000-1247.2018.07.012

构建精准4G网络智能故障诊断运维平台

赵俊德

中国移动通信集团河南有限公司

摘要 为了应对日益增加的运维困难与满足用户不断追求高质量网络的诉求，有效提升运维效率，河南移动构建基于4G网络的智能故障诊断运维平台，通过对4G网络故障特点、故障模型、解决方案的深入剖析，将日常维护场景进行分类与归并，依托于网管数据集中、处理能力强的特点，将运维经验通过平台进行固化和应用。该平台实现了对现网数据的实时分析，分析过程平台化、分析结果智能化、结果呈现图形化，从而实现现网状态的及时监控、网络隐患的及时掌握、设备故障的及时排除。全面提升维护人员对现网各场景问题的发现能力与解决能力，有效降低问题恢复时长，提升客户感知与满意度。

关键词 4G 智能故障诊断运维 运维效率

1 引言

4G网络经过多年的快速发展，已经基本进入稳定阶段，规模巨大的设备存量必然要求设备的平稳运行以及故障的快速恢复。如何减少故障对业务的影响、提升用户感知是运维工作的重中之重。通信行业竞争日益加剧，要保持业界领先地位就必须获得强大的竞争力，而获得竞争优势的首要条件是必须具备良好的网络基础、稳定的网络运行质量。网络维护是体现网络质量的根基，运维专业如何深耕细作、快速有效地发现并解决网络隐患与故障，是当前运维体系面临的共同难题。现网4G基站数量庞大，问题繁多，然而维护资源有限、人员紧缺、支撑手段与平台缺乏，导致难以做到深度精细化维护。这些困难与用户日益提高的网络感知诉求是一个矛盾，如何在现有情况下保障网络安全、提高业务质量、改善现有用户的感知度、支撑网络未来用户的持续增长，是当前网络运维面临的难题。

河南移动的4G网络规模在全国排名第6，是4G网络大省。随着设备与业务规模的快速扩张，4G基站数量已经接近10万台，服务3800万用户。由于传统运维手段单一、手工排障过程繁琐、识别风险问题困难等多种因素，给网络运维带来巨大压力和挑战。如何快速有效地掌控网络现状并实现网络问题的精准、自动定位与恢复，是河南移动实现高效稳健运维的重要目标。

目前，4G网络的传统运维模式是通过工程师对设备告警、网络指标的监控，识别其中的异常点，人工进行分析、筛选、定位、处理。手工筛查效率低，且维护人员技能水平参差不齐，导致维护效率无法有效提升，同时由于4G网络结构的扁平化、设备的集约化程度越来越高，也给网络故障快速定界、定位带来困难。

为了保障现网质量，同时响应集团集中运维要求，河南移动积极探索新的运维方式，逐步实现从依托人员能力的运维到平台运维能力的转变，创新开发4G网络故障智能运维平台。

4G网络故障智能运维以智能化思路为基础，现网故障场景梳理为素材，借助网管数据集中放置的特点，通过对网络故障场景的识别，自动获取相关的故障分析数据，将故障分析思路平台化，实现故障场景自动识别、自动诊断、自动输出根本原因报告，从而解放人工操作，实现故障的快速隔离定界。智能运维工具与传统维护工具对比如图1所示。

2 LTE无线网智能运维系统部署思路

构建运维方式由人员能力的培养、继承向平台能力固化的转变，实现问题发现与问题定界的同步，借助平台对关键数据自动获取、智能分析，从而提升运维效率，确保网络安全。

2.1 传输故障排查类维护经验平台化，实现整网3min排查定界

依托智能诊断平台，一键式输出传输类故障关键信息：故障发生时间、有无人工操作、故障节点位置、故障节点是否汇聚等。通过自动同步、识别网管上链路故障类告警，自动下发Ping、Trace操作，同时关联操作日志进行判断，确定中断类型、中断数量、是否操作导致、中断节点是否汇聚以及识别是否通过其他方式维护等，进行多维度全方位的深入

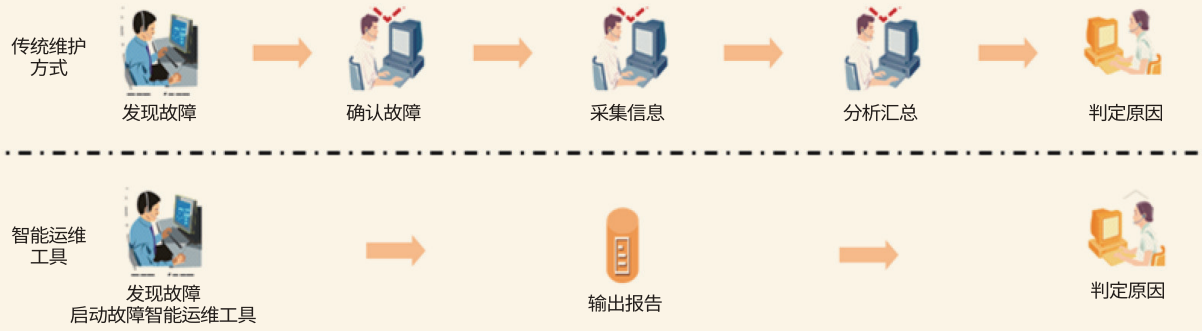


图1　智能运维工具与传统维护工具对比

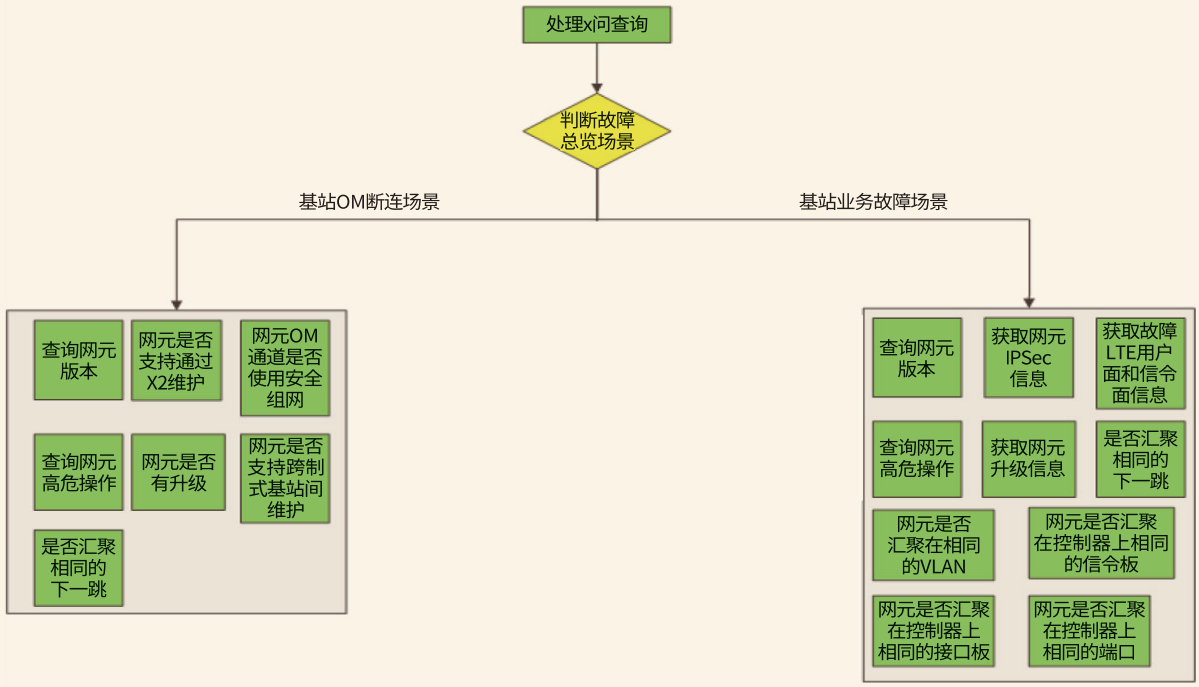


图2　传输故障分析流程

图3　故障关键信息自动整理示意

分析，将故障关键信息自动整理、输出，并且中断节点可以图形化自动输出，以便维护人员用最快的方式定界和识别恢复方法。

传输故障分析流程如图2所示。

故障关键信息自动整理、输出如图3、图4所示。

以100个网元为例，人工分析100个网元的Ping和Trace route结果需要30min，平台2min内就可以完成所有操作，效率提升15倍。

图4　故障关键信息自动输出示意

图5　河南省优秀维护经验分类

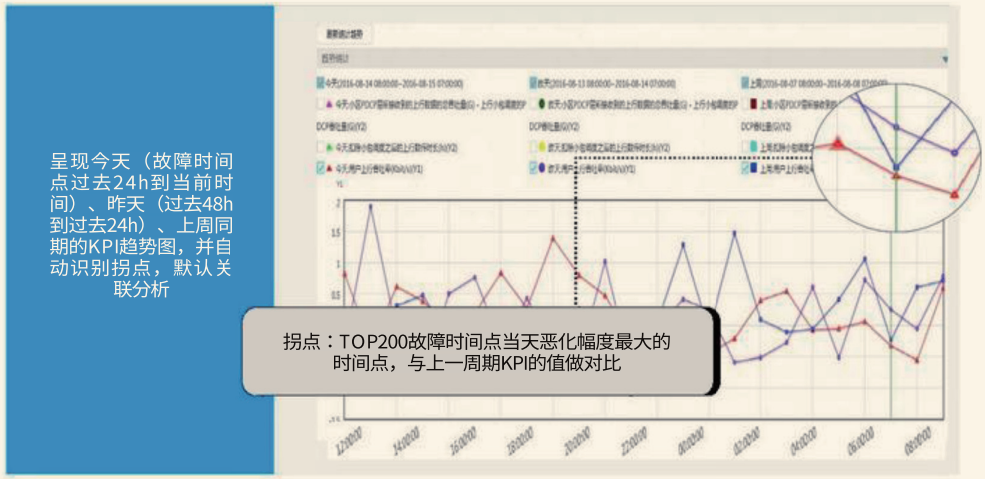


图6　图形化的整网指标现状与同时期指标趋势分布曲线

2.2　无线故障排查维护经验平台化，实现整网指标5min分析

(1)将河南移动优秀的维护经验进行锤炼总结，归纳出7大类、35小类的场景，通过选定场景实现一键式问题分析与定位，具体如图5所示。

(2)基于自定义的无线网络业务指标，提供图形化的整网指标现状与同时期（上周同一天、前一天）指标趋势分布曲线并智能识别业务指标恶化时间点，使故障分析人员从整网角度快速了解历史趋势，具体如图6所示。

(3)提供业务指标恶化TOP站点排序，自动关联业务指标恶化时间点的网络变更信息（配置变更、告警变更）和业务指标恶化原因值，帮助故障分析人员锁定关键节点、关键事件重点分析，具体如图7所示。

(4)通过输出网络指标变化趋势，失败原因值分布，提供业务指标恶化原因和下一步处理步骤等一系列措施，协助维护人员重点识别故障根本原因，实现问题的定位，具体如图8所示。

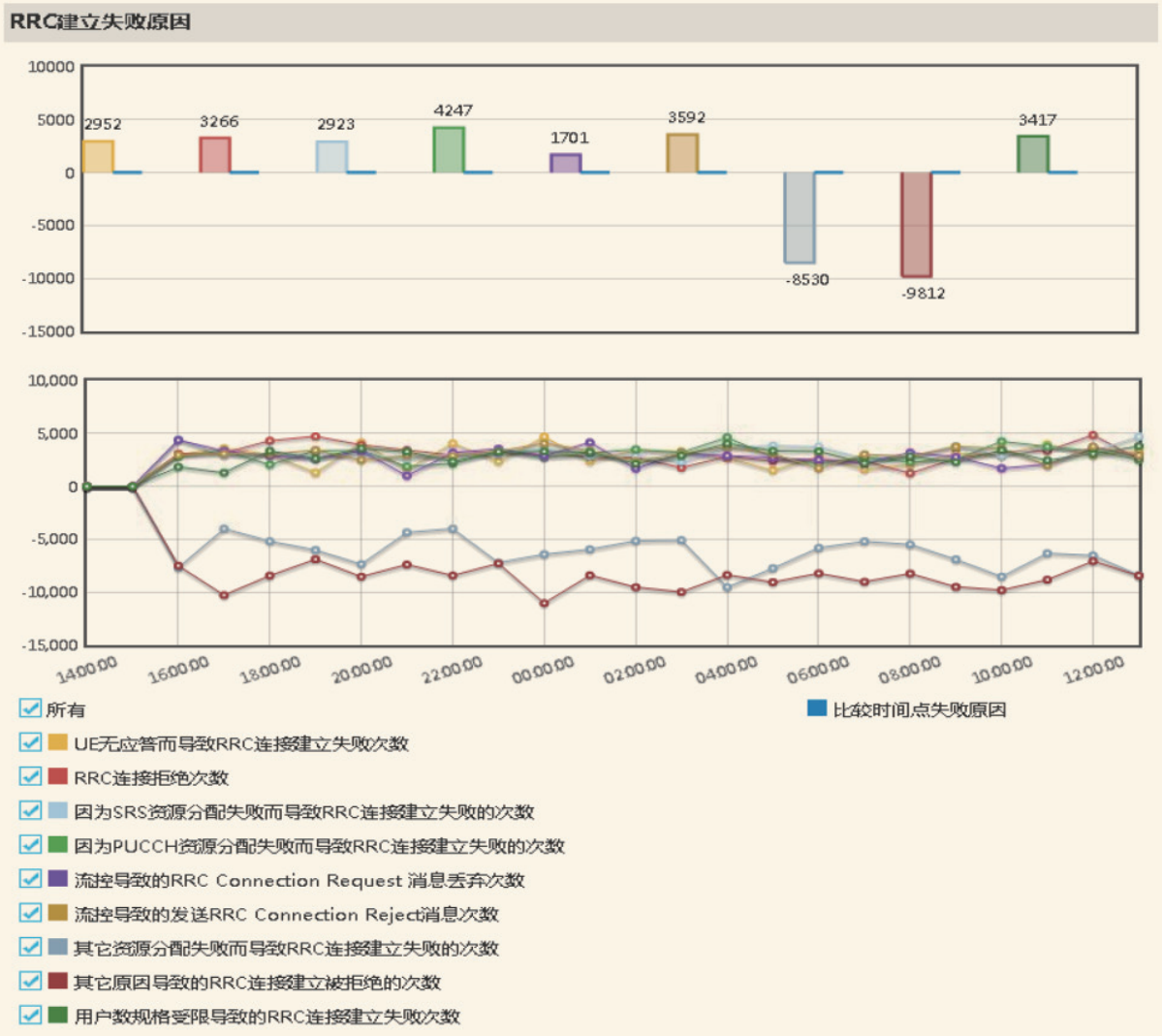


图7　RRC建立失败原因

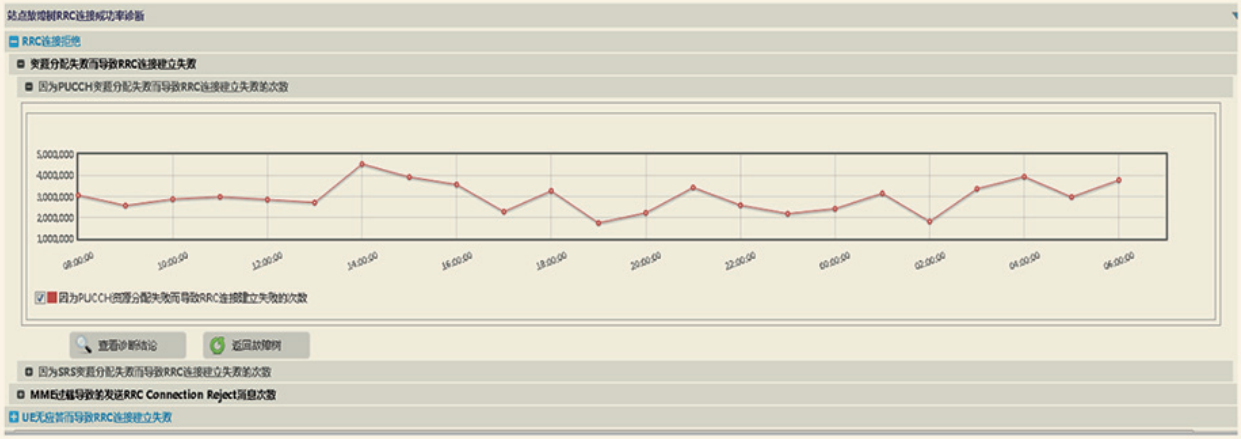


图8　网络指标变化趋势

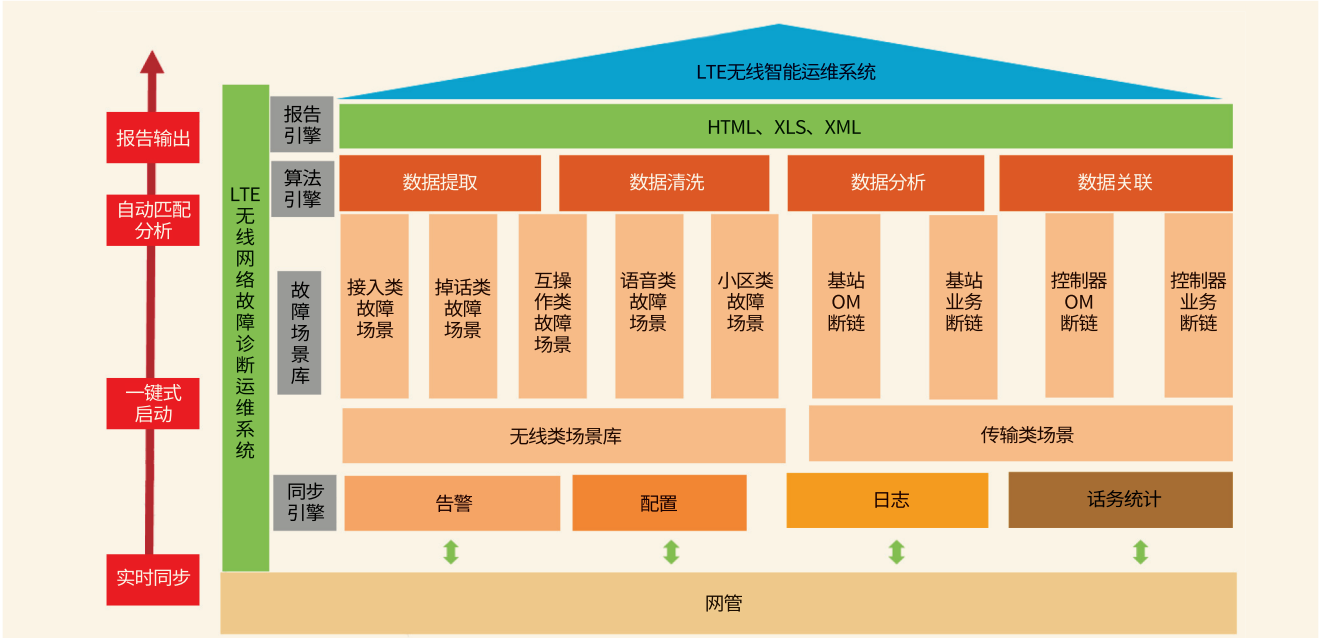
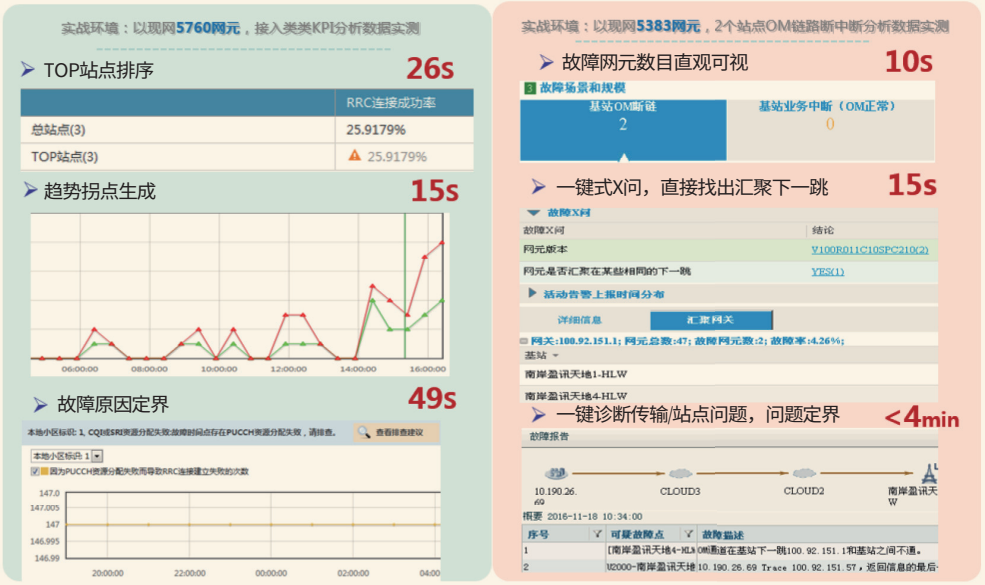


图9　4G网络运维4层系统分离架构示意



(a) 无线模块实战结果　　(b) 传输模块实战结果

图10　实战结果示意

2.3 丰富的日常故障运维场景和运维辅助支撑功能，涵盖日常运维绝大多数场景

平台不仅支持传输类故障场景、网络指标故障场景智能诊断，同时支持网络中小区状态故障类场景的智能诊断以及集成部分日常运维辅助支持功能。可以支持5个日常运维故障场景和4个整网传输质量诊断功能。

2.4 灵活的扩展方式，实现差异化的分析需求

可以通过灵活的方式配置实现不同场景、需求的自定义配置。

Ping包参数自定义：可以对Ping包大小、包长、发包间隔等进行自定义设置，实现对不同传输质量要求的整网级初步诊断。

分组自定义：平台除了自动同步网管的子网设置外，还提供自定义子网功能，可以通过导出和手工填写的方式实现基于不同的业务场景（如：高校、商业区、VIP区域等）组网划分，实现不同业务场景的差异化检测。

业务指标自定义：除通用的网络业务指标外支持新增指标、差异化指标自定义方式，实现差异化网络指标的分析监控。

3 LTE无线网智能运维系统

河南移动积极构建探索全新的4G网络运维模式。以分层的逻辑架构、丰富的故障场景、精准的故障分析算法和多制式的故障分析报告输出，打造4G网络故障智能运维平台，并实现4层系统分离架构，与现网日常维护相辅相成、互不影响，具体如图9所示。

(1)同步引擎层

利用4G网络结构扁平化的特点，依托网管作为4G网络维护中心的优势，通过对话务统计、告警、日志的自动同步获取，避免数据分析人工提取，确保现网数据安全。同时同步层支持基本配置查询下发和结果报文的获取和整理，所得即所见，实现分析数据与现网数据一致。

(2)场景库层

结合河南移动4G网络维护问题的分析和梳理，制定两大类场景：传输类故障场景和无线类故障场景。传输类故障场景可以快速定位链路状态问题，无线类故障场景梳理排查出网络指标类和小区故障类问题。

(3)算法引擎层

传输故障场景：平台自动识别各种链路状态告警（操作维护、信令面、业务面），通过链路状态告警触发对应链路的Ping、Trace操作，收集现网故障链路相关信息，并以图形化的界面呈现链路中断节点，实现维护人员对此类故障的精准判断。

无线指标故障场景：针对预先定义的网络指标计算公式，利用同步的网络话务统计数据进行实时计算，输出整网级的网络指标情况；按照不同基站对话务统计指标恶化的不同程度进行排序，提供网络指标恶化的TOP站点和网络指标化关键点；针对TOP站点的恶化原因值结合恶化时间点的操作日志、基站关键日志等信息进行关联，输出恶化原因和排查建议。

无线小区类故障场景：通过上报网管的小区不可用、小区服务能力下降、射频单元业务不可用告警，和RRU状态、CPRI链路、配置排查等相关信息进行关联判断，输出故障根本原因。

(4)报告引擎层

为了满足不同部门人员审视报告的多样化需求，报告引擎层支持Excel、XML、HTML格式的输出；可以对数据进行图形化处理，维护人员操作更直观，确保问题根本原因快速有效定位。

4 LTE无线网智能运维系统部署效果

自2017年7月河南移动部署智能故障诊断运维平台后，使用平台识别、分析网络传输类故障200多次，利用平台提供的Ping/TraceRT功能快速识别基站网络传输状态500多次。通过平台提供的KPI分析能力，对掉话类、数据传输类、语音类、小区故障类KPI识别问题180多次。平台生成的故障总览报告与诊断报告极大减轻运维人员的分析难度，信息获取效率提升60%，真正实现事故定位快速搞定。实战结果如图10所示。

在使用的过程中，通过对人工单个KPI的分析时间和智能故障诊断运维平台的分析时间的对比，效率提升9倍，有效地提升运维效率，减少人力投入。

5 结束语

高效智能故障诊断运维平台基于故障内容的实时监测机制、多维的诊断汇总算法、合理高效的事故规则设置、完整的检测体系、快速高效的并行协同工作机制、4G网络运维思路和经验等平台核心算法，均是由河南移动网优中心根据工作实践与创新总结出来的。能够在较少资金投入下，实现全量网络故障的实时监测与预警，大大提升运维人员的效率，快速定位问题、解决问题，从而减少故障时间，改善客户应用感知，提高网络满意度。

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

赵俊德

现任中国移动河南公司网络优化中心维护室经理，具有丰富网络工程、维护、规划优化管理经验，主要研究方向为移动通信网络优化新技术和项目管理。

doi:10.3969/j.issn.1000-1247.2018.07.013

多网协同：面向2020年无线目标网的思考与实践

许闱帷

中国移动通信集团上海有限公司

摘要 基于“大连接”战略的指引，依托“以终为始、整体规划、分步实施”的建设思路，坚持“多网协同”的原则，构建一张领先的TDD/FDD&NB&GSM融合网络，GSM设备得以更新，FDD目标网形成并具备能力，NB-IoT网络按需开启，既提升网络质量，降低运营成本，又提升频谱资源利用率。

关键词 GSM NB-IoT FDD TDD 融合网络

1 无线网络发展情况及面临的挑战

上海移动目前拥有GSM和TD-LTE两张主力承载网：GSM主要承载语音业务，TD-LTE承载数据业务。

1.1 4G网络建设多年，但是深度覆盖仍待改善

上海高层建筑、大型楼宇密集，无线环境复杂，建筑物遮挡严重。深度覆盖不足是上海面临的最主要的困难和挑战。

(1)对外环内MR（MR数据取自2017年外环内数据）进行大数据分析

上海外环内79.8%的MR来源于室内，弱覆盖MR的94.6%来源于室内，深度覆盖不足是弱覆盖MR的主要原因。

上海外环内总共有29.5万栋楼宇，其中低于20m的楼宇（低于6层）有26万栋，低层楼宇的弱覆盖占比达71%，说明MR覆盖率差的主要原因是低层楼宇，尤其是居民小区的深度覆盖不足。外环内MR采样点楼宇分析见表1。

经过多年TD-LTE建设，4G站点规模实现快速发展，但现有室外站点密度仍有不足。在过去一年的4G建设中，宏站建设越来越困难，建设方式从宏站为主转向侧重微站（小区覆盖、街道站），TD-LTE网络将更趋向立体化，但是上海楼宇规模巨大，不可能对全部楼宇实现专项覆盖。

另外一方面，VoLTE话务量快速上升，到2017年11月，占比已超过30%。VoLTE业务普及对深度覆盖提出更高要求。

(2)FDD900MHz能有效改善覆盖

选取上海现网几个典型区域（大华、上南和同济大学区域）的2G和4G网络MR覆盖情况进行分析。分析方法采用折算后的FDD 900MHz MR电平（GSM MR电平按照LTE 15kHz带宽折算成FDD 900MHz MR电平）和TDD MR电平进行分布统计，可以看出FDD 900MHz能有效改善深度覆盖。

上海典型城区的TDD和FDD（2G模拟）覆盖情况对比如图1所示。

因此需要考虑利用现有GSM 900MHz频谱向FDD 900MHz演进，并和现有4G（1900MHz/2600MHz）进行充分协同，全面提升深度覆盖能力。

1.2 NB网络建设需求迫切

当前同城运营商正在依托低频FDD网络，积极进行NB-IoT网络部署和商业模式创新，快速部署NB-IoT网络成为迫切的需求。

但目前物联网用户ARPU值低，在当前的商业模式下，未来NB-IoT的收益难以支撑其独立网络的建设和运维投资，因此在蜂窝物联网的商业模式上需要创新对于网络部署，需要考虑基于现有的无线网络基础，采用低成本、GSM&NB&FDD多制式兼容的方式进行部署。

1.3 2G网络老旧比例高，站点结构不合理，未来演进困难

1.3.1 2G网络设备老旧

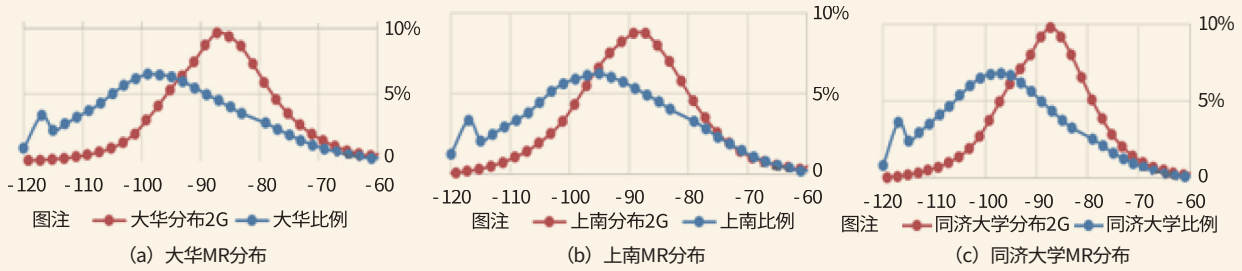
2G设备支持的演进能力见表2。

(1)室外站支持升级的分布式基站比例仅为30%左右；其中部分区域仅12%，部分区域几乎全不支持。

(2)全网76%的基站为传统一体化基站，不适应未来CRAN架构演进。

(3)2G网络设备老旧：设备在网时间较长，全网60%以上基站在网时间超过8年，设备日常维护成本较高。

(4)传统2G设备功耗大：传统机架功耗过高，不利于节支增效，相比分布式宏基站，单站每年增加3万余元电费，2~



(a) 大华MR分布　(b) 上南MR分布　(c) 同济大学MR分布

图1　上海典型城区的TDD和FDD（2G模拟）覆盖情况对比

表1　外环内MR采样点楼宇分析

楼层高度（m）	MR覆盖率	建筑物数量（栋）	话务占比	弱覆盖占比
＜20	87.74%	263500	68.55%	71.32%
20～30	88.92%	11008	5.43%	6.20%
30～40	88.20%	5932	4.24%	4.71%
40～50	88.29%	3694	3.20%	3.47%
50～60	88.11%	4072	3.26%	3.61%
＞60	90.90%	6879	15.31%	10.69%

表2　2G设备支持的演进能力

项目	GSM 900MHz支持升级的分布式基站比例		GSM 1800MHz支持升级的分布式基站比例	
	室外站支持比例	室内站支持比例	室外站支持比例	室内站支持比例
合计	32%	4%	35%	47%

表3　GSM 900MHz 6dB邻区数统计

GSM 900MHz 6dB内邻区数	内环内	内中环间	中外环间	外环外
0	22.9%	19.1%	16.2%	12.6%
1	19.9%	20.0%	22.5%	16.2%
2	17.8%	20.4%	19.4%	14.5%
3	16.6%	16.7%	17.7%	12.0%
4	10.4%	10.7%	13.0%	8.8%
5	7.4%	9.0%	9.2%	8.1%
6	5.0%	4.0%	2.0%	2.9%

表4　天面调研结果

区域	天面规模			总计
	不能增加	资源紧张	资源足够	
比例	46%	35%	19%	100%

3年可省出一套2G设备。

1.3.2 站点结构不合理

GSM 900MHz 6dB邻区数统计见表3。

GSM是异频组网技术，对重叠覆盖区可以采用异频方式避免干扰；FDD-LTE是同频组网技术，需要严格控制重叠覆盖区，现网GSM 900MHz路测数据统计显示，6dB以内邻区数量大于4的比例大于10%（参考TD-LTE指标为小于5%）。因此由于FDD 900MHz和GSM 900MHz对覆盖控制的差异，现网GSM 900MHz网络结构不具备直接向FDD 900MHz升级演进的基础。

1.3.3 天面资源紧张

统计天面资源调研结果，发现外环内主城区绝大多数基站均不具备增加天线的条件，具体见表4。

现网GSM的站点设备和网络结构均不能很好地向FDD/NB平滑演进，因此FDD/NB目标网有必要进行重新规划，优化网络结构，同时由于天面资源紧张，GSM/NB/FDD需融合为一张网。

1.4 面向未来5G演进，对基础资源提出挑战

由于5G NR（3.5G）频谱的覆盖能力远远低于LTE现有频谱，为了确保5G NR部署时不大量新增站址，协议中提出5G和4G的上下行解耦应对，希望能够做到在现有网络结构上不新增站址。因此面向未来5G演进，现在就需要考虑TDD/FDD的协同和融合，为未来面向5G演进奠定基础。

蜂窝物联网的迫切需求对上海移动来说是一个巨大的挑战，但同时又使重构GSM、形成NB/FDD能力、实现TDD/FDD&NB&GSM多网协同的无线目标网成为可能。因此有必要针对下面问题加以考虑，提前做好布局。

基站新架构：现网2G设备在网时间较长、功耗大、架构老旧；同时2G站点结构不合理，站点天面紧张，2G网络如何面向NB和FDD演进，构建一张FDD&NB&GSM融合的网络？

多频段协同：TDD中高频谱资源较为丰富，但覆盖短板明显；FDD中低频谱覆盖较好，但频点资源和站点资源欠缺，如何进行TDD/FDD多频协同？

2 FDD/NB目标网分析和规划

2.1 以FDD 900MHz进行FDD/NB目标网规划

基于无线网络的现状和痛点，明确FDD在4G网络中的定位。

(1)LTE FDD 900MHz：应作为4G主力底层覆盖网络，实现全市连续覆盖

LTE FDD 900MHz网络宏站覆盖要达到或超过2G网络宏站覆盖水平，具备全面承载VoLTE语音业务的能力，弥补TD-LTE在深度覆盖上的短板。

(2)LTE FDD 1800MHz：频率资源丰富，应作为热点区域的容量补充手段

热点地区容量补充：在高流量场景，TD-LTE网络容量不足，LTE FDD 1800MHz的终端成熟，可部署LTE FDD 1800MHz 用于容量补充。

基于FDD 900MHz网络定位以及NB-IoT在900MHz上的部署需求，坚持“以终为始、整体规划、分步实施”为原则，确定“以FDD 900MHz进行FDD/NB目标网的规划”为思路，然后基于FDD目标网络按需选取1:*N*站点作为NB-IoT网络规划。

NB-IoT业务速率诉求比较低，允许的MCL较大，在基于FDD规划的网络基础上建设，有较多的覆盖余量。在满足一定的覆盖要求余量条件下，可以从目标网站点中按照1:*N*比例调整站点进行NB-IoT的部署。

2.2 FDD规划关键问题分析

(1)GSM频谱具备释放条件

从2014年以来，2G网语音话务量平稳小幅减少，数据业务快速下降，导致网络利用率降低，具备GSM频谱腾挪的空间和基本条件。根据2G业务量测算，900MHz可以全网退频5MHz，1800MHz可以全网退频10MHz。

(2)上海网络用户终端具备条件

通过对现网4G终端统计分析，上海手机终端硬件支持LTE FDD终端比例达到80%；其中支持B8 900MHz的终端，比例接近50%，上海现网终端已具备相应的条件。

(3)FDD关键技术nTnR的选择

FDD多T多R是未来技术发展趋势，在海外已开始规模部署。

与中国移动自身的GSM 900MHz网络相比，由于技术制式的原因，当900MHz重耕到FDD后，FDD 900MHz上行控制信道比GSM 900MHz弱2.5～5.5dB。为了确保频谱重耕后的覆盖能力（上行）不下降，并且保持网络的领先优势，有必要在建设FDD网络时，采用4R的组网规格。测试数据表明，FDD 4R相比2R，接入能力提升约3dB；或相同上行速率，4R相比2R上行覆盖能力提升3～4dB。

理论分析，FDD 4T组网时，针对2R终端可以降低网络干扰，提升小区容量；对于支持4R接收的终端，FDD 4T可以开启单用户4流，理论上可提升用户峰值体验一倍。

上海金桥FDD/TDD LTE融合组网示范区的测试充分体现了4T4R对现网2R/4R终端的增益。上行对于现网终端，网络侧4R相较于2R在边缘速率上提升近100%；下行4×4 MIMO相较2×2 MIMO在中点速率提升近100%，远点提升近200%。

金桥FDD 4R增益及金桥FDD 4T增益如图2、图3所示。

随着终端和芯片产业链的成熟，高端机已在1800MHz及以上频段实现四天线技术，故建议FDD 1800MHz优先选择4T4R部署；由于手机在低频900MHz实现四天线难度较大，当前还未看到可行的实施方案，故对FDD 900MHz网络，综合考虑投资回报等因素，优先以2T4R为主。

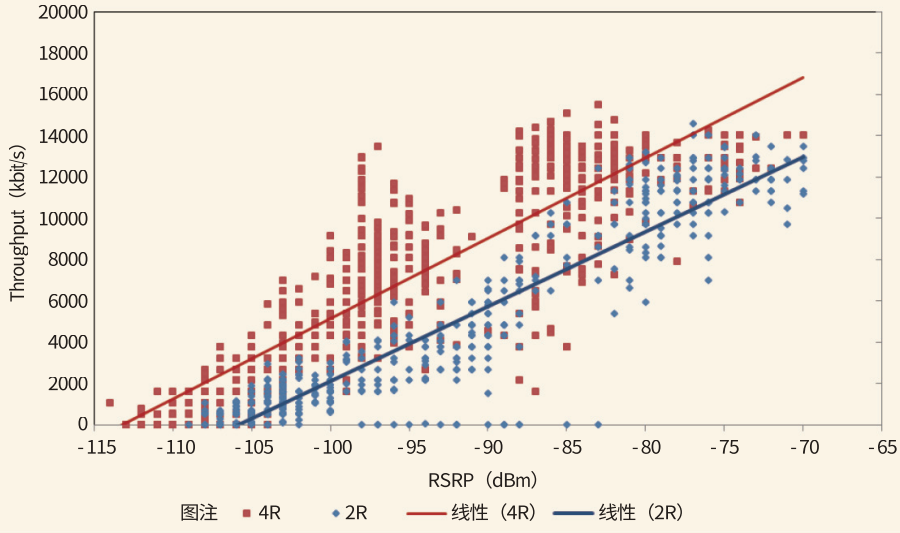


图2 金桥FDD4R增益

(4)规划站址选择

TDD和GSM站址情况如图4所示。

TDD站点是GSM站点的1.5倍，基于2G/4G全部物理站址库规划部署FDD/NB目标网，选择余地更大，网络结构更趋合理，可获得更加理想的网络性能。若只基于GSM站址，性能难以达到最佳。

2.3 FDD/NB目标网规划仿真

仿真规划结果：FDD目标网全部利用现网站址，目标网站址与TDL站址共址率达98%，与GSM

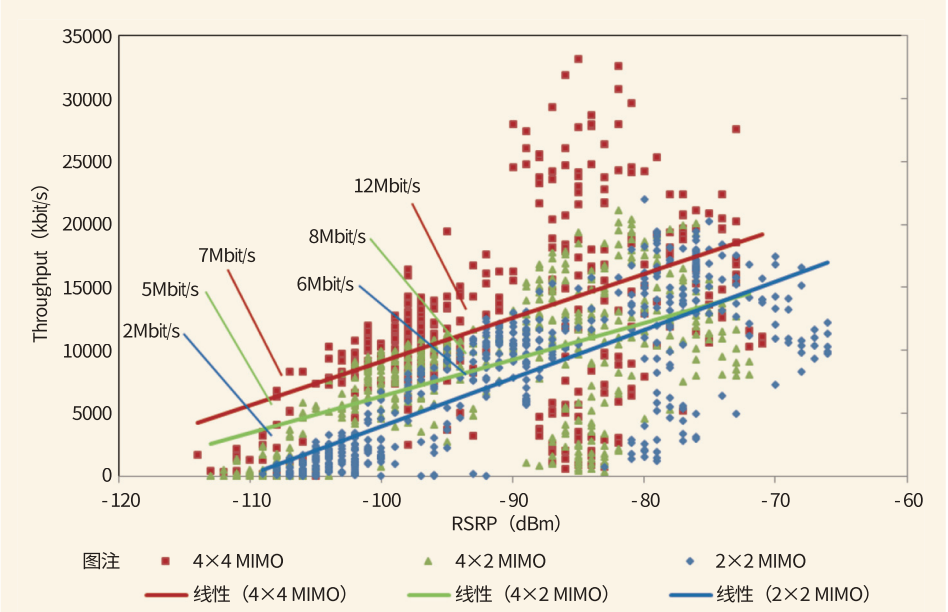


图3　金桥FDD 4T增益

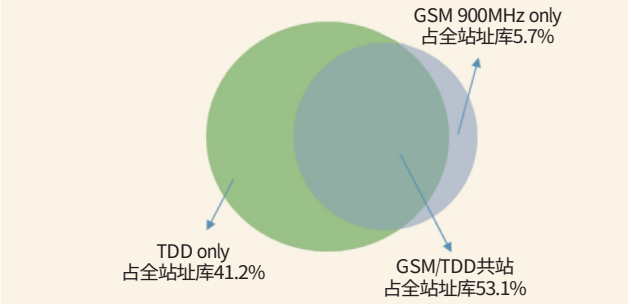


图4　TDD和GSM站址情况

表5　上海移动LTE 900MHz规划仿真结果

区域	覆盖面积（km^2）	FDD宏基站平均站间距（m）	GSM物理宏基站平均站间距（m）	TD-LTE物理宏基站平均站间距（m）	与GSM共站率	TD-LTE的共站率
主城区	664	470	585	392	52.0%	98.1%
一般城区	1038	655	756	593	41.8%	98.8%
县城	3178	957	1362	846	53.4%	99.6%
乡镇	1301	1436	2275	1361	60.0%	99.8%

站址共址率为50%。上海LTE 900MHz规划仿真结果见表5。

从规划结果可以得知，FDD 900MHz/NB的目标网和现网GSM结构之间差异较大，LTE FDD的部署重点在于与TD-LTE之间的协同与融合。

3 TDD/FDD协同的可行性与必要性

3.1 可行性

TDD和FDD的协同指的是TDD和FDD的互操作，包含以下几个层面。

基于覆盖和负载均衡的基本互操作：实现多频多模站内或站间的切换等互操作，确保用户在大网范围内的平滑移动，以及频点/制式间的初步均衡等。

基于业务的互操作：在基本互操作基础上，进一步分析各频点各制式的上下行网络资源使用情况（找出短板资源），以及现网用户个体行为（业务类型）等，合理匹配用户行为和网络资源（比如TDD优先承载下行为主的业务，FDD优先承载上行为主或对称业务等），提升多频多模的频谱使用效率和用户体验。

载波资源池实现融合：把站内或站间多频多模频谱资源融合成一个资源池（TDD/FDD载波聚合），供本区域所有用户共享，网内任一用户均可同时使用多频多模的所有资源，不仅能提升整网频谱效率，还是实现用户体验均衡的最优解决方案。

TDD/FDD协同的目的是均衡多频点之间和上下行之间的资源负荷，保障用户感知。基于负载的基本互操作通过参数设置在X2接口加以实现，能达到初步的资源均衡效果，TDD/FDD协同的最高境界是融合，融合组网是具有TDD与FDD频谱运营商的最优选择。

3GPP在R12协议中，已经开始定义TDD+FDD的载波聚合（CA）功能，并随着R13之后的协议演进，LTE将通过CA技术，实现全频点协同，TDD/FDD最终走向深度融合。

3.1.1 TDD/FDD高低频协同，提升用户边缘体验和峰值体验

TDD/FDD高低频协同的原理如图5所示，虽然高频资源多，但覆盖差，用户很容易回落低频，资源较难充分应用；低频覆盖好，但资源少，回落低频的用户体验较难保障。由于LTE普遍为上行覆盖受限，特别是大功率基站与Massive MIMO技术的应用，可以提升高频下行覆盖能力5～10dB，而受限于手机功率等因素，致使高频上行覆盖短板更加突出。故只要能补齐上行覆盖短板，就可以提升高频下行的有效覆盖范围。

在现网进行测试和验证，相关测试结果如图6所示，TDD覆盖提升10dB以上，边缘用户体验提升100%以上。

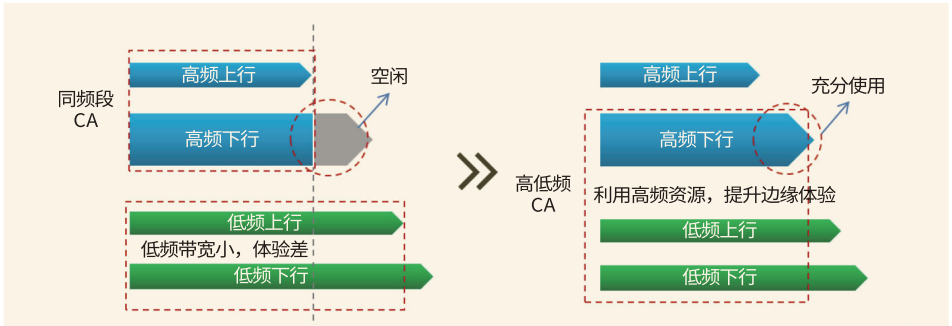


图5　LTE高低频协同原理

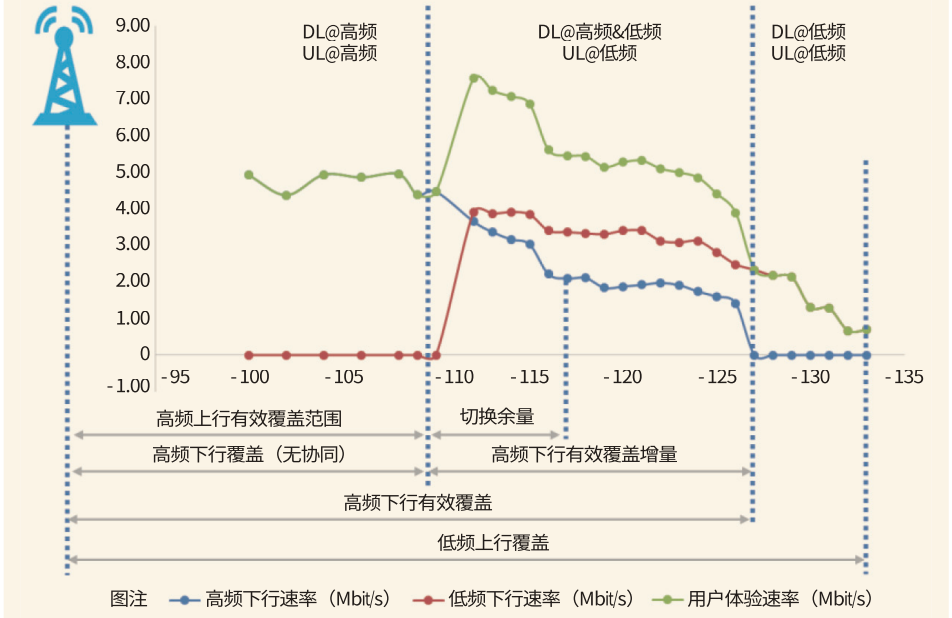


图6　LTE高低频协同上海现网测试结果

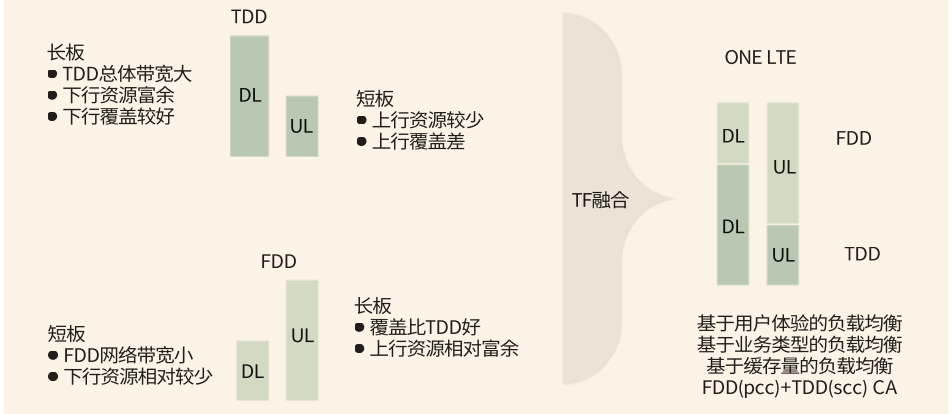


图7　TDD/FDD上下行资源互补原理

3.1.2 TDD/FDD上下行互补，提升频谱资源利用率

TDD/FDD上下行互补原理如图7所示。

TDD/FDD上下行互补，提升频谱效率。中国移动及国内外TDD、FDD大网数据表明，当TDD下行和上行时隙配置为3:1时，网络忙时下行资源相对上行空闲近50%，FDD上行资源相对下行空闲。故TDD/FDD融合组网，正好可以取长补短，提升TDD下行和FDD上行频谱利用率。在现网高话务区域对此进行验证和研究，结果表明：在TDD/FDD融合互操作的情况下，较好地实现了TDD和FDD之间的均衡，提升上下行流量50%以上。

秒级FDD和TDD小区的PRB利用率均超过90%，PRB充分利用，达到FDD小区和TDD小区PRB利用率均衡的效果。上海现网PRB利用率测试结果如图8所示。

3.1.3 TDD/FDD融合共建，降低建设维护成本

TDD/FDD融合的硬件基础是BBU实现融合，FDD/NB-IoT可以利旧已有的TD-LTE BBU设备，利旧或新增基带板，利旧TD-LTE传输链路及IP地址等，可以节省建设成本10%～20%。同时多模共BBU，还可以节省备件种类，降低电费等。

3.2 必要性

通过FDD目标网的规划可以看到，FDD站址与TD-LTE站址共址率达98%，因此TDD/FDD协同与融合非常重要。

其次，随着资费的降低，流量快速增长，按DOU增长与流量需求进行超容占比分析，预测到2020年，近28%的扇区超过F频段/D频段/900MHz频段/1800MHz频段承载能力。

FDD的频率有限（目前900MHz频段仅5MHz，1800MHz频段仅10MHz），越是高流量的热点区域，FDD面临的流量

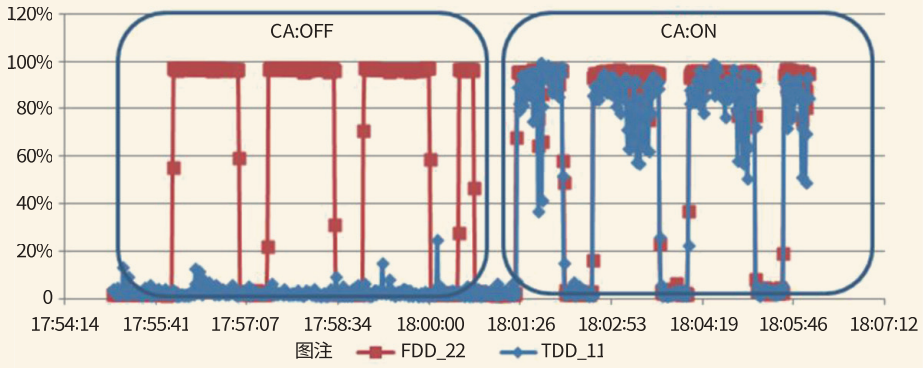


图8　PRB利用率上海现网测试结果

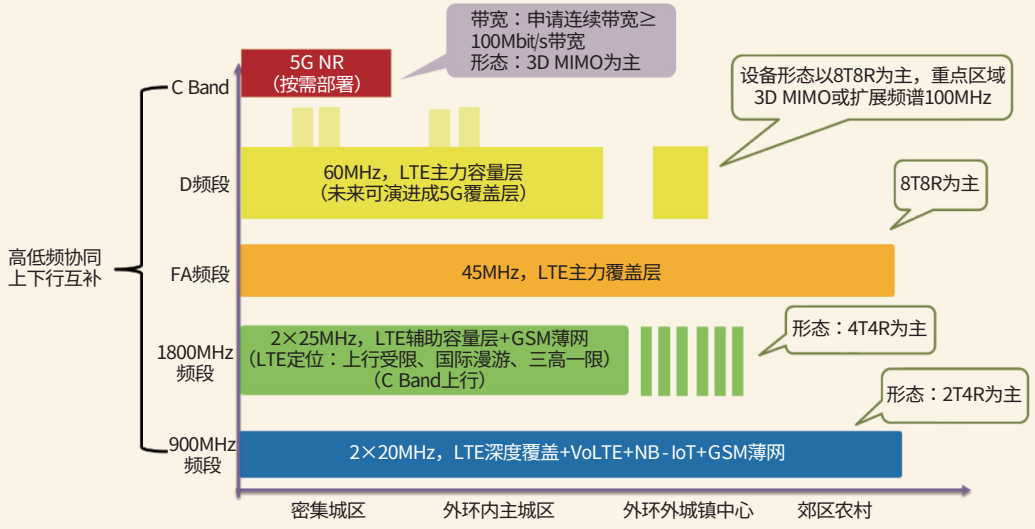


图9　2020年无线目标网络架构

承载压力越大，越需要和TDD进行良好的协同。从地理分布上看，超容小区主要分布在外环内，因此外环内价值城区FDD有必要和现网TDD网络形成良好的融合。

TDD/FDD融合是TDD与FDD协同的最优选择，可以视场景分区域部署，外环内主城区作为高流量的价值区域是首选。

4　面向2020年无线目标网架构

2020年无线目标网络架构如图9所示。

FA频段（1885～1915MHz，2010～2025MHz）总计带宽45MHz。由于目前F频段已经是4G的基础覆盖层，因此FA频段将作为LTE的主力连续覆盖层长期存在；随着后续支持A频段的商用终端逐步上市，软件升级即可支持A频段TD-LTE。

D频段（2575～2635MHz）总计带宽60MHz。目前外环内和外环外城镇中心已经实现基本的F+D双层网，用于高流量区域。D频段将作为LTE的主力容量层长期存在。

900MHz频段总计带宽2×20MHz，预期未来将作为LTE深度覆盖+VoLTE深度覆盖+NB-IoT使用，同时保留部分频点，用于GSM语音业务的连续覆盖。

1800MHz频段总计带宽2×25MHz，预期未来将作为LTE的辅助容量层使用，同时部分GSM高话务区域仍将保留部分频点，用于承载GSM基础语音业务。

适应网络发展的不同阶段，基于FDD目标网络按需选取1:*N*站点作为NB-IoT网络规划。

参考文献

[1]　2017上海移动蜂窝物联网建设工程可行性研究报告[Z]

[2]　中国移动通信集团上海有限公司.中国移动上海有限公司2017-2019年网络发展滚动规划[Z]

[3]　2017中国移动TDD/FDD融合对比测试上海外场测试报告[Z]

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

doi:10.3969/j.issn.1000-1247.2018.07.014

Web Cache在互联网国际出入口的部署应用

马兆铭
上海邮电设计咨询研究院有限公司

摘要 在互联网国际出入口部署Web Cache系统，存储国外互联网中的热点内容或特定内容，通过重定向机制引导国内用户的访问请求到Web Cache系统。当命中访问请求内容后，由Web Cache系统直接为国内用户提供国外热点内容服务，从而提升国内用户访问国外内容的速度和业务质量，有效缓解国际出入口链路的拥塞问题。

关键词 Web Cache 重定向 负载均衡

1 引言

互联网国际出入口链路是国内外互联网用户进行信息交互访问的关键信息通道，现阶段我国互联网国际出入口链路主要由国内三大基础运营商负责建设维护，集中部署于北京、上海、广东三地。近年来随着国内互联网的迅猛发展，以及企业国际互联业务的持续拓展，大量用户的P2P下载、在线视频、国际互联网访问等需求给互联网国际出入口链路带来较大的压力，导致互联网国际出入口链路拥塞严重，用户体验降低。

根据有关研究统计，超过80%的互联网流量由20%经常被访问的互联网内容构成。在这一规律下，利用Web Cache系统将国外热点内容缓存在国内缓存服务器中，并由国内Web Cache系统为国内用户提供国外热点信息服务，减少大量重复内容流量对互联网国际出入口链路的占用，有效缓解互联网国际出入口链路的拥塞问题，同时能改善用户对国外互联网信息的访问速度和业务体验。

目前，Web Cache系统在内容分发应用领域发展迅速，已经发展出HTTP小文件缓存（页面缓存）、HTTP大文件缓存、视频文件缓存、P2P等多种缓存业务，可满足目前用户互联网访问的基本需求。Web Cache系统在降低带宽成本、提高网络效率、提升用户体验方面对互联网国际出入口链路起到改善和优化作用。

2 系统工作原理

系统通过统计用户访问情况判断国外热点内容，将国外热点内容或特定内容下载存储到国内缓存服务器中，通过重定向方式将用户访问请求引导到Web Cache系统中，由Web Cache系统为国内用户提供所需的资源内容。系统工作原理如图1所示。

(1)访问请求的采集

在互联网国际出入口链路上部署分光器，对国内用户访问请求流量进行镜像采集。通过深度报文检测技术对分光流量进行协议识别、解析，提取出用户的访问请求信息。

(2)热点判断

将用户访问请求与Web Cache系统已缓存内容信息进行查询对比，如果Web Cache系统已缓存用户所需访问的国外内容，则用户访问请求命中，并启动重定向机制将国内用户访问请求引导至Web Cache系统，由Web Cache系统分配相应资源为国内用户提供内容访问服务。如果Web Cache系统未缓存用户所需访问的国外内容，Web Cache系统利用热点内容分析算法对某一时间内的用户请求进行热点分析，若用户访问内容已达到系统设定的热点阈值，则系统代理用户向国外源站下载缓存内容，同时系统重定向用户访问请求，由Web Cache系统为国内用户提供该热点内容的访问服务；若用户访问内容未达到系统设定的热点阈值，则系统对用户访问请求不做响应，用户通过国际出入口链路获取国外内容。

(3)重定向

- DNS重定向机制

系统通过检测用户发出的DNS解析请求，如果用户访问的域名属于系统已缓存的热点内容，则在DNS响应消息中向用户返回缓存服务器的IP地址，引导用户的访问请求重定向至Web Cache系统，由Web Cache系统响应用户访问请求。

- HTTP重定向机制

当系统检测到用户发出的HTTP访问请求属于系统已缓存的热点内容，由Web Cache系统向用户返回HTTP 302重定

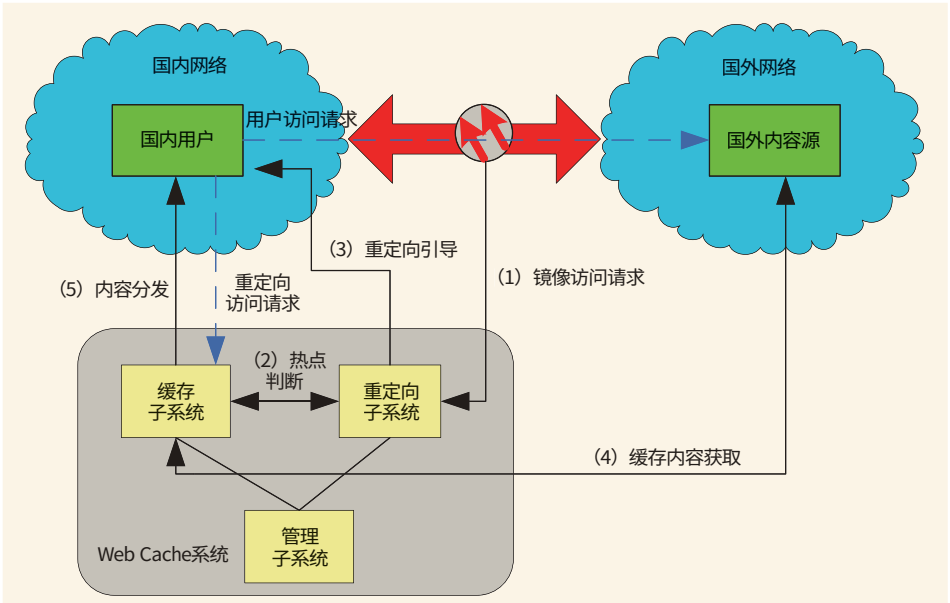


图1 系统工作原理

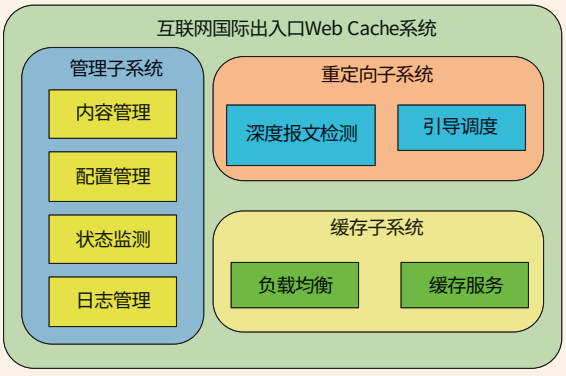


图2 系统功能架构

向报文，响应报文的目标地址为缓存服务器的IP地址，用户接收到HTTP 302响应消息后，将重定向至Web Cache系统并发起访问请求。

(4)缓存内容获取

当Web Cache系统中未缓存用户访问内容，同时用户访问内容已达到系统预设的热点阈值时，Web Cache系统通过互联网国际出入口链路对国外热点内容进行下载缓存，并更新系统内容缓存信息列表，为后续用户访问请求提供服务。系统还需定期更新缓存内容，保证所提供的缓存内容在有效期内是最新的。

(5)内容分发

对命中的用户发送访问请求，系统分配相应的缓存资源，向国内用户提供各类基于HTTP的互联网页面的访问和文件下载服务，将缓存服务器的缓存内容传送至请求该内容的用户终端。

3 系统功能架构

互联网国际出入口Web Cache系统主要由三个部分组成：重定向子系统、缓存子系统和管理子系统，系统功能架构如图2所示。

3.1 重定向子系统

重定向子系统包括深度报文检测功能和引导调度功能。

(1)深度报文检测功能

通过对互联网国际出入口链路中的原始流量进行协议解析，在获取基本IP地址信息的基础上，深度检测数据流应用层信息，进行特征信息比对，实现对互联网访问流量的精确识别与解析。在识别出会话类型或报文协议后，支持按照设定的配置策略将满足匹配条件的流量转发至用户请求引导调度功能模块，如DNS解析请求、HTTP访问请求等。过滤匹配规则可以是指定协议类型、IP地址、端口号、流量方向、应用层特征等组合。能够针对访问频次、带宽、流量、连接次数等指标进行统计，可对热点内容的排名次序进行统计分析。

(2)引导调度功能

处理接收到的用户请求报文，根据系统状态、策略配置及资源分布情况，生成对应的响应消息，将用户访问请求引导至本地的缓存系统。

在DNS重定向模式下，判断国内用户访问国外资源的DNS请求中所需解析的域名是否已缓存，如果用户请求的域名属于Web Cache已缓存的热点内容，则引导调度功能根据系统状态、业务策略、资源分布、网络条件、IP地址配置等情况，将Web Cache系统的对外IP地址作为DNS响应内容发给国内访问用户。在HTTP重定向模式下，判断国内用户向国外网站发起的HTTP请求，如果属于Web Cache已缓存的资源，则由引导调度模块根据系统状态以及参数配置等情况，构造HTTP 302重定向消息并发给国内访问用户。

3.2 缓存子系统

缓存子系统包括负载均衡功能和内容缓存功能。

(1)负载均衡功能

负载均衡功能是将用户请求引导调度数据按照配置的负载均衡算法分发到不同缓存服务器进行处理。当用户请求到达缓存子系统时，负载均衡功能根据用户请求、服务器状态

等情况，选择特定的缓存服务器响应用户的访问请求。

负载均衡模块能够充分利用现有缓存服务器的软硬件和网络资源，将所有引导调度流量均衡地分配到缓存服务器中，尽量避免“不平衡”现象的发生。能通过多种方式监控缓存系统中服务器的健康状态，如果某台服务器失效，则按照策略将负载分发到其他缓存服务器。

(2)缓存服务功能

缓存服务功能提供对各类基于HTTP的互联网页面对象和文件的缓存能力，实现为国内用户提供国外热点缓存内容的输出功能，将缓存服务器的缓存内容传送至请求该内容的国内用户。接收到用户发送的访问请求时，缓存服务模块需分析该请求是否在缓存服务器已缓存，若为缓存命中请求则系统直接响应；对于未命中的请求，系统对用户请求不予响应。

缓存服务功能可以对网页中的html、xml、js、css、zip、mp3、图像等多种静态互联网HTTP对象进行缓存，能对不同静态对象的缓存进行策略配置。缓存服务满足HTTP大文件的缓存加速功能，如游戏软件、升级包等。缓存服务功能需满足HTTP视频文件的缓存，主要针对各种在线视频网站，文件类型包括FLV、MP4、MOV、WMV、RMVB、F4V等文件格式。

缓存服务功能满足多维度的缓存策略管理，系统管理员可以严格、清晰地定义缓存服务模块的访问控制策略，通过ACL访问列表，可以对用户的请求进行访问控制。缓存服务功能可以对缓存内容进行管理，并根据热度策略实现对缓存文件的更新替换。在硬盘存储到一定比率时，能够根据对象的访问频率和文件大小核算对应的热度值，访问频率越高权值越高，热度值较低的缓存对象将会被优先删除。

3.3 管理子系统

管理子系统提供网络管理功能和系统管理功能，具体功能如下。

(1)状态监测

实现系统网管功能，对重定向子系统和缓存子系统的可用性、设备性能、网络指标等进行实时监测，实时获得业务系统的资源使用情况和健康状态。

(2)管理配置

提供Web管理界面，对系统的工作模式、参数、策略进行配置管理，可以依据用户、URL等维度实施区分处理，支持对缓存内容的监管配置管理，提供热点管理相关策略等参数的配置。

(3)日志管理

对系统产生的各种数据进行记录和分析，自动生成常规报表和个性化报表，支撑各类分析管理需要。

(4)内容管理

分析用户访问数据和系统缓存数据，实时维护系统的内容分布信息，形成内容资源视图，并能将内容视图数据通过接口传送至其他设备，如用户请求调度设备、全网管控中心、互联网内容资源管理平台等。

4 系统部署方式和安全策略

4.1 系统网络结构

国际出入口路由器作为连接国内网络与国外网络的骨干设备，主要部署在北京、上海、广东三地，国内用户的国际访问业务经国内运营商骨干网汇接到京、沪、穗三地，通过国际出入口路由器连接国外网络。为了缓解互联网国际出入口链路的带宽压力，在京、沪、穗三地分别部署一套重定向子系统和缓存子系统，对流经三地的用户国际访问业务提供缓存加速服务，重定向子系统和缓存子系统均接入本地的骨干网路由器。集中部署一套管理子系统，管理和配置国际出入口Web Cache系统。系统网络结构如图3所示。

在国内骨干网路由器和国际出入口路由器之间进行分光，镜像国际出入口链路的流量至重定向子系统。重定向子系统的解析识别出用户访问请求，通过HTTP重定向和DNS重定向两种方式，将用户的访问请求引导和调度到缓存子系统，由缓存子系统为国内用户提供国外热点内容，以降低国际出入口的带宽压力。

缓存子系统上联国内骨干网路由器，利于业务流及重定向子系统管理的IPSec接入。缓存子系统可通过VPN方式实现缓存子系统之间的内部管理及信息同步。缓存子系统设备包括缓存服务器、负载均衡服务器、交换机。缓存服务器负责热点资源的本地缓存，对符合缓存规则的内容资源进行拉取并存储；以及将已缓存资源分发给国内用户，国内用户的请求被重定向后，用户会转向缓存模块请求资源，并与缓存模块建立数据传输连接；缓存服务器包括大文件缓存服务器、热点小文件缓存服务器及冷点小文件缓存服务器。负载均衡服务器对小文件服务器起负载均衡作用，接受用户小文件请求，并按照缓存命中率和负载情况将请求分发到不同的小文件缓存服务器。

管理平台采用集中式部署模式，为管理员提供统一的全网Web Cache系统管理配置界面。管理平台可对京、沪、穗三地的缓存系统进行信息采集和数据配置，能获取各节点当前的资源情况、热点内容、流量信息以及用户访问信息，能够通过标准接口向各节点缓存系统下发管理配置数据，使缓存系统生效。

4.2 系统安全防护策略

(1)系统回源防护策略

由于国际缓存的回源安全直接影响系统可用性，需将缓存系统的回源IP地址纳入安全域。

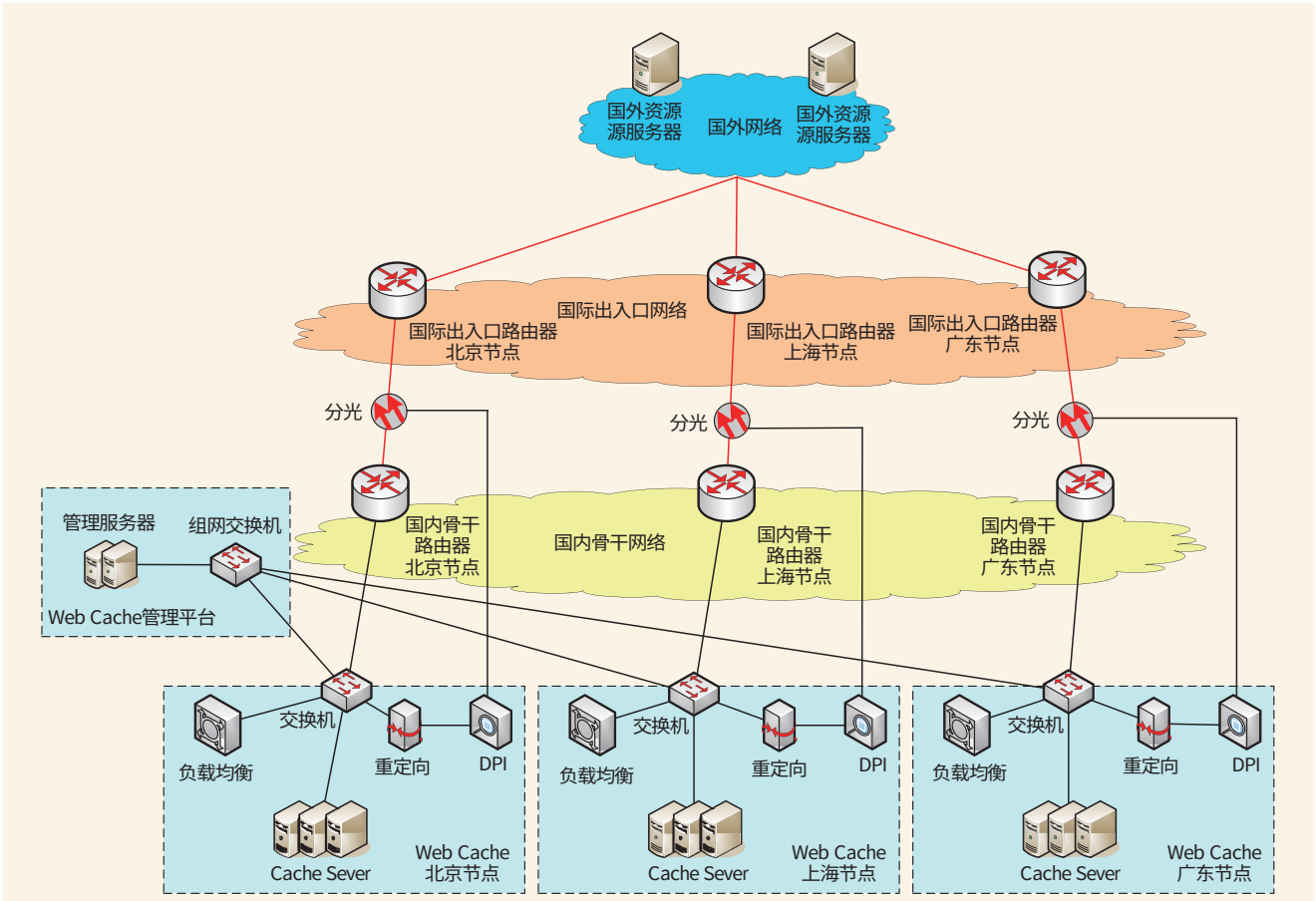


图3　系统网络结构

设置ACL限制访问IP地址，只允许回源域发起国际的HTTP和UDP53请求；采用1025～65535的端口向外访问，禁止外部对1～1024端口访问；或者采用安全监控服务，出现异常流量攻击，将IP地址应急替换。

(2)高流量域名防护策略

当前互联网中热门网站中的热门域名是集中受到性能、流量攻击的主要对象。将TOP100的域名按每一域名分配一个IP地址，以便热门域名遭受攻击时可以快速剥离。按照热门域名流量模型设定流量异常阈值，当流量超出阈值，即认定为域名遭受攻击。缓存系统停止响应，将攻击流量放行至国际链路，避免缓存系统遭受不必要的攻击。

5　结束语

在互联网国际出入口部署Web Cache系统，一方面可提高用户访问国外互联网内容的使用体验，缩短用户访问响应时长，对在线流媒体数据具有加速作用；另一方面，Web Cache系统大幅减少互联网国际出入口的流量，从而降低了互联网国际出入口的带宽扩容压力，对互联网国际出入口链路的优化扩容建设提供应用参考。

参考文献

[1]　冯铭能.HTTP缓存系统部署研究[J].广东通信技术,2014(11)

[2]　于绍晨.Web Cache系统部署方案研究[J].电信工程技术与标准化,2012(11)

[3]　张全明,张新有.基于会话劫持的HTTP资源缓存系统设计[J].成都信息工程学院学报,2013,28(4)

[4]　殷俊,王海燕,潘显萌.基于DNS重定向技术的网络安全审计系统[J].计算机科学,2016,43(Z11)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

马兆铭

硕士，工程师，现就职于上海邮电设计咨询研究院有限公司，主要研究方向为互联网信息安全咨询与设计。

doi:10.3969/j.issn.1000-1247.2018.07.015

有源室内分布系统在4G网络的使用

崔文标

中国电信股份有限公司深圳分公司

摘要 4G时代，室内分布建设仍以利旧及新建DAS室内分布系统为主。面对日益增长的网络需求，传统室内分布系统弊端日益突出。各设备商抓住机遇，各自提出颠覆传统的创新室内覆盖解决方案——有源室内分布系统覆盖方案。该创新方案具有稳定、高速率、高容量、可维可管的特点，更加适应当前的4G网络建设需求及用户需求，可完全替代传统室内分布系统，成为日后4G室内分布建设的首选方案。文中主要从规划设计及建设的角度，探讨有源室内分布系统在4G网络中的使用。

关键词 有源室内分布系统 DAS 4G

1 移动网络新时代

各种新的需求需要更庞大的数据流量作为支撑，将对现有的无线网络带来空前的压力，以及更苛刻的要求：稳定、高速率、高容量、可维可管。4G时代，覆盖是竞争关键，室内覆盖优劣成竞争关键因素。

2 传统室内分布现状

在2G及3G时代，各运营商在室内采用分布式天线系统方案，已建成相当规模的室内分布系统，并且该室内覆盖方案一直沿用至今。4G时代，对于网络速率有更高的需求，MIMO技术已成为提升速率和网络流量的最佳技术手段。如此传统的建设方案，在当今的移动流量时代呈现出力不从心的状态：

施工难——物业协调和工程施工难度日益增加；

维护难——系统网管无法管理，现场排查问题耗时长；

质量差——室内分布系统节点多、器件多，器件质量仍需提升；

MIMO改造难——实现MIMO需要增加一个通路，通道不平衡也会导致吞吐率下降。

应对4G网络的挑战，亟需一种新型室内分布系统覆盖方案以满足稳定、高速率、高容量、可维可管的网络需求。

3 创新室内覆盖解决方案

3.1 有源室内分布系统原理

各设备厂商为抓住4G网络机遇，各自提出颠覆传统的创新室内覆盖解决方案——有源室内分布系统覆盖方案。在此介绍以下三种系统：华为的Lampsite有源室内分布系统、中兴的QCell有源室内分布系统以及爱立信的RadioDOT有源室内分布系统。

3.1.1 Lampsite系统及QCell系统

华为与中兴的有源室内分布系统原理较为相似，具体方案如下：通过基带单元（BBU）的CPRI端口将光信号传输至远端汇聚设备RHUB（中兴为pBridge），远端汇聚设备将数据通过电信号传输至微型远端数字单元（pRRU），再通过pRRU的内置射频天线完成室内信号覆盖。

3.1.2 RadioDOT系统

通过数字基带单元（DU）的CPRI端口将光信号传输至室内射频单元（IRU），IRU再将中频信号通过网线传输至无线电系统（RadioDOT），DOT通过内置射频天线完成室内信号覆盖。

有源室内分布系统方案均通过光纤传输光信号、网线传输电信号。如需引入2G信号，可在BBU与汇聚设备之间引入2G馈入单元（DCU、MAU、MEU）。

图1为有源室内分布系统的组网。

如需引入2G信号，可在BBU与汇聚设备之间引入2G馈入单元（DCU、MAU、MEU）。馈入2G信号的华为&中兴系统组网如图2所示，爱立信有源室内分布系统组网如图3所示。

3.2 有源室内分布系统建设

有源室内分布系统的实际建设中，信源BBU可集中放置于机房或随站点放置，并为其提供直流供电。汇聚设备（RHUB、pBridge、IRU）可根据设计方案中远端天线的位置选择集中或分散放置于弱电井，使用市电220V交流电进行

供电，BBU与扩展单元之间通过尾纤进行信号传输。有源天线单元（pRRU、DOT）安装于站点天花板，或通过外置天线型号通过馈线外引板状天线覆盖电梯井，扩展单元与有源天线单元之间通过超五类线或六类线进行信号传输，并对其进行供电。实际建设如图4所示（以中兴QCell系统为例）。

3.3 有源室内分布系统优势

与传统室内分布相比，有源室内分布有多个方面的优势。

3.3.1 易部署

从上述组网图可直观地看出，除使用外置天线设备及馈入2G信号需要用到馈线以外，4G有源室内分布系统完全抛弃了粗重的馈线，全套系统采用细软的尾纤及网线完成部署。

3.3.2 广覆盖

与传统室内分布相比，远端射频单元功率强于传统室内分布天线，部署密度低。在此列举不同场景下，有源与无源的天线间距对比见表1。

3.3.3 弹性容量

传统室内分布系统容量取决于信源RRU，系统建设完成时即确定该站点的小区数，扩大容量首先需要增加信源容量，需要二次上站安装设备等，容量调整不灵活；有源室内分布系统则更为灵活，单套系统多个小区，容量可达DAS系统的数倍，可通过后台网管系统设置小区合并或小区分裂，从而灵活调整容量。

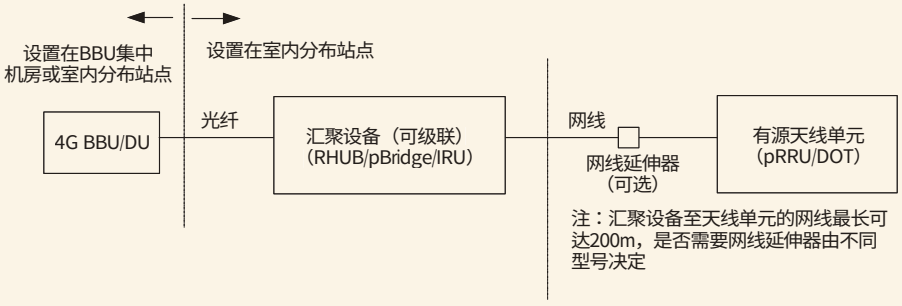


图1　有源室内分布系统组网示意

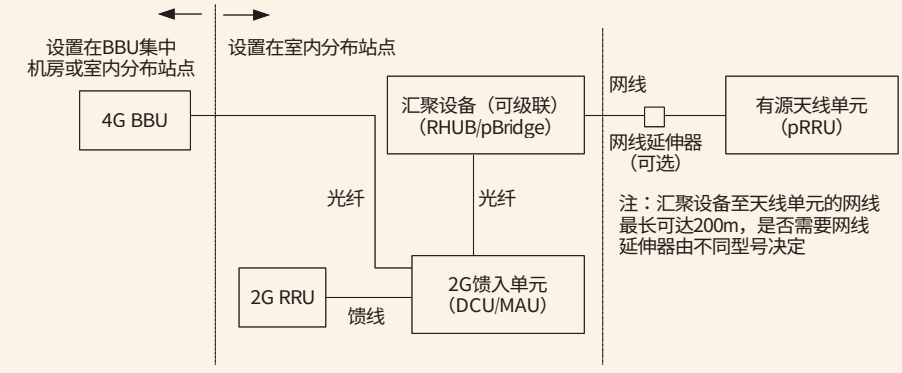


图2　馈入2G信号的有源室内分布系统组网示意（华为&中兴）

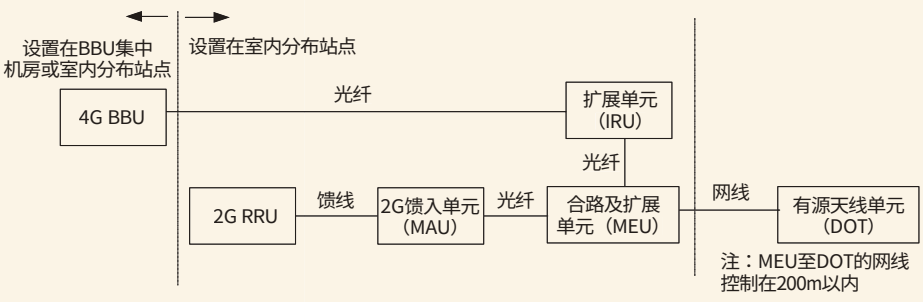


图3　馈入2G信号的有源室内分布系统组网示意（爱立信）

3.3.4 可维可管

传统室内分布系统的网管在末端只可监控到信源RRU，分布系统处于监控盲区，分布系统出现故障时，需人工现场从多角度分析定位故障点。而有源室内分布系统从信源BBU到末端的射频单元，各节点设备均可由后台网管监控，网络状态一目了然。

3.3.5 多模多频集成

站点引入多种频段时，传统室内分布系统需增加不同频段的信源RRU，新增或更换合路器等。部署MIMO时，需新增一套DAS系统，建设困难，且双链路容易出现不平衡的情况，反而给用户带来较差的上网体验。有源分布系统本身已集成多模多频，一次工程、一套系统即可支持MIMO。

除以上优势之外，有源室内分布系统远端射频单元造型时尚美观、类似Wi-Fi路由器，更容易被业主及用户接受。各厂商产品造型示意如图6所示。

4 有源室内分布系统的使用

4.1 适用场景特点

前期已有测试数据表明，

在单用户话务贡献能力方面，有源室内分布系统是DAS系统的120%左右。在单位面积话务贡献能力方面，除居民住宅低话务场景外，其他场景有源室内分布系统贡献能力均是DAS系统的1.15倍以上。在高话务场景的学校，有源室内分布系统话务贡献能力是DAS系统的近20倍；用户平均速率方面，各场景下，有源室内分布系统明显优于DAS系统，用户下行速率基本是DAS系统的10倍左右，上行速率是DAS的3倍左右；业务平均时延方面，在各场景，有源室内分布时延均小于DAS，平均时延减少7ms以上。

为建设高质量的4G网络，提高用户体验，有源室内分布系统更适合部署在话务量大、人流量大的高价值区，具有性能优、容量大、部署方便、成本低的优点。

(1)在人流量大、话务量大、空旷隔断少的场景，比如火车站、机场、大型商场等，有源室内分布造价和新建DAS的造价相当或略低。

(2)在隔断较多的场景，比如经济型酒店、医院、宿舍等，有源室内分布的造价比新建DAS造价略高。具体见表2。

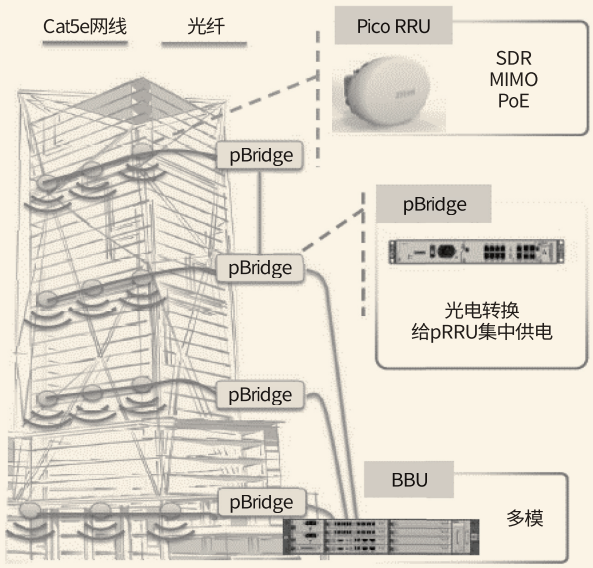


图4　QCell系统部署示意

表1　有源无源天线间距对比

场景类型	有源点位间距（m）	无源天线间距（m）	比例
机场	33	17	1.94%
车站	28	15	1.87%
写字楼	26	14	1.86%
商场	33	18	1.83%
会展中心	28	15	1.87%
酒店	18	14	1.29%

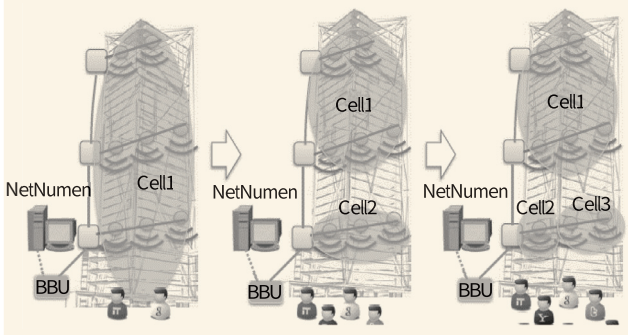


图5　小区规划示意

4.2 案例分析

以下分析实际建设的有源室内分布系统站点案例，分别为高校、大型购物场所、汽车站和办公楼。

(1)某高校

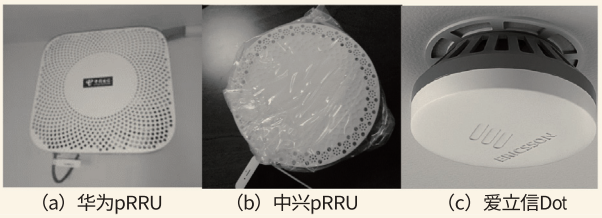
某学院分为宿舍区、教学区和食堂，共有1万人。此次采用20MHz带宽的2100MHz的QCell覆盖栋宿舍楼，共1884个房间，采用了4个站，共40个小区，89个pRRU。

校园内部有一个15MHz带宽的1800MHz宏站，建设在食堂楼顶，共三个小区，小区50覆盖A、B、C三栋宿舍楼和教学楼，小区49覆盖D、E、F、G 4栋宿舍楼。

根据覆盖目标，采用链路预算、射线跟踪仿真和点信源摸测相结合的方式，确定如下方案：隔层部署，2层和5层各安装一层pRRU；单pRRU单边覆盖4个房间，共覆盖24个房间，约500m^2；安装位置在走廊水泥屋顶，采用钢筋下沉的方式，大部分位于两个寝室之间，正对隔墙。

QCell部署后，测试数据见表3。

按照RSRP≥−110dBm的标准，覆盖率为98.4%。最差



(a) 华为pRRU　(b) 中兴pRRU　(c) 爱立信Dot

图6　各厂商产品造型示意

表2　不同场景成本对比

场景	成本比例
大型交通枢纽	0.85:1
大型办公场所	1.23:1
大型购物中心	1.04:1
学校宿舍楼	1.34:1
小型办公场所	1.12:1

楼层的下载速率77%，部分大于70Mbit/s；最好楼层的下载速率绝大部分大于70Mbit/s，平均值接近100Mbit/s。由此可以看出，覆盖和性能均得到明显提升。

(2)某大型购物场所

一座集购物、餐饮、休闲、娱乐为一体的大型综合购物中心，日均人流超过1万人次，周末达到2万人次。

该购物中心有地下1层、地上5层和夹层空间停车场，单体总建筑面积约15万平方米，外墙主体为混凝砖土，内墙贴有玻化砖，在3个出入口处有镂空玻璃幕墙，除3个出入口位置，建筑物其他外墙均无窗。

其室内人流密集，高端用户集中，业务量大，要求同时兼顾覆盖和容量，商场物业对覆盖部署要求高，易安装、易维护的同时要兼顾美观性和隐蔽性。其商场经营业态丰富，主要包括百货、超市、影院、各种餐饮、游乐区等。

在对该商场进行了QCell有源室内分布系统部署后，对网络进行测试，具体如图7所示。

下载速率峰值从62Mbit/s提高至150Mbit/s，覆盖与速率都得到非常明显的提升。

(3)某市汽车站

某市汽车站候车大厅高达12m，总面积超过1万平方米，为该市最大的汽车客运站。施工时间紧，建设传统室内分布困难重重。且业主因为传统室内分布馈线需要在钢结构的横梁走明线，非常抵触传统的室内分布建设方案。因此对该点采用有源室内分布方案：一层候车大厅共使用8个DOT点，覆盖130m长、80m宽超过10000m^{2}的敞开式区域，平均每个DOT覆盖超过1200m^2；二层和三层商铺办公区域考虑到隔断较多的情况，共使用了4个DOT进行覆盖。图8为该站点候车大厅的点位平面图。

全部设备安装仅用了两个晚上共计10个小时时间，在客户认为不可能的情况下，完成了客户在清明小长假流量高峰前建站的任务。开通DOT后，日均流量迅速由2GB增长到7GB，目前平时日均流量已经到达10GB。

(4)某地办公楼

该办公楼共9层高，约10800m^2。该楼为室外宏站覆盖盲区，收到较多投诉。

为紧急处理该楼的客户投诉，该点采用有源室内分布系统进行覆盖，办公楼共需5个小区，36个DOT点位，并在6天内成36个点安装并开通。覆盖方案点位图如图9所示。

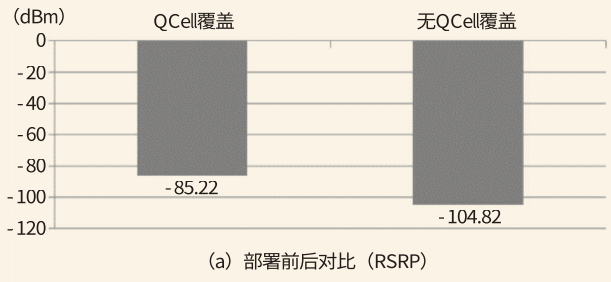
站点开通后，对该楼分别进行了RRC连接用户数及用户总流量的数据统计，如图10所示。点系统站点开通后RRC连接用户数显著提升；日均下行流量增长5.5倍，日均上行流量增长9.8倍。

开启有源室内分布系统后，该系统在各定点测试中的无线环境良好，速率表现优秀，极大地提升了原本宏站覆盖区域的吞吐率。

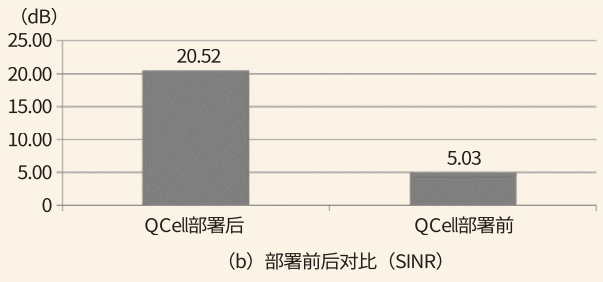
从上述测试结果可以看出：该有源室内分布系统解决了高质量高话务场景的需求，安装后零投诉；施工便捷，满足办公人员无线网络部署需求；安装后各项性能指标提升明显，流量快速增长，收益明显。

表3　测试数据对比

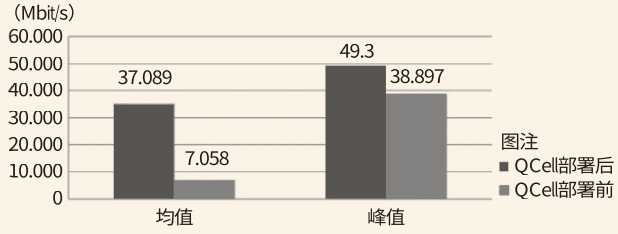
楼层	RSRP均值	SINR均值	下载速率均值
部署pRRU的楼层	＞-80dBm	＞25dB	100Mbit/s
无部署pRRU的楼层	＞-95dBm	＞20dB	70Mbit/s



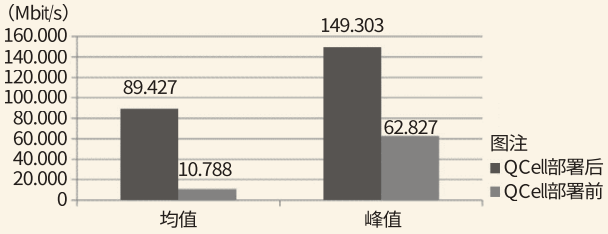
(a) 部署前后对比（RSRP）



(b) 部署前后对比（SINR）



(c) 部署前后对比（上行速率）



(d) 部署前后对比（下行速率）

图7　QCell部署前后对比（覆盖/速率）

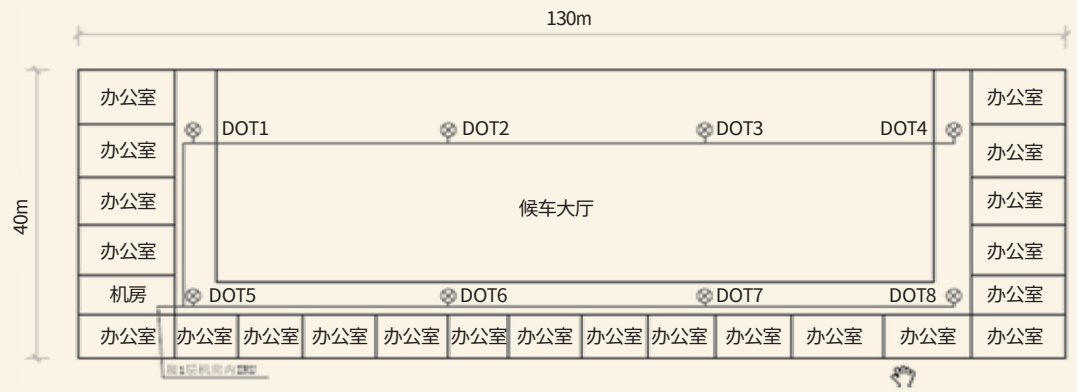


图8　候车大厅点位平面图

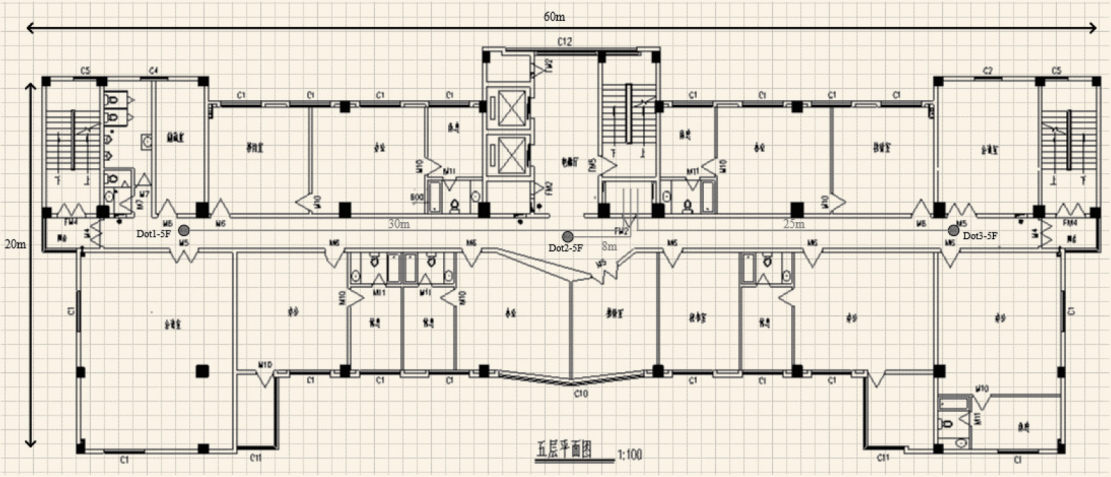
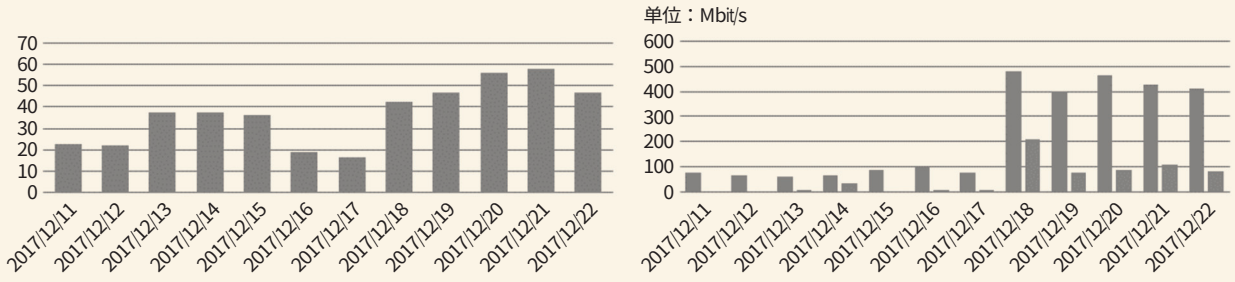


图9　点位平面安装图



图注：■ RRC连接用户数

(a) 开通前后RRC连接用户数对比

图注：■ PDCP下行流量 ■ PDCP上行流量

(b) 开通前后PDCP上下行流量对比

图10　18号站点开通测试对比

5 结束语

有源室内分布系统具有稳定、低延迟、高速率、高容量等优点。在规划设计、建设及运营方面均有着传统室内分布无法比拟的优势，充分满足当前室内分布建设需求、用户网络需求，极大地提高室内网络质量，给予用户更好的上网体验。

参考文献

[1] 未来五年移动数据流量增长八倍[Z].中国信息产业网—人民邮电报(北京),2016

[2] 苹果APP Store 10年:下载量与用户收入均超千亿[Z].新浪财经,2018

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

doi:10.3969/j.issn.1000-1247.2018.07.016

人工智能中的个人信息保护

鲁泽霖
北京邮电大学国际学院

摘要 随着人工智能的不断发展，个人信息保护成为人们关注的重点问题。阐述人工智能技术对法律法规提出的新要求，从多个方面分析人工智能对个人信息保护的影响，并讨论人工智能技术中个人信息保护立法的国际进展及未来的立法方向。

关键词 人工智能 个人信息保护 立法

1 人工智能技术对法律法规提出新要求

随着计算能力的提升、数据的爆发式增长、机器学习算法的不断进步，人工智能技术正在兴起和成熟。自动驾驶、无人机、智能医疗、工业机器人、智能家居助手等人工智能产品和应用孕育兴起。随着人工智能技术的快速成熟和普及，采集用户个人信息的频次大幅增多，自动采集更为普遍，人工智能产业高速发展的同时，凸显了法律、伦理规则滞后的问题。

与互联网、大数据、云计算等技术不同，人工智能技术有其独特性质，规则制定应与产业发展同步，甚至适度早于产业发展。传统互联网领域的立法思路是坚持鼓励发展、宽松包容的原则，产业发展先行，待问题暴露之后再根据实际需要制定相应的法律规则。但人工智能自主性及其带来的控制等问题，使得监管面临着以前从未有过的困难，比如，自动驾驶汽车产业发展需要事先制定相应的法律法规，才能试运行。如果不事先设定好相应的规则，事中和事后的监管以及法律责任关系的处理就变得非常复杂。一方面，人工智能依赖的核心技术是以深度学习为代表的机器算法，使得人工智能应用或程序具备飞速的自我学习能力。例如，谷歌研发的围棋机器人AlphaGo通过数据训练和自主学习，一年之内击败了包括李世石、柯洁在内的人类顶尖棋手。在AlphaGo出现前，人工智能专家们认为还需要5～10年才能够出现具备与人类围棋世界冠军分庭抗礼的计算机程序。另一方面，人工智能技术依赖机器学习算法产生决策的过程难以把控，这对于监管机构和企业来讲都是难题。由于当前人工智能以大数据和深度学习为基础，在面临动态变化的环境，信息不完全、存在干扰或虚假信息时，人工智能系统可能做出错误的判断或决策，这是企业难以预料和需要提前应对的。此外，机器学习算法和数据都是企业的核心资产和商业机密，监管机构难以知悉，更难以在用户受到损害时还原事件原委。

人工智能技术立法思路还没有明确答案，但在基本原则方面形成了一些共识。2017年1月，在加利福尼亚州举办的阿西洛马人工智能会议上，知名物理学家史蒂芬·霍金、特斯拉CEO埃隆·马斯克及近千名人工智能和机器人领域专家联合签署了阿西洛马人工智能23条原则，呼吁全世界在发展人工智能的同时严格遵守这些原则，共同保障人类未来的利益和安全。此原则由生命未来研究所（Future of Life Institute）订立，实际上是对1942年提出的“机器人三大定律”的延伸性诠释，涵盖科研问题（5条）、伦理价值（13条）、长期问题（5条）在内的三类规则，体现产业对人工智能长期安全的担忧。

2 人工智能对个人信息保护的影响

人工智能技术在个人信息收集、使用及其他环节上都发生了根本性的变化，对个人信息保护问题提出新挑战和新问题。

第一，个人信息收集规则发生转变。传统收集规则和人工智能技术特点之间的矛盾在人工智能时代将逐渐凸显。目前，在用户个人信息收集过程中，需要征求用户同意，并告知目的和范围，不得收集与提供服务无关的个人信息。人工智能技术收集用户个人信息的普遍化、规模化，使得征求用户同意的过程变得极为频繁，同时一些人工智能技术的即时性特点导致征求用户同意变得不可能。例如无人驾驶技术中，正在行驶的无人驾驶车辆通过摄像头采集行人信息，就无法逐一征求被征集者的同意。同时，人工智能技术往往依

赖大数据技术，通过深度学习来提高人工智能技术水平，需要采集尽可能多的信息以有利于人工智能深度学习，大规模的机器自动收集着成千上万的用户数据，涉及到包括个人姓名、性别、电话号码、电子邮箱、地理位置、家庭住址在内的方方面面，这些数据的海量收集形成对用户的全面追踪。

第二，个人信息使用方式发生调整。相较于网络运营者收集个人信息的方式，在人工智能场景下，个人信息收集的方式变得更为普遍、频繁，对个人信息的组合使用更为常见，以提高人工智能技术的智能化，促进人工智能深度学习。特别是为了提高数据收集、分析能力，个人信息共享场景发生深刻变化，人工智能技术向第三方共享的场景大为增加，且难以实时获取用户同意。大数据分析技术广泛使用，数据经挖掘能分析出深层信息，不仅可以识别出特定的个人，还能分析出个人的购物习惯、行踪轨迹等信息，进一步扩大了隐私暴露的风险。

第三，个人信息相关环节出现变化。收集、使用环节是个人信息保护的重点，除此之外，个人信息保护还包括存储、跨境传输等环节。在这些环节中，人工智能技术也对传统个人信息保护造成影响，带来新的问题，需要予以新的考虑。同时，涉及个人信息泄露问题，在人工智能领域也面临新的挑战。在整个数据的生命周期中，由于黑客攻击、系统安全漏洞等原因，个人数据始终面临着被泄露的安全风险。

3 人工智能技术中个人信息保护立法的国际进展

美国、英国、日本等国家近年来已经看到人工智能带来的正面影响，但同时也注意到人工智能在法律和伦理方面存在的问题和挑战，政府、行业和企业等各方面主体都开始考虑相关应对方案。

主要国家出台的人工智能战略或官方报告都涉及到人工智能伦理和法律问题，一些国际组织开始从行动上致力于研究和应对这一难题。

联合国教科文组织和世界科学知识与技术伦理委员会（COMEST）于2016年联合发布一份关于机器人伦理的初步草案报告，对机器人以及机器人技术造成的伤害承担机制进行讨论，认为人工智能系统决策“可追溯”是至关重要的。美国国家科学技术委员会于2016年10月发布《国家人工智能研究和发展战略计划》，将人工智能涉及的法律和伦理问题解决作为7大战略之一，认为当前需要研究及了解人工智能的伦理、法律和社会影响，并开发设计符合伦理、法律和社会目标的人工智能系统方法。英国下议院的科学和技术委员会于2016年10月发布一份关于人工智能和机器人技术的报告，其中的“伦理道德和法律”方面阐述了人工智能的创新发展及其监管带来的一系列潜在问题和挑战，包括传统方法无法检验和确认不断发展的人工智能系统、人工智能决策透明化缺失、自动驾驶汽车归责制度尚未建立等，倡导建立一个更加多元化的人工智能领导委员会，监管不断变化的科技实践。

从国际社会重点关注的问题来看，主要涉及到机器人伤害责任分担、数据滥用、算法歧视和机器人法律地位等4个方面。其中个人信息保护无疑是重点问题。值得注意的是，数据匿名化是发达国家个人信息保护立法中的新动向，以保证实现技术发展的同时，避免个人数据被挖掘和滥用。欧盟《一般数据保护条例》对个人数据处理中的匿名化进行了模糊的要求，规定个人数据存储的形式能够识别数据主体的程度不得超过数据处理目的的必要。日本《个人信息保护法》对匿名个人信息的生产、向第三方提供和禁止识别进行详细规定，明确个人信息匿名标准、商业经营者公开义务，以及向第三方提供匿名个人信息的声明要求。

4 未来立法方向

不同时期的个人信息保护的诉求大不相同。前互联网时代和互联网时代，人们对于个人信息保护的态度相差较远。渴望交际是人的基本情感需求之一。在前互联网时代，很多人都主动把自己的个人信息向社会公布。然而，进入互联网时代后，人与人之间交流联系越来越方便，沟通联系的诉求相对饱和。个人信息的传播和滥用开始演变为对个人生活安宁的侵犯。人工智能时代，个人信息保护应当秉持什么样的原则，决定了未来相关立法的思路和走向。个人信息保护规则需要适应新的技术环境的要求，在人工智能技术运用场景下，与国内个人信息保护现行立法的制度匹配，对收集、使用、存储、跨境等环节进行逐一设计。

我国在顶层战略中专门强调了人工智能法律法规、伦理规范和政策体系建设的重要性。2017年7月20日，国务院印发《新一代人工智能发展规划》，在战略目标中对法律和伦理体系建设提出要求：到2020年，部分领域的人工智能伦理规范和政策法规初步建立；到2025年，初步建立人工智能法律法规、伦理规范和政策体系，形成人工智能安全评估和管控能力；到2030年，建成更加完善的人工智能法律法规、伦理规范和政策体系。法律法规和伦理道德框架作为人工智能产业健康发展的保障，未来应开展与人工智能应用相关的民事与刑事责任确认、隐私和产权保护、信息安全利用等法律问题研究，重点围绕自动驾驶、服务机器人等应用基础较好的细分领域，加快研究制定相关安全管理法规。

总体思路上，需要在个人信息保护的框架下，围绕人工

（下转71页）

doi:10.3969/j.issn.1000-1247.2018.07.017

城域传送网接入层光缆分层建设分析

赵小军　朱家胡
中国移动通信集团广东有限公司中山分公司

摘要　从现阶段接入层光缆建设模式出发，提出接入层光缆分层的概念，具体分析接入层光缆分层模型，进而分析各分层模式的纤芯分配情况，并总结接入层光缆改造模型的意义。对于传送网接入层光缆规划、建设和优化具有一定的参考意义。

关键词　接入层光缆结构　主动分层　主干光缆　配线光缆

1 引言

目前，部分运营商城域传送网接入层光缆建设思路基本上是面向业务的，即跟着基站业务走的被动建设模式。这种模式主要是以镇区汇聚层节点为中心，以环状、辐射状或树状向外覆盖，同一镇区内的接入层光缆未分层进行建设，当有新的基站业务需求时直接从临近的光缆进行割接，并抽取部分纤芯至该基站。这种未分层、面向业务的接入层光缆建设方式存在以下几个问题：首先，不利于传送网整体规划，特别是在城域传送网接入层很难形成一种分层分区、有序接入、适当超前的建设和管理理念；其次，由于新业务的地点、范围以及带宽需求的不确定性，接入基站节点承担着新业务的接入任务，如光纤接入大客户或集团用户，以及出租光纤业务，目前跟着基站业务走的这种纤芯分配方式，导致光纤调度不灵活，接入层光缆通融性差，势必影响今后新业务的发展；最后，这种建设模式产生大量的接入层跳纤点，增加线路损耗和故障点，不利于施工及维护。

因此，在建设城域传送网接入层光缆时，非常有必要引入分层建设的主动模式，将接入层光缆分成接入层主干光缆和接入层配线光缆。将现有的接入层光缆暂时划分为接入层配线光缆，大力建设接入层主干光缆。待接入层光缆网络分层建设形成一定的规模后，对接入层设备组网的纤芯路由占用进行整改，以FP点（光汇聚点）为中心来划分接入点的归属区域。

2 现阶段城域接入光缆结构

现阶段面向业务被动的城域接入层光缆建设模式主要有主干直接分纤、接入点直连、光交接箱分纤和基站汇聚分纤4种典型的接入层光缆结构，具体的方式和缺点表述如下。

(1)主干直接分纤：在大芯数主干光缆新做接头，割接抽取部分纤芯至接入点。

这种光缆结构安全性、衰耗特性、经济性方面都很不错，但纤芯利用率低，且因为纤芯分配复杂，在割接时容易出错。宜使用在管道资源匮乏、接入点较为密集、需布放大芯数光缆的地区。

(2)接入点直连：基站至两个汇聚节点（或同汇聚点的两个路由）需经过其他几个接入点的跳纤，光缆在接入点全进全出，并全部成端在ODF上。

这种结构的缺点是故障点多、衰耗大、扩容性差、经济性差；优点是纤芯可利用率是最高的，而且施工操作简单。可应用在接入点稀疏、不需建设大芯数光缆的地区。

(3)光交接箱分纤：与主干直接分纤类似，不过在密集地区使用光交接箱代替光接头，经过交接箱间接分纤。

这种结构除了投资较大，应用范围有限制外，不仅具有直接分纤原有的优势，还具有很高的纤芯利用率与维护简便的优点。可视周边市场发展情况和发展潜力，在接入点非常密集的写字楼区、住宅区、商业区等区域使用。

(4)基站汇聚分纤：对于一些零散、无法直接接入主干光缆或汇聚节点的基站，可以末梢形式串接到附近基站，由该基站分纤跳接后接入主干。

这种接入方式的缺点在于网络的安全性比较差，当相对靠近主干的基站发生中断时，可能影响到多个基站的业务。在山区，接入路由比较单一，这种接入情况会比较常见。

3 接入层主干光缆改造

3.1 城域光缆层次及接入层光缆分层

将接入层光缆进行层次划分，分为两层：接入层主干光

缆和接入层配线光缆。将现有的接入层光缆暂时划分为接入层配线光缆，大力建设接入层主干光缆。城域传送网光缆分层示意如图1所示。

图1中可看出，光缆网络分为骨干层光缆、汇聚层光缆、接入层光缆。骨干层光缆是用于沟通骨干机楼之间的光缆，一般为骨干节点间直达光缆。汇聚层光缆是用于沟通汇聚层节点之间、汇聚层节点与骨干节点之间的光缆。接入层光缆主要用于沟通接入点与汇聚层节点之间、接入点之间、接入点与用户终端之间的光缆。其中，可以把接入层光缆再细分为：接入层主干光缆，指接入层的光汇聚点（FP点）与汇聚层节点之间、光汇聚点之间的光缆；接入层配线光缆，指接入层的光汇聚点（FP点）与接入点的光分配点（DP点）之间、光汇聚点以下的接入点之间，以及接入点与用户终端之间的光缆。图1中，光汇聚点（FP点）是指接入层主干光缆与配线光缆之间的衔接点，也称为接入主干节点或光灵活分配点；光分配点（DP点）指的是配线光缆之间的调度衔接点。

3.2 接入层光缆组网模式

针对中山移动光缆管道资源现状、本地传输网的组网特点（主要是双归网络的改造）以及今后突发业务的应急能力，文中提出以下两种接入层光缆组网模式。

模式一：主干光缆单归，而配线光缆双归

模式一组网结构示意如图2所示。

说明：模式一主要用于汇聚节点的机房条件和光缆进出的路由条件较好，而FP点光缆进出路由不佳的情况。适用于市区或镇区内单汇聚节点，且接入点不需要进行双归的情况，如骨干机楼下自带的城区接入环。

模式二：主干光缆双归，且配线光缆双归

模式二组网结构示意如图3所示。

说明：模式二主要是为双归网络提供物理路由，同样适用于FP点光缆进出路由不佳的情况。 其中方式一主要应用在同一镇区内有多个汇接局的情况，如小榄、古镇、中山港等；方式二主要应用于临近镇区间组成双归网络的情况，如南头黄圃、东凤阜沙、三角民众等。

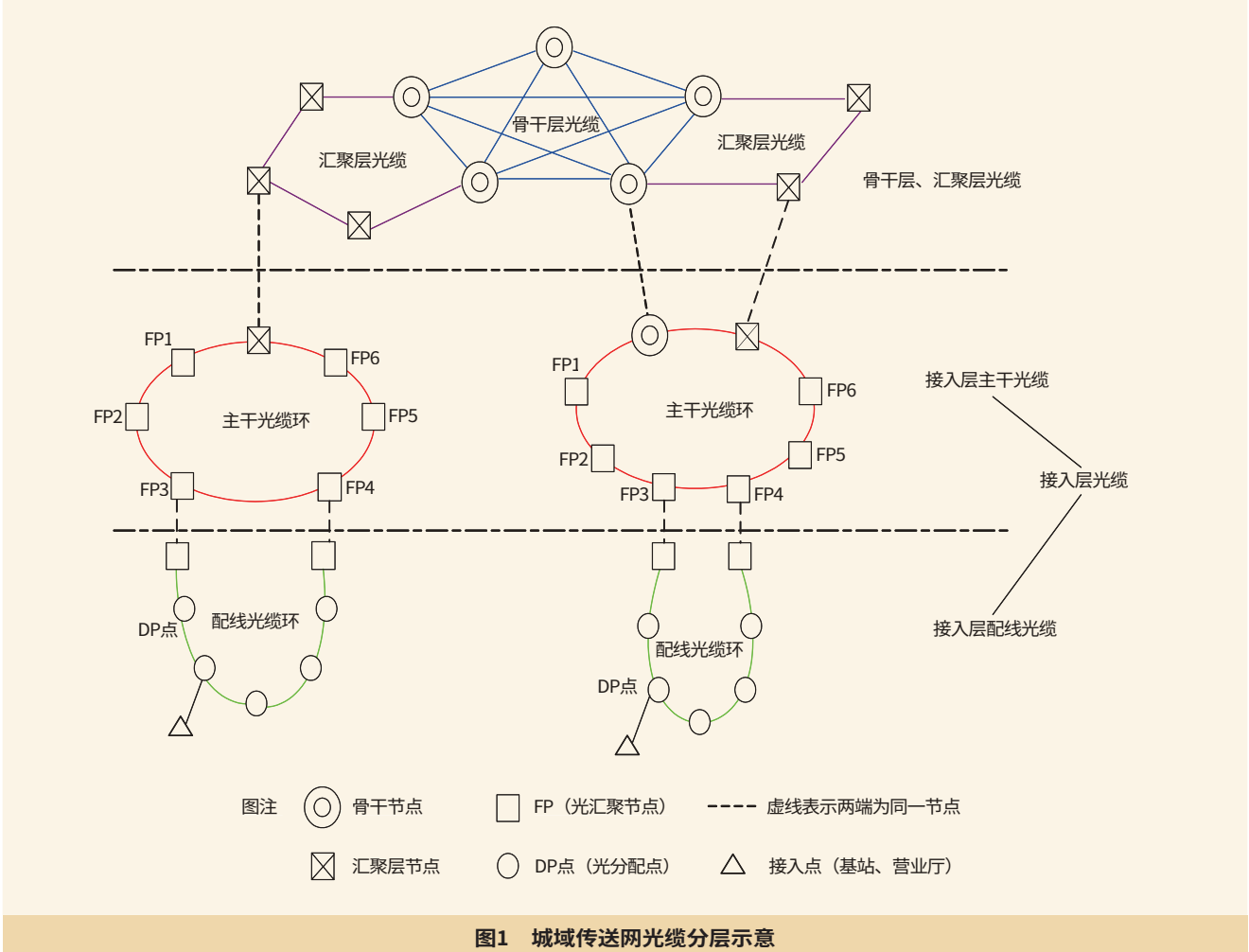


图1 城域传送网光缆分层示意

3.3 接入层光缆纤芯使用

层次化后的接入层光缆另一个重要的问题就是如何进行纤芯分配，有目的地使用不同纤芯。接入层主干光缆纤芯分配，建议采用“环型无递减交接配线法”，能够很好地解决以上问题。

接入层主干光缆的纤芯种类有：共享纤芯、独享纤芯，以及只熔接不终端的预留公共纤芯。

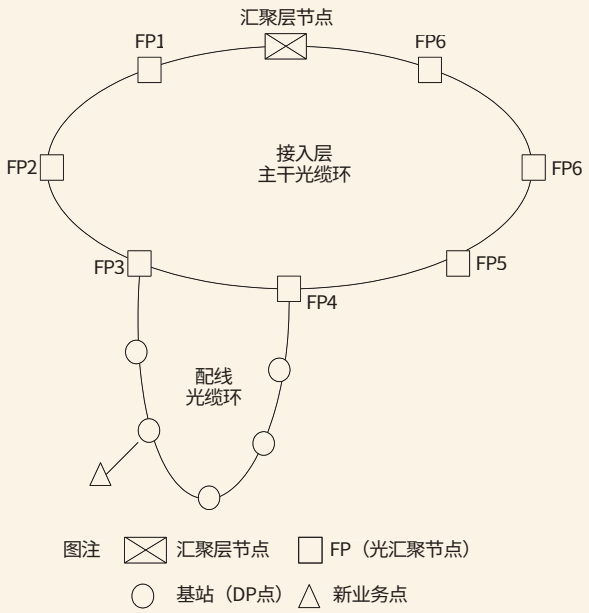


图2　模式一组网结构示意

(1)共享纤芯

在经过的每个接入层FP点都进行熔接终端，作为公共纤芯。该纤芯带一般用于SDH设备组网。也可以利用这些光纤，组成FP点（FP点设在无线基站或接入点机房时）至汇聚层节点大容量SDH或波分环为用户提供数据业务，对于不具备接入设备安装条件的节点（如室外型光交接点），可以暂不考虑配置共享纤芯带。

(2)独享纤芯

为各节点独享，每个接入层FP点独立占用主干光缆环若干芯光纤（一般为12芯），建立与上级汇聚层节点的直达纤芯通道，且有两个不同方向的光缆物理路由。独享纤芯一般先按每个方向12芯配置，在主干光缆的使用达到一定规模后再统一调整。

(3)预留公用纤芯

主干光缆预留的公用光纤在FP点内只熔接不终端，且封存在各个FP点ODF或光缆交接箱内。可以作为以上两种纤芯的预留，在业务发展过程中可将此纤芯带调整成共享纤芯或独享纤芯，以及增加新的FP点时的配纤，还可以为汇聚层组网备份第二光缆路由。

以下就两种组网模式的配纤方式加以说明。

模式一：主干光缆单归，而配线光缆双归

模式一配纤示意如图4所示。

共享纤芯：分配12芯；

独享纤芯：每两个节点分配24芯，两两共享24芯主干光缆；

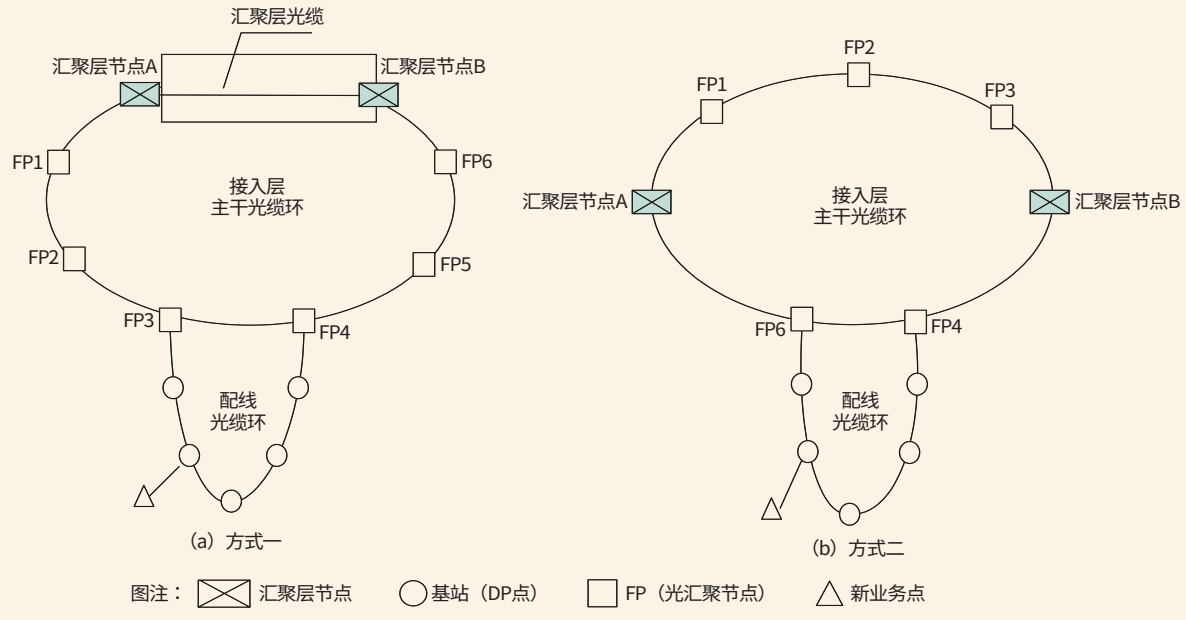


图3　模式二组网结构示意

预留公用纤芯：剩余纤芯作为预留纤芯。

模式二配纤示意如图5所示。

共享纤芯：分配12芯。

独享纤芯：每两个节点分配24芯，两两共享24芯主干光缆。

预留公用纤芯：剩余纤芯作为预留纤芯。

对于模式二，也可采用环型无递减交接接力配纤法。

模式二交接接力配纤示意如图6所示。

共享纤芯：分配12芯。

独享纤芯：FP1、FP2共同独享12芯，FP2、FP3共同独享12芯，以此类推。

预留公用纤芯：剩余纤芯作为预留纤芯。

说明：模式二第二种配纤模式“环型无递减交接接力配纤法”可以进一步提高光纤的通融性，为FP点提供更多的光纤资源，但对光纤资源的管理要求较高。

4 接入层光缆改造模式的意义

4.1 安全性

接入层主干光缆采用环型组网，为传输网络设备组网提供物理路由。由两个（一对）FP点共同管辖区域内的基站，使该区域内的接入点(基站)双归至两个FP点。接入层主干光缆上的FP点，双归至同一汇聚区内的两个汇聚层节点。即使一个FP点搬迁或变更，导致光缆割接，由于SDH环的倒换，也不会影响下带接入点的业务。

4.2 灵活方便性

采用以上方法可使接入层光缆网组网灵活方便：每个FP均有独享纤芯和共享纤芯，以及只熔接不终端的预留公共纤芯。

(1)独享纤芯：使得光缆跳纤点大为减少，并大大降低光纤跳接损耗，有利于日常维护和光纤的调度，大大缩短了

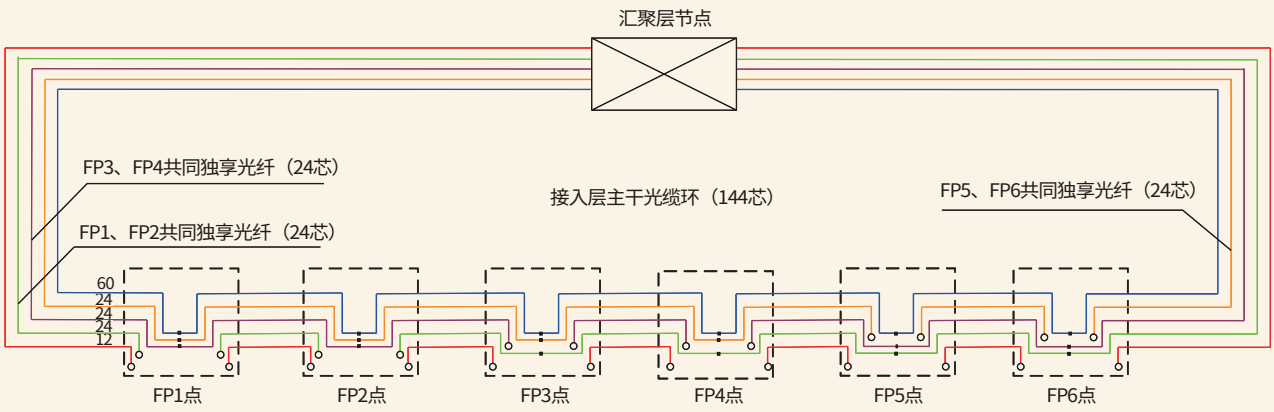


图4 模式一配纤示意

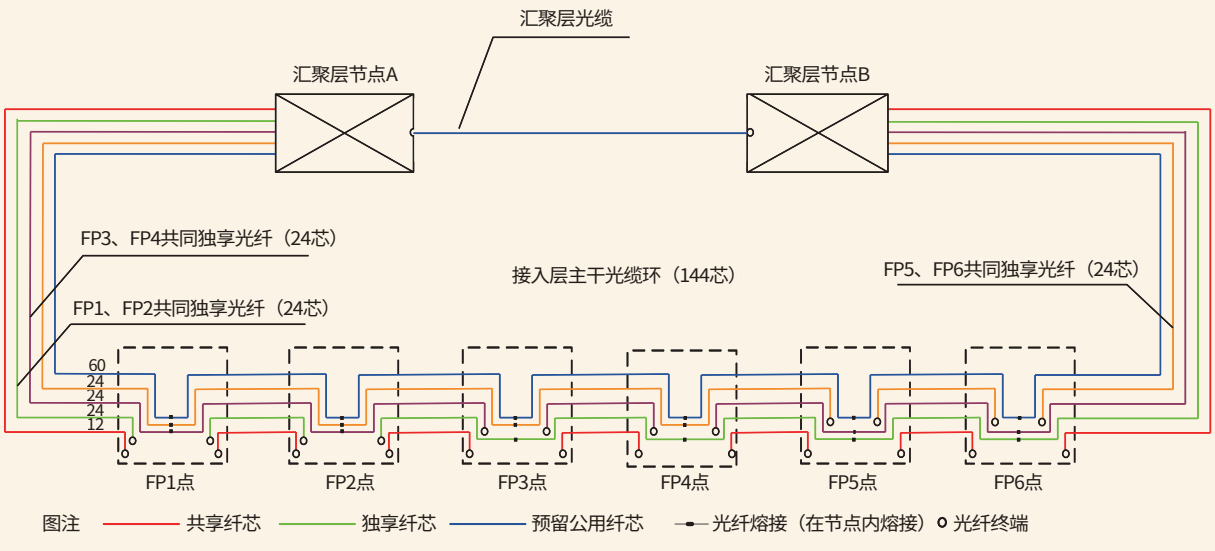


图5 模式二配纤示意

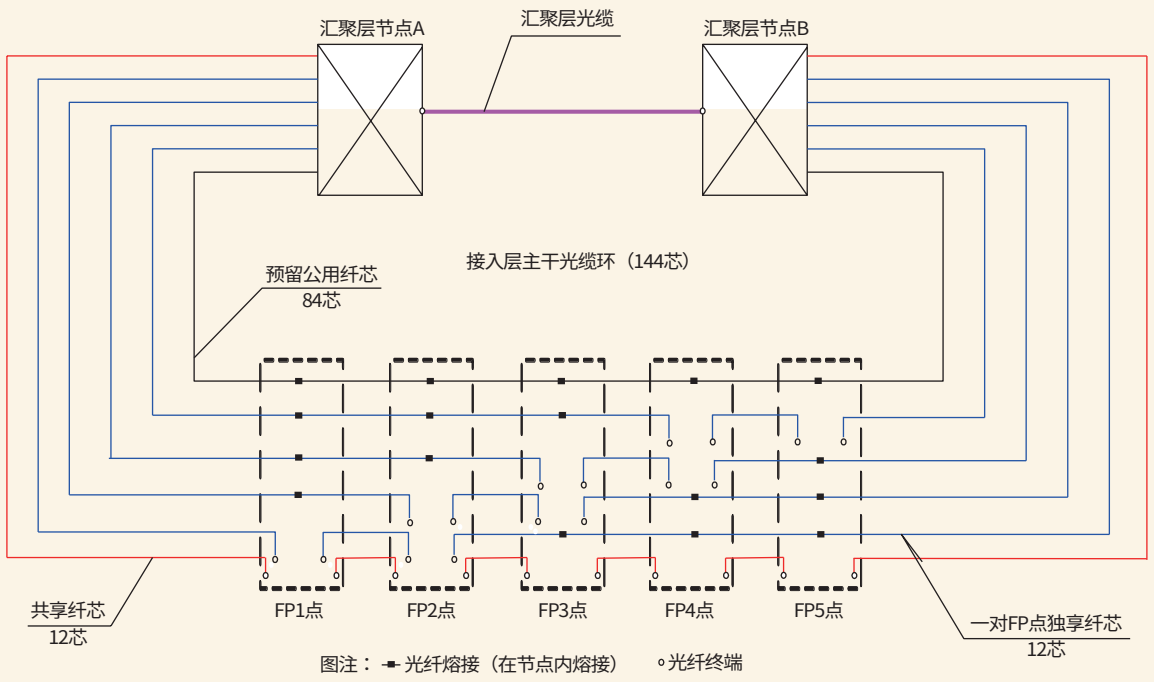


图6 模式二交接接力配纤示意

光纤调通时间。

用途：移动基站SDH设备组网、数据业务及大客户等业务。

(2)共享纤芯：使得接入层光缆网灵活性和通融性大大增加，主干光缆环上的纤芯由所有FP共享，这将大大提高主干光缆环的纤芯利用率。

用途：移动基站SDH设备组网备份第二光缆纤芯物理路由。也可以利用这些光纤，组成FP点至汇聚层节点大容量SDH或波分环为用户提供数据业务。

(3)预留公用纤芯：可以作为以上两种纤芯的预留，在业务发展过程中可将此纤芯带调整成共享纤芯或独享纤芯，以及增加新的FP点时的配纤，同时为汇聚节点间备份第二光缆路由。

4.3 扩展性

由于将接入层光缆又进行了分层，因此扩展性极佳，哪一层受限，就扩哪一层，而且能分段扩容，以下就几种扩容模式分别说明。

(1)新增汇聚节点——扩容或新增汇聚层光缆

扩容或新增汇聚层光缆示意如图7所示。

(2)接入层分层分段扩容

一般来说，一期工程的主干光缆已经能满足组建环型网的要求，扩容工程主要是满足直达光纤的需求，接入层分层扩容示意如图8所示。

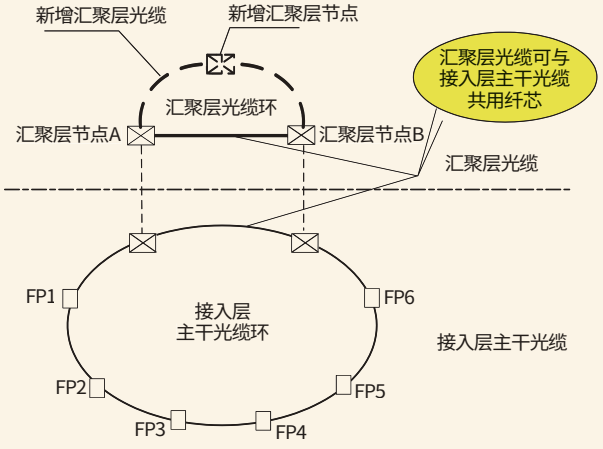


图7 扩容或新增汇聚层光缆示意

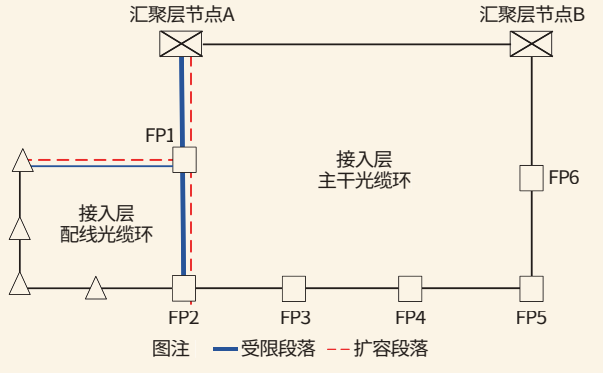


图8 接入层分层扩容示意

4.4 适应性

能满足将来业务发展需要，现有的接入层光缆可根据需要割入主干光缆环，新建的基站和新业务点应新建接入层配线光缆接入主干光缆环，FP点的预留公共纤芯也可以作为汇聚层节点间的备选第二条路由，可以为业务点提供低损耗的直达光纤。

5 结束语

(1)从战略资源上考虑

光缆与通信机楼、管道都属于传输网络的基础资源，而接入层光缆又处于传输网络最底层，最贴近用户，最能体现网络基础资源的能力。

(2)从企业的可持续发展上考虑

移动重组后，中山移动需要丰富的光缆资源支持业务，拓展和全业务运营。

(3)从业务需求上考虑

除满足现有的无线基站接入外，今后发展3G、IP客户、集团大客户、FTTH等新网络及新业务需要大量的光纤资源。

(4)从管道资源上考虑

接入层光缆通过统一规划，以及建设大芯数的接入层主干光缆，可以大大减少对管道管孔的占用，从而节省管道资源，这也符合中山移动的实际情况。

采用这种接入层光缆的建设模式和纤芯分配方式，可大大提高主干光缆纤芯调度的灵活性和纤芯利用率，为将来新业务提供光纤保证。

参考文献

[1] 中国移动传输接入网优化指导意见[Z]

[2] 广东移动本地传输网一张光缆网规划指导意见[Z]

作者简介

赵小军

本科，现任职于中国移动通信集团广东有限公司中山分公司传输资源中心。

朱家胡

硕士，现任职于中国移动通信集团广东有限公司中山分公司传输资源中心。

（上接65页）

智能技术发展情况，平衡个人信息保护与数据流通利用，引入隐私影响评估、增强透明度、灵活的告知同意机制、场景导向的思路等，处理好个人信息保护与信息经济发展的关系。实现个人对其自身信息的保护、网络信息服务提供者对个人信息的利用和国家维护信息安全之间的平衡。对此，《网络安全法》已经提出一些总体的要求，未来通过体系化的个人信息保护立法，将形成全面、明确的个人信息保护总体思路。

针对个人信息保护收集、使用等环节，应当调整个人信息保护规则，适应人工智能技术特点，做出有针对性的制度安排。坚持安全与发展相平衡的原则，既鼓励促进人工智能技术发展，同时也使个人信息得到充分保护。考虑在《个人信息保护法》中增加相关内容，或者考虑针对人工智能领域专门立法，建立特殊规则，还可以通过法律解释、司法解释等途径明确人工智能领域个人信息保护适用规则。具体来说，一是要处理好技术规则与法律规则的关系，代码是网络空间的法律，人工智能技术应用发展中已经形成一些通用的规则，这些技术规则中有哪些以及在什么程度上升为法律制度，是制定中首先要考虑的问题；二是要处理好安全与发展的关系，法律规则可为产业发展提供最基础的保障，我国人工智能领域立法要最大程度地控制和减少人工智能带来的公共危险和对私人权利的侵犯，以实现安全、可控的基本目标，对安全问题特别是公共安全问题的考虑要优先于发展问题；三是要处理好近期与远期的关系，当前阶段的人工智能更多地作为工具和产品辅助人的工作，而未来的人工智能则可能会替代人，不同阶段应该有不同的法律规则；四是处理好国内立法与国际规则的关系，人工智能的发展在全球带来的挑战是同步的，有赖于制定共同遵守的规则，在此基础上发展产业，因此，在国内立法的同时更应该跟踪、参与和推动国际规则的制定，以应对人类共同的机遇和挑战。

具体立法层面，需要进一步完善人工智能语境下的个人信息保护。在现有个人信息保护法律体系下，针对人工智能发展带来的影响，对相关制度进行动态调整。个人信息界定方面，非个人信息经过大数据分析可变成个人信息，例如智能终端设备数据、IP地址等是否属于个人信息需要未来立法进行明确。个人数据权利方面，欧盟所提出的被遗忘权、可携带权等新型数据权利已经引起各方高度重视，但其实践经验尚待验证，且对产业发展和创新存在重大影响，需要在评估其立法价值的基础上权衡是否纳入到未来个人信息保护立法之中。数据跨境流动方面，人工智能发展对数据跨境流动有着极大需求，如何在确保个人数据安全和数据跨境流动中取得平衡需要进一步考虑。

doi:10.3969/j.issn.1000-1247.2018.07.018

依托数据挖掘分析 构建移动用户差异化创新服务管理机制

熊斯敏

中国电信股份有限公司湖南分公司

摘要 借鉴银行等非电信企业的先进管理思路，基于海量数据的挖掘分析，创新变革企业移动用户信用度管理，通过对无正常授信的移动用户实施动态临时授信服务，减少良好信用用户停机，实现客户感知和企业收入双提升。以数据挖掘分析为基础，实现移动用户信用度等级精确划分和动态管理，以“动态信用度管理授信流程再造”为抓手，实现移动存量用户“动态信用度管理”客户服务管理机制创新。

关键词 动态信用度 授信流程 信用度管理

1 引言

随着移动互联网的兴起，电信行业的竞争正在从三大运营商之间的竞争演变为面向移动互联网的全产业链竞争。运营商如何能创新思维寻求突破，实现有效益地规模发展和市场份额提升成为迫切需要解决的问题。

通过分析，管理机制是制约企业规模发展的原因之一。原有移动用户服务管理机制存在以下弊端。

(1)刚性用户停机控制策略严重影响客户感知。对信用良好、通信需求稳定的用户执行信控额度为零的严格停机策略，严重影响用户满意度，甚至会造成用户投诉。

(2)简单的用户信用度管理机制造成企业收入隐形流失。对信用良好、通信需求稳定的用户执行信控额度为零的严格停机策略，抑制用户潜在通信消费能力，减少企业收益。经初步估算，造成的收入损失每月近100万元。

2 动态信用度管理的主要内涵和做法

“动态信用度管理”移动用户服务管理机制创新的内涵是：借鉴银行等非电信企业的先进管理思路，基于海量数据的挖掘分析，创新变革企业移动用户的信用度管理，通过对无正常授信的移动用户实施动态临时授信服务，减少良好信用用户停机率，实现客户感知和企业收入双提升。具体做法如下。

(1)用户圈起来，突出目标

通过梳理用户停机、授信和欠费管理现状，形成基于数据挖掘的移动用户信用度差异化服务模型，确定无限信用、零信用、无信控需求、不满足评级条件4类用户不参与移动用户动态信用度评级，确保最终参与评估的用户优质高效且可为企业带来收入。移动用户动态信用度评级分类见表1。

(2)等级细下去，精细管控

打破原有的无限信用、有限信用、无信用的三级简单用户信用管理级次，将移动用户信用度管理等级调整扩充为A、B、C 3类，5A～1C 10个等级，授信范围从政企、托收、担保以及VIP客户拓展到所有信用良好的移动用户，实现移动用户信用度精细化管理。

3 移动用户服务管理机制

移动用户动态信控由省公司集约管控，省客户服务部统筹服务，市场经营部统筹业务，省IT部负责基于数据挖掘的运营实施，各市州分公司负责服务协同以及欠费的管控。

(1)等级动起来，实现信用动态调整

每季度根据移动用户历史信用、通信需求、支付能力、违约成本和社会属性指标，对移动用户信息综合得分和信用等级进行重新评定，确保用户信用等级评定真实、准确、有效。

(2)额度控起来，实现授信精确管控

结合客服和业务部门要求，严格根据移动用户信用等级及自身消费能力精确设置动态信用额度，最高不超过50元，满足用户停机后来不及缴费的通话需求，同时最低限度降低欠费风险。

(3)流程动起来，实现用户方便快捷服务

对于选取出来的信用等级较高用户，简化用户获取动态信用额度流程，实现动态信用度主动授信，同步提供取消授

信、信用调整、特殊变更等丰富的用户短信提醒功能，确保用户能第一时间方便、快捷地获取服务。主动授信流程如图1所示。

4 主要执行方法

4.1 扩充移动用户信用管理覆盖，实现移动用户信用等级精确划分

4.1.1 梳理移动用户信用管理现状，扩充移动用户信用管理覆盖范围

“动态信用度”客户服务管理机制首先要解决的问题是：梳理用户停机、用户授信和欠费管理现状，形成基于数据挖掘的移动用户信用度差异化服务模型，扩充信用度评估用户范围至所有移动出账用户，确定如下4类用户不参与信用度评级。

无限信用用户：指用户超过缴费期后，在一定期限内享有无限量的电信业务使用权限。这类用户主要包括党政军等政企关键人及其他特殊关系户。该类用户采用免停免催的方式实现延迟停机，目前免停免催的C网用户可部分转为信控方式实现，以减少手工工作量。

零信用用户：指一旦欠费或余额不足必须马上停机，不能授予信用额度的用户，包括如下类型。

- OCS用户。
- 信用不良的用户：信用不良用户指最近6个月停机超过n次且平均停机时长超过y小时的用户，参数具体取值由数据分析确定。
- 无线上网卡用户：销售品为无线上网资费的用户。

无信控业务需求用户：指业务管理上无信控金额设置需求的用户，具体包括如下类型。

- 标准后付费用户，因为标准后付费用户出账后本来就有一个月缴费期，所以无需设置信控金额。
- 测试用户及公免用户。
- 银行托收用户。
- 内部职工用户。

不满足评级条件用户：指暂时不满足评级条件而不进行评级的用户，用户一旦满足评级条件之后则进行评级，具体包括如下类型。

- 入网3个月以内的用户：即入网时间少于等于3个月的用户，预开户用户需要从激活日期开始计算。
- 批开用户，批开用户激活之前不能参与评级。

4.1.2 实现移动用户信用度管理等级精确划分

“动态信用度”客户服务管理机制要解决的第二个问题是：综合考虑用户基本信息、业务订购信息、历史信用、消费能力、通信行为、企业风险、交往圈影响等多方面因素，通过数据挖掘精确划分移动用户信用度管理等级。

(1)信用评估指标体系设计

用户信用度即用户遵约守信的程度，外部环境、用户历史表现、用户态度及消费能力都会影响用户的信用度。

用户历史表现即在历史上客观表现出来的遵约守信记录，譬如缴费及时率、大额欠费、欠费销户等有关用户信用的记录。

用户态度包括用户忠诚度和满意度。忠诚度衡量用户对运营商业务和服务的依赖程度，譬如重复购买、预存话费、合约捆绑等情况。忠诚度高的用户，信用损坏的代价会更高，满意度衡量用户的期望与需求被满足的差距，譬如通信趋势、投诉及业务退订情况。满意度低的用户有潜在补偿心理。影响用户消费能力的因素包括身份背景、消费力和消费意愿。

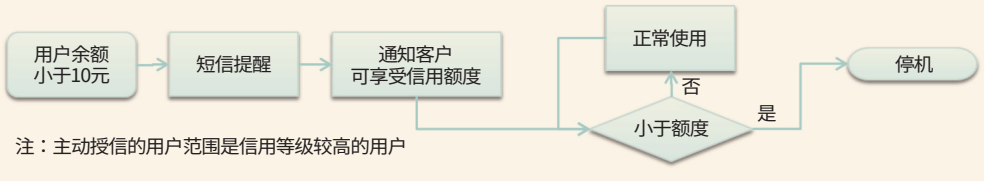
(2)根据信用评估指标体系，将移动用户分为A、B、C三大类，5A～1C 10个信用等级

A类用户分为5个等级：包括5A政企重要用户、4A职工用户和银行托收用户、3A单位担保用户及2A/1A VIP用户，沿用目前的信用等级。

B类用户分为三个等级：是根据信用度评级模型确定参与动态信控管理

表1　移动用户动态信用度评级分类

用户细类	用户数	用户所属信控范围
免催免停用户	57903	无限信用
银行托收用户	62017	
后付费用户	110763	
信控用户（钻金银）	60690	无需设置新信控金额
预付费用户（OCS）	649553	零信用用户
无需宽带用户	135906	
入网三个月以内用户	708922	不满足评级条件
出账金额0～20元用户	1046057	
建议参与评级用户	2501300	纳入动态信控管理的用户
总用户数	5333111	



注：主动授信的用户范围是信用等级较高的用户

图1　主动授信流程

信用等级评级的用户，根据信用度评估模型分别确定为3B～1B三个信用等级，授予10～50元的动态信控金额。

C类用户分为三个等级：3C信用评级模型确定的低信用用户、2C入网3个月以内暂时不能参与评级用户和1C零信用用户。

信用等级划分要求遵循易于一线业务人员理解、易于系统支撑的原则。若调整过程中遇到信用额度起伏较大的情况，需要分析确认原因并与业务部门沟通后再进行调整。

4.2 制定低风险移动用户信用度控制策略，实现客户信用度的全过程动态管控

4.2.1 用户信用度刻画

从历史信用、通信需求、社会属性、违约成本和支付能力5个方面对用户信用度进行刻画，确保移动用户动态信用度管理控制策略低风险。具体变量分类见表2。

4.2.2 定义信用不良用户

通过统计13天内停机记录（如果一个用户存在多次，则取停机前欠费金额最多的记录），观察其两个月后的复机情况，结果如图2所示。

表2　具体变量分类

变量分类	变量名称
历史信用	近6个月双停次数
	近6个月平均双停时长（h）
	最近一次双停时长（h）
通信需求	近1个月活跃天数
	近3个月平均通话时长（h）
	近3个月通话时长趋势
	近6个月漫游月份数
	近3个月平均短信次数
	同用户下产品用户数（C网、宽带和固话）
	近3个月漫游通话时长占比
	近3个月平均流量（GB）
	近3个月流量趋势
社会属性	近3个月交往圈用户数
	用户年龄
	是否校园用户
	主叫本地交往圈用户占比
	主叫交往圈用户占比
	网间交往圈用户占比
违约成本	在网时长（h）
	近6个月平均每次缴费金额（元）
	是否捆绑用户（1机补、0话补、-9未知）
支付能力	近3个月平均ARPU（元）
	ARPU趋势
	终端价格（元）

从图2可以看出，用户停机5天后复机率趋于平稳，低于3%；30天后日均复机率不足2%。因此将欠费停机30天以上未复机的用户定义为信用不良用户。

4.2.3 实时调整用户信用度等级

限制用户授信有效期为3个月，确保每季度进行用户信用度等级评估。用户授信调整需要避开春节、国庆等长假。若出现如下情况之一，则必须及时变更用户信用等级。

(1)被信控停机。信控金额用完之后仍未及时缴费造成停机的情况，每停机一次信用等级降低一个档次。

(2)过户。用户过户后3个月内不参与信用评级，因此过户后需要将信用等级置为“不满足评级条件”。

(3)套餐变更。主销售品发生变更后，保底消费金额发生变化，需要相应调整用户信用等级。

(4)VIP用户降级。VIP用户降级后，需要同步变更用户信用等级。

4.2.4 设置用户动态信控金额

根据停机前用户的欠费金额分析，欠费金额在10～50元的用户复机率最高，因此动态信控金额设置建议在10～50元。用户动态信用度管理信控金额计算公式为：

$$(Xi \times Ai - \min(Xi \times Ai)) / (\max(Xi \times Ai - \min(Xi \times Ai)) \times 50$$

其中Xi为信用度评分，Ai为用户的最近三个月的平均ARPU值：

3C等级直接置为0元；

1B～3B等级的用户按此计算公式向上按10元取整数。

具体用户信用度等级和动态信控金额设置见表3。

4.3 以“动态信用度管理授信流程再造”为抓手，实现移动存量用户“动态信用度管理”客户服务管理机制创新

4.3.1 面向用户的动态信控管理服务流程

对于实施动态信控的用户，用户可感知的服务内容包括动态授信通知服务、用户动态信控取消流程、用户消费已达

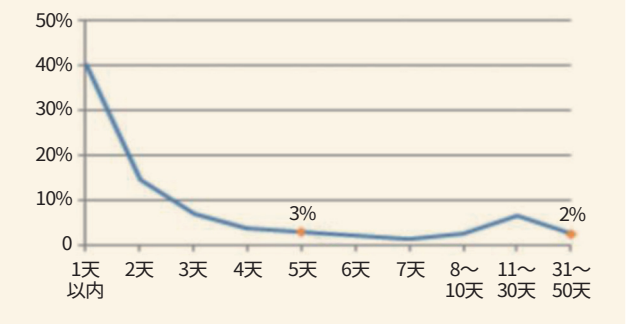


图2　停机用户复机时限

表3　用户信用度等级和动态信控金额

类别	等级	适用对象		信用额度上限（元）	动态信控	停机服务策略	费用提醒策略
A	5A	政企重要用户及重要领导		无限	不参与	免催免停，用户欠费在一个自然年度内不停机。人工催缴、停机	人工催缴
	4A	职工用户、银行托收用户		无限	不参与	后付费方式，超过缴费周期，系统自动停机	系统催缴
	3A	单位担保用户（包括其他特殊用户）		300	近3个月平均消费金额×信用等级系数	停机条件是余额+信控，系统自动催缴	余额提醒，信用额度使用提醒，缴费提醒，停机提醒
	2A/1A	VIP用户（第4类）	钻石卡（2A）	300	按集团公司规范执行	停机条件是余额+信控，系统自动催缴	
			金卡（2A）	200			
			银卡（1A）	100			
B	3B	信用度模型评定信用等级	$x1$≤信用评分	10～50	最高不超过50，且不超过套餐保底消费金额	停机条件是余额+信控，系统自动催缴	余额提醒，信用额度使用提醒，缴费提醒，停机提醒
	2B		$x2$≤信用评分＜$x1$				
	1B		$x3$≤信用评分＜$x2$				
C	3C	模型评分结果 0≤信用评分＜$x3$		0	不参与	余额不足停机，系统自动催缴	余额提醒，停机提醒
	2C	入网3个月以内用户		0	不参与	余额不足停机，系统自动催缴	余额提醒，停机提醒
	1C	零信用用户，包括OCS用户、信用不良用户和无线上网卡用户		0	不参与	余额不足停机，系统自动催缴	余额提醒，停机提醒

到动态信控额度后的提醒、用户动态信控到期后的流程等。

(1)动态授信通知服务

对于动态信用度管理实施目标用户，在余额不足时（按提醒服务规范的要求）系统自动短信主动告知，不需要用户确认，系统自动启用动态信控。

(2)用户动态信控取消流程

对于实施动态信用度管理的移动用户，可通过短信形式取消授信。

当用户成为VIP客户且申请VIP信控成功后，动态信控自动失效，依据正常信控规则对用户提供服务。

(3)用户使用临时信用额度时的提醒

对于实施动态信控的移动用户，当其可用余额不足并将使用临时信用额度时，将发送短信提醒用户。

(4)用户动态信控到期后的流程

动态信控到期后，对于可继续实施动态信控的用户，由系统自动做延期处理，并短信通知。

对于动态信控到期后的用户，如果取消其动态信控，系统也自动进行短信告知。

(5)达到信控值停机

实施动态信控的移动用户超过其动态信控额度后，系统立即触发停机指令进行停机。

4.3.2 动态信用度管理用户投诉处理流程

(1)动态信控取消流程

如用户对授予的动态信控使用功能不认可，首先由客服做好解释工作由用户通过短信取消，如果用户坚持要求取消动态授信，可做好用户资料记录工作，并派单至IT部完成用户动态授信的取消工作，并将该用户纳入动态信控黑名单。

(2)费用争议处理流程

如用户对动态信控后超出部分的使用费用不认可，首先由客服做好解释工作；如果用户坚决不认可，可对用户超出额度的使用费退费，但不进行双倍补偿；并将该用户纳入动态信控免打扰名单。

4.3.3 动态信用度管理实施管理流程

移动用户动态信控由省统一实施，具体由省市场部、服务部统筹，省IT部实施；各市州分公司负责服务协同及欠费的管控。

(1)信控名单生成

根据对信用度等级分批次提供信用度名单给大数据平台，大数据平台必须过滤当前停机数据。后续按月计算需要调整信用额度的用户清单。每三个月全量提供名单，每月提供增量名单。

(2)信控名单优化

大数据平台关联用户的实时停复机状态，将其中已停机的用户剔除掉，并将结果数据共享给CRM系统。

(3)批量授信

CRM系统批量向用户进行主动授信，并发送短信告知用户授信情况。大数据平台负责将需要调整信用额度的用户数据共享至CRM系统，CRM每月根据大数据平台提供的用户数据进行授信处理或信用额度调整处理。新授信的用户有效期为三个月（有效期内如果用户办理过户业务，系统会自动取消当前的信用额度），CRM系统完成授信后发送提醒短信。

(4)授信确认

按照“面向用户的动态信控服务内容和流程”落实好动

（下转79页）

doi:10.3969/j.issn.1000-1247.2018.07.019

LTE异频组网在特殊场景的应用

何长圣　冯昌杰

中国联合网络通信有限公司六安市分公司

摘要　六安联通通过理论分析和实践探索，在高铁沿线进行LTE异频组网应用，优化相关参数。实践证明，LTE网络异频切换时延与同频相比无较大差异，且LTE同频切换没有软切换增益。通过网络指标对比分析表明，高铁LTE异频组网是完全可行的。

关键词　高铁　LTE　异频组网　下载速率　干扰　重叠覆盖

1 引言

合武（合肥-武汉）高铁为国铁Ⅰ级双线铁路，是国家规划的“四纵四横”快速客运网的重要组成部分，该专线经六安市的金安区、裕安区、金寨县，中穿大别山进入湖北省，六安境内全长约140km。合武高铁沿线4G网络目前采用1800MHz单频点FDD组网的方式，由于FDD是小区间干扰系统，为了降低模三干扰带来的RSRP收缩及SINR较差等影响，六安联通在高铁沿线选取16km路段尝试采用LTE 1800MHz和LTE 2100MHz混合组网覆盖策略。期望通过该实验，能够为高铁场景采用异频组网的应用提供一些经验。

2 现网同频组网方案

合武高铁-六安段全长约140km，其中平原地区线路总长约44km，其余96km均为山区线路。从六安石婆店镇至金寨县斑竹园镇为隧道桥梁群，隧道桥梁群总跨长约96km，共26条大小隧道，主要有六安和金寨两个车站（如图1所示）。目前该线除隧道外，已实现FDD-LTE全覆盖，共开通61个FDD-LTE站点，均采用LTE 1800MHz同频组网方式，具体见表1。

LTE 1800MHz M同频组网方式的优点是频谱利用率最高，节约频率资源，简化频率规划，在总带宽相同的情况下，具有更高的小区峰值速率；缺点是小区边缘干扰严重，下倾角下压严重，覆盖不足。

2017年4月起六安进行了高铁专项优化，历时一个半月，共核查调整天馈67站次，对石婆店以东基站进行站内小区合并，通过本次优化指标有明显改善。

从表2可以看出，SINR和下载速率明显改善，用户感知显著提升。但是，RSRP≥-105dBm的比例下降约9%，平均RSRP下降约5dB。由此可以看出在LTE 1800MHz同频组网的配置下，为了降低同频干扰，高铁RF优化的主要方法是调整相邻两个小区之间的下倾角，但是天线下压较大后，会出现覆盖弱区甚至盲区；如果下倾角压的不多，高铁沿线两个相邻小区会出现重叠覆盖度过大的情况，模三干扰严重。

基于这种情况，六安联通在高铁沿线选取16km路段尝试采用LTE 1800MHz和LTE 2100MHz混合组网覆盖策略。具体做法为：沿线顺次一个1800MHz FDD站点和一个2100MHz FDD站点混合组网。异频组网的优点是允许较大的重叠覆盖区，保证了较高的RSRP，同时由于互相重叠的两个小区是异频，相互之间不会产生干扰，保证了良好的SINR，从而确保维持较高的下载速率。

3 异频组网方案应用及效果分析

3.1 异频组网方案

本次异频组网实验方案选取从合肥进入六安境内的第一个基站起的16km路段进行实地验证，该段路线包含乡村、开发区、城区、跨地市等多种场景，实验效果将具有一定的代表性和可复制性。六安目前的FDD1800主设备厂商为华为，UMTS2100主设备厂商为中兴，为了快速部署，尽快实施，本次实验将采取直接升级中兴U2100基站为ULTE 2100MHz基站，该实验方案只需在现网U2100基站上进行简单的改造（增加基带板）即可。本次高铁异频组网采用华为LTE 1800MHz和中兴LTE 2100MHz异厂商异频组网模式。在试点段依次交叉采用FDD1800和FDD2100混合组网，共计11个基站，列车通行时长5～6min。为了实现LTE 2100MHz与LTE 1800MHz异频间隔改造，现网对5个U2100基站进行ULTE 2100MHz升级改造，其中2T2R站点6个，1T1R站点5个。

异频组网的优势在于降低相邻小区的同频干扰，小区

表1　FDD LTE站点统计数据

地市	线路	最高时速	线路长度	线路站点数	开通站点数	开通比例	平均站间距	平均站轨距	站间距小于1.5km比例	站轨距小于400m比例	站点左侧站点数（北）	左侧站点占比	站点右侧站点数（南）	右侧站点占比
六安	合武高铁	300km/h	140km	60	61	102%	1.5km	196km	50%	84.62%	34	57.62%	25	42.37%

表2　合武高铁-六安段全段测试指标（1800MHz同频组网模式下）

地市	线路	方向	测试日期	RSRP≥−110dBm的比例	RSRP≥−105dBm的比例	平均RSRP（dBm）	SINR≥0的比例	平均SINR（dB）	平均调度值	平均下行速率（Mbit/s）	RANK 2比例	测试设备	车型
六安	合武	麻城北-南京南（DL）	2017年4月8日	-	86.74%	-93.95	88.16%	7.89	905.17	33.51	42.27%	E392	CRH380B
六安	合武	麻城北-南京南（DL）	2017年5月17日	92.50%	77.76%	-99.14	97.10%	10.29	952.23	50.73	49.60%	Coolpad 8675-A	380B

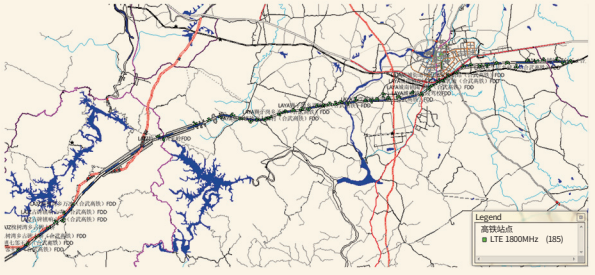


图1　合武高铁六安铁路段

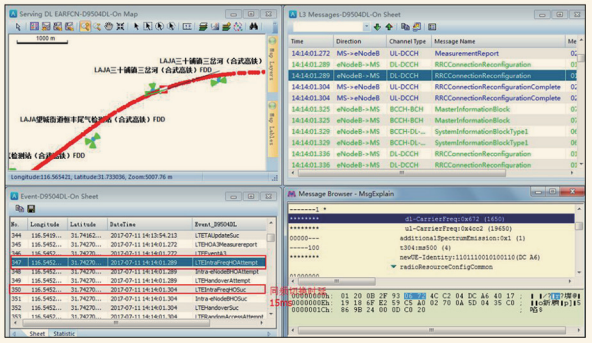


图2　同频切换时延

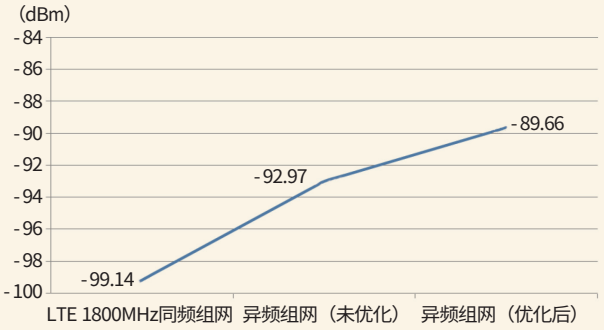


图3　异频改造前后RSRP指标对比

边缘吞吐量获得提升；缺点是异频邻区测量需要启动GAP（UE射频切换的时间），而在启动GAP的时间内，系统调度会减少25%，所以开启GAP时吞吐量会降低。

3.2 异频组网测试情况

3.2.1 同频与异频切换时延对比

首先，验证4G同频与异频切换时延的差异。

如图2所示，从发起同频切换到同频切换成功，整个同频切换时延为15ms。

LTE 1800MHz切换至LTE 2100MHz的异频切换策略采用A2+A4，通过实际测试发现异频切换时延非常小，只有26ms左右，与同频组网方案相差无几。

LTE 2100MHz切换至LTE 1800MHz的异频切换策略采用A2+A3，测试发现异频切换成功，时延也非常小，仅有26ms，与同频组网方案相差无几，LTE异频组网模式可行性高。

3.2.2 切换门限优化

异频改造后，测试发现下载速率由之前同频组网的50.73Mbit/s下降到改造后的31.4Mbit/s。分析原因是A2启动测量过早，从A2到A4事件发生的时间过长，这段时间内下载速率一般低于25Mbit/s。

A2与A4门限优化前，从1650频点切换到500频点，A2持续12s异频测量后才发生A4异频切换。由于开启GAP测量，消耗资源导致在12s内速率都低于25Mbit/s。

参数核查发现现网异频A1与A2时间迟滞设置为640ms，A1设置为−85、A2设置为−90、A4设置为−85，这样会出现长时间的A2测量，但是切换至异频网络较慢，最终导致低速率占比较长，影响用户的感知。经过不同组合参数修改尝试，将这些站点的A1与A2时间迟滞设置为1024ms，A1设置为−95、A2设置为−100、A4设置为−97，可以达到相对较好的效果。

上述优化方案实施后，复测发现速率掉坑的时间大幅缩短。A2与A4间的间隔缩短到1s左右，下载速率较低的占比明显减小，用户感知提升明显。

3.2.3 异频改造后DT指标对比

从图3可以看出，改造后平均RSRP达到−89.66dBm，将

近提升10dB。

从图4可以看出，改造优化前SINR有所降低。主要原因是改造前A2、A1、A4等参数门限设置不合理导致。修改切换门限：A1和A2时间迟滞设置为1024ms，A1设置为-95、A2设置为-100、A4设置为-97，异频组网的SINR达到12.56dB，优于异频改造前。

从图5可以看出，在异频参数没有优化到合理的区间时，异频改造后下载速率有所降低。但是对异频切换门限优化后，切换顺畅，下载速率得到提升。下载速率由改造前的50.73Mbit/s提升到57.62Mbit/s，提升幅度达到13.58%。本次实验LTE 2100MHz均采用1T1R的分集接收方式，根据此次实验结果，后期若将LTE 2100MHz扩至2T2R，下载速率将达到72Mbit/s，提升比例高达41.9%。

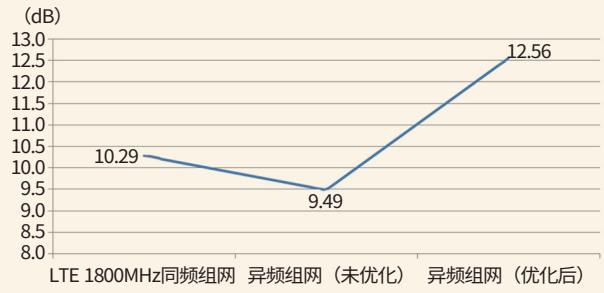


图4　异频改造前后SINR指标对比

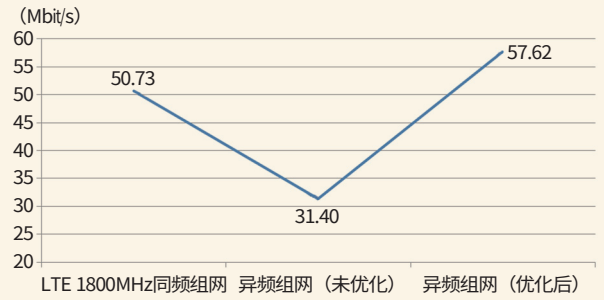


图5　异频改造前后平均下载速率指标对比

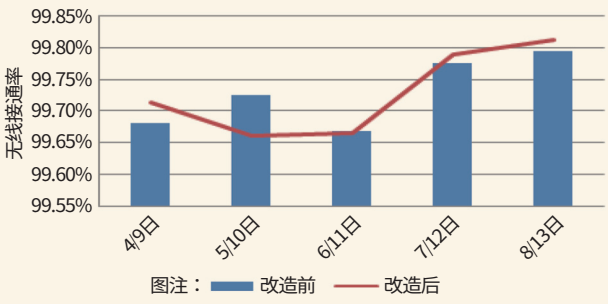


图6　2017年7月异频改造前后无线接通率指标对比

3.3 异频组网指标分析

为了验证异频组网对网络是否有其他方面的影响，六安联通对改造前后11个站点的无线接通率、掉话率、CSFB响应成功率、异频切换成功率进行了对比。

从图6可以看出，修改前5天平均无线接通率为99.73%，

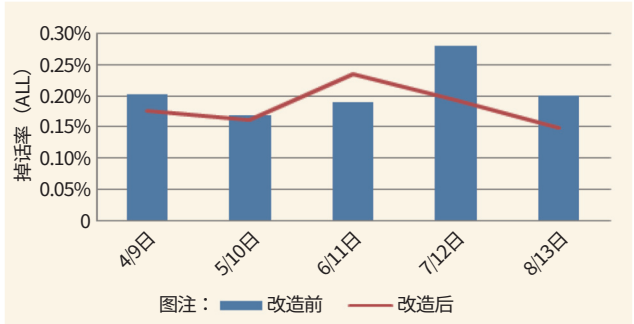


图7　2017年7月异频改造前后掉话率指标对比

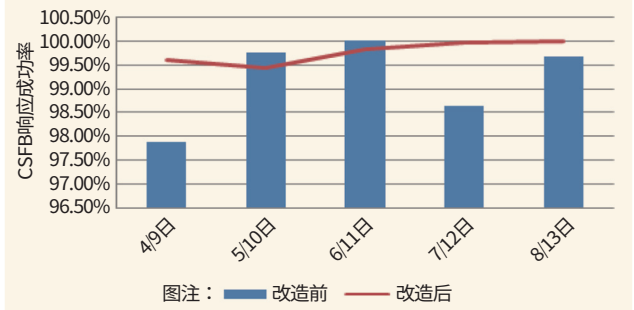


图8　2017年7月异频改造前后CSFB响应成功率指标对比

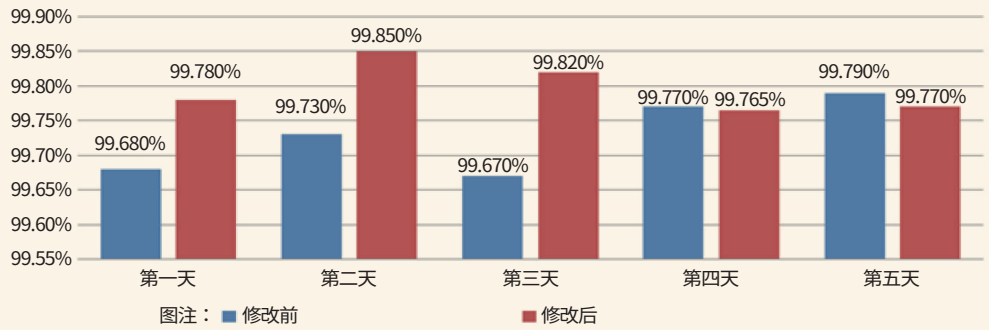


图9　异频改造前后切换成功率指标对比

改造后5天平均无线接通率依然为99.73%，改造前后无线接通率持平。

从图7可以看出，异频掉话率在改造前后分别为0.21%、0.18%，都保持在一个比较好的水平。

从图8可以看出，CSFB响应成功率由改造前的99.17%提升到改造后的99.76%。

从图9可以看出，实施异频组网后，所有改造小区的异频切换成功率为99.9%，高于同频切换率的99.65%。

从以上主要指标分析来看，异频组网在提升RSRP、SINR及下载速率的情况下，对现网关键指标无明显影响，达到预期效果。

4 结束语

从六安联通合武高铁异频组网改造测试情况来看，LTE异频组网效果明显，表现为六安高铁实验段的RSRP、SINR和下载速率均明显提升。同时从六安现网的实施影响来看，切换成功率、无线接通率、CSFB响应成功率、掉话率等关键指标均与同频组网方式下基本一致。LTE异频组网的切换时延在30ms以内，与同频组网的15ms相比，切换时延虽略有增长，但均低于用户面切换时延标准值50ms，而且对用户感知基本无影响。因此可以确认，LTE异频组网的效果优于同频组网。但是，本次实验所有数据均是在高铁时速为200km/h的条件下得出，时速为300km/h的情况有待于进一步验证。后期将测试异频组网模式下复兴号高铁在时速300km/h时的网络KQI指标及对KPI的影响，为下一步开展高铁全程异频组网优化改造积累经验。

参考文献

[1] 华为技术有限公司.LTE基本原理[Z].2013

[2] 华为技术有限公司.LTE高铁网络优化指导[Z].2015

[3] 李佳俊,宋甲英.TD-LTE和LTE FDD混合组网的互操作研究[J].移动通信,2015(8)

[4] 吴晓霞,刘云,王淑英,等.异频组网方案的应用研究[J].青春岁月,2011(14)

[5] 张晨,陆清清.LTE F/D/E多频段混合组网策略的应用[J].移动通信,2015(8)

作者简介

何长圣

本科，工程师，现就职于中国联合网络通信有限公司六安市分公司，主要从事移动通信规划建设管理工作。

冯昌杰

本科，工程师，现就职于中国联合网络通信有限公司六安市分公司，主要从事移动通信规划优化工作。

（上接75页）

态信控提醒服务和相关用户可感知的流程。

CRM授信后，用户接收到告知短信后可以回复相应指令代码进行信用额度的取消操作，由CRM系统与短信渠道配合实现。

(5)获取免打扰名单

大数据平台收集主动取消信用额度的用户信息并建立免打扰名单库保留这些信息。

(6)动态信控形成欠费的管控流程

省、市分公司加强每月移动欠费分析，及时发现欠费异常，做好问题的跟踪、协调和解决，确保动态信控后欠费可管控。

IT部加强欠费停机及时性管控，针对超过动态信控欠费的用户及时发起停机，并针对停机未成功的用户多次触发停机指令，并生成异常号码清单，供分公司核查分析。

4.3.4 成果效益

(1)方案实施后对客户服务指标增长的影响

方案实施后的分析表明：授信用户中停机过的用户占比36.85%，比未授信用户低10%，说明实施信控后能有效降低用户停机率。

通过信用度评估模型选取的授信用户信用度较好、风险较低。其在授信后3天复机率和5天复机率分别提升1.29%和2.89%。

(2)方案实施后对企业业务收入增长的影响

系统内动态授信用户212万户，经业务部门确认，1～12月份累计增收1135万元。

doi:10.3969/j.issn.1000-1247.2018.07.020

LTE弱覆盖专项优化预分析策略

张　喆
中国移动通信集团设计院有限公司

摘要　在LTE网络优化工作中，弱覆盖整治是极其重要的一环。中国移动某省公司集中网优原有工作模式存在弱覆盖问题点总量大、省网优分析人员不足、对地市的现场具体情况了解不充分等情况，导致工单分析不聚焦，对地市支撑作用不大。针对该问题，提出一套弱覆盖问题点预分析策略，得到省公司网优主管认可，并在该省某市试点阶段取得良好效果，极大提升省市两级网优工作的效率。

关键词　弱覆盖整治　功率调整　过覆盖　规划站匹配　故障告警

1 前言

当前中国移动某省公司网络优化工作仍面临两大挑战：第一，网络覆盖不足导致客户感知及网络满意度全国排名靠后；第二，深度覆盖不足已成为最大短板，是无线优化的主战场。鉴于此，该省公司面对外部和内部的多重挑战，确立了2018年无线优化工作的总体思路：紧扣公司“一二五”核心战略思想，以保障网络领先优势为目标，以“客户感知提升，保持竞对领先优势”为工作主线，推动“四个转变”，开展8项重点工作，进一步打造领先的4G精品网络。

在各项重点专项优化工作中，弱覆盖整治是极其重要的一环。该省集中网优原有工作模式为首先由省网优分析人员对弱覆盖问题点工单进行全量初步分析，之后派发地市进行详细分析。由于工单中问题点数量太大，省网优分析人员不足，加之对地市的现场具体情况了解不充分，导致工单分析不聚焦，对地市支撑作用不大；另外，地市也无法处理海量的工单。针对该问题，对问题点工单分析流程从优数量和提质量两方面进行改进，研究出一套预分析策略，使得省市两级网优工作更有效率，并取得省公司网优主管认可。

2 弱覆盖问题点派单规则及解决标准

该省某市2018年LTE弱覆盖专项优化工作主要包括4G弱覆盖整治与4G竞对弱覆盖整治两大类问题点。派单规则及解决的判断标准如下（LTE MR覆盖率≥-110dBm采样点数/RSRP总采样点，取MR开启周期的A+B类网格整体指标）。

(1)4G弱覆盖整治

对MRO数据和信令软件采集（A+B类网格）数据中符合以下情况的小区进行派单：

- 室外小区小于-110dBm采样点占比大于20%的小区；
- 室内分布小区小于-110dBm采样点占比大于10%的小区；
- 剔除采样点小于1000的小区。

已解决的判断标准为：通过MRO数据和信令软采数据进行评估，室外小区覆盖率≥80%、室内分布小区覆盖率≥90%视为已解决小区。

(2)4G竞对弱覆盖整治

对符合以下情况的小区进行派单：

- 移动覆盖率＜80%但竞对覆盖率＞80%的小区；
- 80%＜移动覆盖率＜90%但劣于竞对覆盖率5%以上的小区。

其中，竞对覆盖率为开启异频测量获取到的友商RSRP覆盖率（RSRP≥-113dBm的采样点占比），有效小区为友商月总采样点总数＞1000的小区。

已解决的判断标准为：待整治覆盖劣于中国联通、中国电信小区、属于全网开启异频测量的有效小区，移动MR覆盖率>80%且劣于竞争对手覆盖率5%以内。若移动覆盖率≥90%，则也视为已解决小区。

3 弱覆盖问题点归类规则

根据导致弱覆盖问题的常见原因，可将弱覆盖专项问题点归为参数、故障、覆盖和其他4大类，每一类均有对应的优化方案，具体见表1。

3.1 参数

3.1.1 功率调整

适当地提升小区功率可扩展小区的覆盖范围，解决覆盖

空洞，以及楼宇密集区域（城中村、CBD等）深度覆盖不足的问题。由于某市基站设备由华为、中兴两家设备商提供，下面分别论述两家设备商关于小区RS参考信号功率是否有提升空间的计算方法。

(1)华为

①通过小区RRU型号得到该小区RRU最大发射功率（W）。

②网管平台提取小区RS参考信号功率（dBm）现网值，并转换为单载波功率（W），转换公式如下。

$$P_{\text{单载波功率(W)}}=(RB\times12\times10^{\frac{PA}{10}}\times10^{\frac{RS}{10}})/1000\times N_{\text{channels}} \quad (1)$$

其中RB为小区带宽对应的RB数，PA为通过不同PA和PB值设置RS信号在基站总功率中的不同开销比例，RS为小区参考信号功率（dBm），N_{channels}为小区RRU通道数。

③功率余量(W)=RRU最大发射功率(W)-已使用功率(W)，其中已使用功率(W)为该小区共向各载波功率之和。

④根据单载波功率、功率余量、每载波功率允许最大值（规定单载波功率上限：城区A网格40W，郊区C网格80W）得到每载波功率建议值(W)，并将其转换为RS参考信号功率最终建议值(dBm)，转换公式如下。

$$RS_{\text{dBm}}=10\times\lg_{10}(P_{\text{单载波功率建议值(W)}}\times1000)/(N_{\text{channels}}\times RB\times12\times10^{\frac{PA}{10}}) \quad (2)$$

其中RB为小区带宽对应的RB数，PA为通过不同PA和PB值设置RS信号在基站总功率中的不同开销比例，N_{channels}为小区RRU通道数。

⑤功率余量(dBm)=RS参考信号功率最终建议值(dBm)-RS参考信号功率现网值(dBm)，考虑到需要为小区未来扩充载波预留一定的功率空间，因此功率余量(dBm)≥3dB的情况下才可提升小区功率。

(2)中兴

①网管平台提取小区实际发射功率(dBm)和最大发射功率(dBm)现网值，并将功率单位换算为W，转换公式如下。

$$P_{\text{W}}=10^{\frac{P_{\text{dbm}}}{10}}/1000 \quad (3)$$

②计算多载波均摊功率，公式如下。

$$P_{\text{多载波均摊功率(W)}}=\begin{cases}\dfrac{P_{\text{最大发射功率(W)}}}{2\times N_{\text{折算载波数}}}, & \text{小区带宽=20MHz}\\ \dfrac{P_{\text{最大发射功率(W)}}}{2\times N_{\text{折算载波数}}}, & \text{小区带宽=10MHz}\end{cases} \quad (4)$$

③根据多载波均摊功率(W)、每载波功率允许最大值（规定单载波功率上限：城区A网格40W，郊区C网格80W）得到每载波功率建议值(W)，并将功率单位换算为dBm，转换公式如下。

$$P_{\text{每载波功率建议值(dBm)}}=10\times\lg_{10}P_{\text{每载波功率建议值(W)}}\times1000 \quad (5)$$

④RS参考信号功率最终建议值(dBm)=RS参考信号功率现网值(dBm)+$P_{\text{每载波功率建议值(dBm)}}$-$P_{\text{小区实际发射功率现网值(dBm)}}$。

⑤功率余量(dBm)=RS参考信号功率最终建议值(dBm)-RS参考信号功率现网值(dBm)，考虑到需要为小区未来扩充载波预留一定的功率空间，因此功率余量≥3dB的情况下才可提升小区功率。

3.1.2 重选切换参数调整

从设备厂商网管平台提取小区重选及切换现网参数。

表1　问题归类及优化方案

问题归类	优化方案
参数	功率调整
	重选切换参数调整
故障	服务小区故障
	邻区故障
覆盖	天馈调整
	规划建设
其他	地市深入分析

表2　邻区搜索范围

弱覆盖小区类型	问题点小区夹角门限（°）	邻区夹角门限（°）	搜索半径（此距离内站点入选）（m）
室内分布	360	360	200
宏站	60	360	500
微小	60	360	200

表3　重要告警

华为	中兴
射频单元维护链路异常告警	单板电源关断
射频单元业务不可用告警	小区退服告警
BBU IR光模块收发异常告警	单板通信链路断
小区闭塞告警	网元断链告警
射频单元驻波告警	单板硬件故障
BBU IR光模块/电接口不在位告警	同步丢失
射频单元交流掉电告警	GNSS接收机故障
小区服务能力下降告警	GNSS天馈链路故障
射频单元光模块收发异常告警	天馈驻波比异常
BBU IR接口异常告警	RRU链路断
eNodeB退服告警	设备掉电
射频单元光模块/电接口不在位告警	RX通道异常
	SCTP 偶联断
	以太网物理连接断
	S1断链告警
	光口接收链路故障
	MME偶联全断
	软件运行异常
	PB链路断

表4　XXX小区过覆盖判断示例

小区名称	用户随机接入时TA值在区间0范围的接入次数	用户随机接入时TA值在区间1范围的接入次数	用户随机接入时TA值在区间2范围的接入次数	用户随机接入时TA值在区间3范围的接入次数	用户随机接入时TA值在区间4范围的接入次数	用户随机接入时TA值在区间5范围的接入次数	用户随机接入时TA值在区间6范围的接入次数	用户随机接入时TA值在区间7范围的接入次数	90%用户TA最远值	站间距平均（m）	过覆盖判断	用户在分布TA最大区间	用户分布TA最大区间对应距离（m）
XXXF-HLH-1	0.94%	85.61%	99.90%	100.00%	100.00%	100.00%	100.00%	100.00%	624	268	TRUE	1	156～312
XXXF-HLH-2	2.78%	87.65%	99.84%	99.99%	100.00%	100.00%	100.00%	100.00%	624	268	TRUE	1	156～312
XXXF-HLH-3	1.89%	82.68%	97.69%	98.04%	99.98%	100.00%	100.00%	100.00%	624	268	TRUE	1	156～312

对于重选参数，主要核查小区最低接入电平QRxLevMin设置是否合理，对小于−124dBm的问题点小区归类为重选参数设置不合理，避免UE在接收信号电平很低，无法提供用户满意的通信质量的情况下重选至该小区；对于切换参数，主要核查基于A3的A2门限与基于A4/A5的A2门限设置是否合理，对A2门限小于等于−108dBm的问题点小区归类为切换参数设置不合理，避免UE在切换时由于启测门限过小，未能及时切换到信号较好的邻区而导致弱覆盖。

3.2 故障

站点退服或重要告警会影响周边小区的MR覆盖率。如果弱覆盖小区及其邻区存在退服或严重告警，需要输出小区清单，纳入告警监控，并优先处理，推送维护部门尽快解决故障。

从设备厂商网管平台提取问题点派单前一周的告警信息。分别核查问题点小区及其邻区是否存在重要告警，其中邻区搜索范围定义见表2（夹角门限：小区天线朝向与两小区连线的夹角，范围[0,360°]）。

各设备厂商影响MR覆盖率的重要告警参考见表3。

3.3 覆盖

(1)天馈调整

从设备厂商网管平台提取问题点小区TA数据，针对宏站问题点小区，若出现过覆盖现象，需结合站点天馈实际情况进行天馈调整，适当增大机械下倾角或电子下倾角。注意事项：增加的度数不宜过多，一般在3～6° 即可，需要结合天线高度与预期覆盖目标合理控制倾角度数。若倾角下压过多，超过8° 时，会使覆盖范围收缩过多，产生覆盖空洞，对小区覆盖率没有提升。

过覆盖判断步骤：

①通过PRS获取小区*TA*值分布情况，累积*TA*0～*TA*7每一分段的用户数占比，将每*TA*分段百分比向后求和，该分段求和值大于90%时，取该分段的最远距离为*T*1；

②计算出弱覆盖小区距离最近*N*个宏站的平均站间距*T*2，只计算现网站点与宏站之间平均站间距（*N*建议值为3）；

表5　规划站匹配规则

弱覆盖小区类型	规划站小区类型	问题点小区夹角门限（°）	规划站小区夹角门限（°）	搜索半径（此距离内站点入选）（m）
宏站	宏站	60	360	500
宏站	微站	60	360	200
宏站	室分	60	360	200
微站	宏站	60	360	200
室分	宏站	360	360	200

③比较*T*2与*T*1，如果*T*1大于1.5倍*T*2，则判断该小区过覆盖。

举例（小区名以XXX代替）：XXXF−HLH−1在*TA*分段为2时，用户数占比累积大于90%，则此时*T*1取该分段的距离最大值624m，弱覆盖小区距离最近宏站的平均站间距*T*2为268m，由于*T*1>1.5×*T*2，故该小区存在过覆盖现象，详细见表4。

(2)规划建设

针对长期弱覆盖或者覆盖率很差的小区，核查周围是否存在规划站。如果存在，可考虑规划站点规划升级，加快建设入网。规划站匹配规则如下（夹角门限：小区天线朝向与两小区连线的夹角，范围[0,360°]）。规划站匹配规则见表5。

3.4 其他

对于无法归类为参数、故障、覆盖任意一类的问题点，建议直接派发至地市，由地市结合现场情况进一步深入分析。

4 弱覆盖问题点归类流程及结果

图1展示了问题点归类流程，结合多种因素考虑后，最终确定对问题点进行归类的判断顺序为：故障→规划站→RS功率提升→重选切换参数→过覆盖，使得各类问题点均达到合适的比例。

截至2018年3月，该市4G弱覆盖整治及4G竞对弱覆盖整治专项问题点，共计派单6228个，根据预分析规则，按照问题点归类流程，将所有问题点归为参数、覆盖、故障、其他4大类，并统计相应的优化方案，如图2、图3所示。其中参

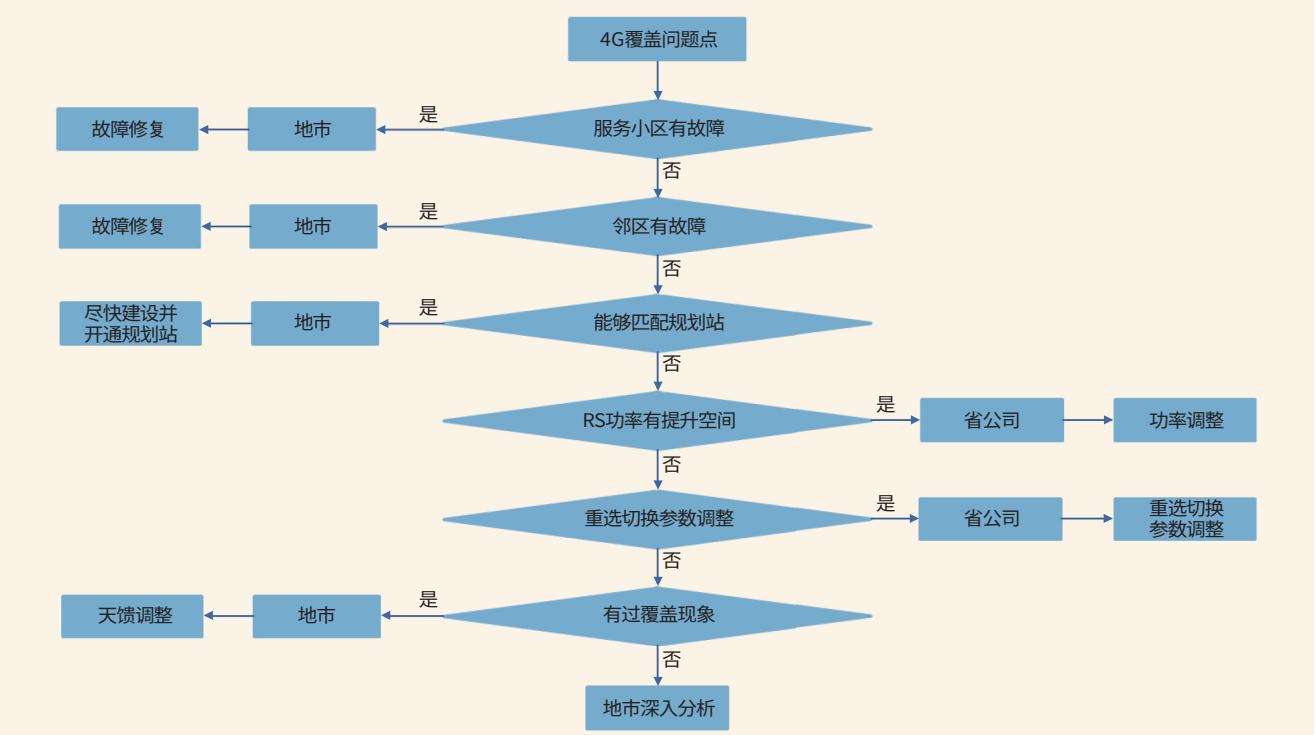
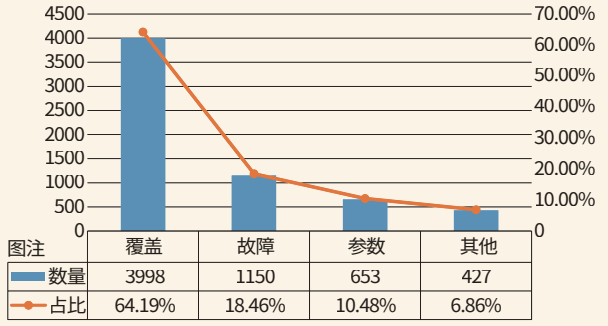
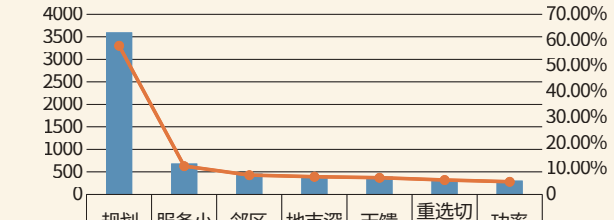


图1　问题点归类流程



图注	覆盖	故障	参数	其他
数量	3998	1150	653	427
占比	64.19%	18.46%	10.48%	6.86%

图2　问题点归类占比



图注	规划建设	服务小区故障	邻区故障	地市深入分析	天馈调整	重选切换参数调整	功率调整
数量	3596	684	466	427	402	348	305
占比	57.74%	10.98%	7.48%	6.86%	6.45%	5.59%	4.90%

图3　优化方案占比

数类问题点（约10.5%）由省公司优化人员进行分析，其余问题点直接下派地市进行分析。

5 结束语

网络覆盖不足是导致4G客户感知不好的根源，是各项重点专项优化工作的重中之重。综上提出一种弱覆盖问题点预分析策略，可协助省市两级网优分析人员对弱覆盖问题点做出精准定位，提供更加具备针对性的优化方案，极大地提升省市两级网优工作的效率。鉴于此模式已在中国移动某省市试验阶段取得良好效果。可供其他省市参考借鉴。

参考文献

[1]　程功利，张南国．大数据分析在LTE无线网规划建设中的应用[J]．移动通信，2018，42(4)

[2]　吕亚莉，肖育苗．解决深度覆盖的原则和思路浅谈[J]．移动通信，2017，41(13)

[3]　梁金山，马宁，赵明峰．基于多维度的LTE室内分布MR弱覆盖小区优化方法[J]．移动通信，2017，41(5)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

张喆

硕士，工程师，主要从事网络优化咨询等相关工作。

doi:10.3969/j.issn.1000-1247.2018.07.021

家庭宽带安全体系的优化设计

段 琼 刘 义
中国移动通信集团河南有限公司

摘要 通过建立完善的家庭宽带安全体系，不仅可以保护用户隐私，而且可以提高运营商的宽带服务质量，提高运营商口碑，建立强大的品牌优势。依托目前主流的光纤入户接入方式，分别从用户宽带接入设备安全、宽带接入服务器安全以及宽带认证服务器三个方向阐述如何建立完善家庭宽带安全体系。

关键词 宽带安全 家庭宽带 安全体系

1 宽带安全体系优化方向

目前主流的宽带接入系统，主要包含用户接入设备、宽带接入服务器（BRAS）、宽带认证服务器（RADIUS），家庭宽带安全体系如图1所示。

图1中蓝色箭头为宽带用户认证时的数据流向，根据用户认证流程的先后顺序，分别阐述家庭宽带的各个组成部分。各部分的主要作用如下：

(1)用户宽带接入设备安全，即保证用户使用的是经过运营商认证的拨号设备，防止用户宽带信息被拦截；

(2)BRAS安全，即保证BRAS是经过运营商认证的设备，且设备信息应录入RADIUS平台，保证设备合法性，防止非法BRAS接入导致运营商的损失，且接入服务器应保证足够健壮，具备健全的容灾机制；

(3)RADIUS安全，即认证服务器应具备完整的防攻击、防渗透机制，保证用户宽带信息安全。

2 用户接入设备安全

用户宽带接入方式作为用户接入运营商宽带网络的基本设备，伴随着互联网的发展，经过了电话拨号上网、调制解调器拨号上网、光纤入户上网。为了响应工业和信息化部关于提高用户带宽的通知，光纤入户的接入方式越来越受到重视，而光调制解调器（俗称光猫）作为必要的接入设备，更应该加强相关光猫的安全性，防止非法设备盗取用户隐私数据，为用户安全上网保驾护航。下面着重阐述光调制解调器的设备安全。

目前，光猫作为基础的宽带接入设备，应由运营商指定标准规范，并指定厂商进行生产，经过运营商的严格入网测试，应具有功耗低、可靠性高、具有完整的告警状态指示等标准。

光猫作为用户接入宽带的基础设备，应具备如下几点。

(1)宽带认证发起方

光猫作为互联网接入设备，用户宽带信息应由光猫保存并进行加密处理，防止用户宽带信息被盗取，光猫作为宽带接入发起方有如下优点。

- 用户账号和密码复杂度可控，即可以在光猫安装时使用专用设备将用户账号和密码写入光猫，尤其可以设置高安全强度的用户密码，进一步加强用户宽带信息的安全性。
- 认证请求由光猫发起，用户无需知道宽带具体信息，防止用户泄露宽带账号和密码信息，进一步加强宽带账号安全性。

(2)封闭性

光猫作为一种网络接入设备，应保持对用户的封闭特性，用户不得随意修改光猫配置，应由专业的工程师进行初始化配置，此后相关配置信息应对用户封闭，具备如下优点：

- 防止用户私自篡改配置，造成软件故障；
- 防止用户私自下载、升级光猫固件，导致光猫的硬件故障；
- 将光猫与用户进行绑定，宽带认证时使用动态密码进行认证，配合宽带认证服务器，使用户不局限于使用静态密码，从而在更高程度上保证用户宽带信息。动态密码算法一般可以根据光猫唯一号+用户账号+当前时间使用算法生成动态密码。

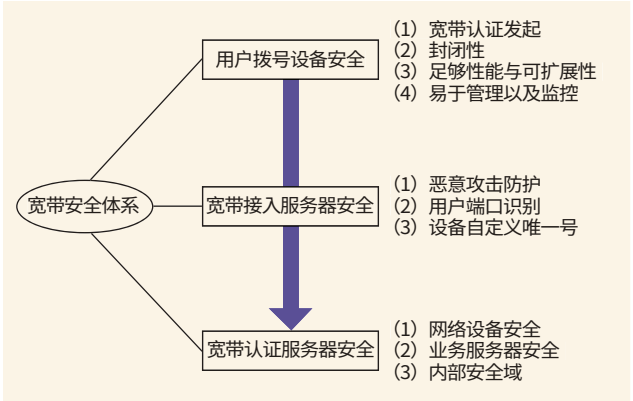


图1　家庭宽带安全体系

(3)足够性能与可扩展性

用户使用宽带的需求与互联网的建设是动态发展的，因此光猫在满足现有带宽的需求下，应至少提供现有性能50%左右的剩余性能，防止后期推出更高带宽的产品时，需要更换光猫设备，从而提高用户和运营商成本。

(4)易于管理与监控

用户在使用互联网时，随时可能发生故障，当发生故障时，光猫设备应具备足够简单明了的告警状态指示，帮助客户快速排查故障。例如光衰超过正常范围值或者认证故障时，有相应的状态指示。

3 宽带接入服务器安全

宽带接入服务器作为光调制解调器和宽带认证服务器连接的桥梁，将用户账号和密码上传到认证服务器，并根据认证成功与否来决定用户是否被许可接入互联网，因此其重要性不言而喻。关于宽带接入服务器的安全主要围绕恶意攻击防护、用户端口识别以及设备自定义唯一号进行阐述。

3.1 恶意攻击防护

由于宽带接入服务器在用户的上行方向，用户自组网络不受控，恶意用户或者恶意程序就可构造非法协议报文或者广播报文并向上发送，这不仅会导致设备处理性能下降，还会导致接入服务器宕机，该接入服务器下的所有用户上网活动瘫痪。

针对恶意攻击防护，宽带接入服务器应具备自动流量分析功能，在网络侧检测到过量的协议报文、广播报文、组播报文以及不同源MAC地址的报文时，BRAS应立即将该端口进行通信，以免其他用户受到影响。上述4种报文中，前三种报文会大量吞噬设备处理资源，第4种会占用交换芯片有限的MAC地址表资源，因此都需要进行控制。

为了增强安全性，在接入网络，一般要求在接入节点处实现用户端口隔离：在同一个VLAN下的用户相互不通信，且只能和上行汇聚端口互通。用户端口隔离目前主流业界采用私有虚拟局域网技术实现，这样可以保证单个用户的隔离性，防止恶意程序在同一个VLAN下用户之间进行快速传播。

3.2 用户端口识别

BRAS应具备识别其下用户的能力，即可以根据接入信息精准定位每一个用户，不可使多个用户共享同一接入信息，更不可使多个用户共享同一宽带账号，从而给运营商造成经济上的损失。

家庭宽带用户的接入方式依然是有线接入方式，在宽带接入服务器上应可以精确定义不同用户，保证一个用户有且只有一个用户接入信息，因此可以配合宽带认证服务器进行精确的用户认证定位，从根本上防止多个用户共享同一宽带账号，造成运营商的损失。

目前用户端口识别主要采用RADIUS协议中的Nas-Port-Id属性值进行区分，应由运营商定义具体规范，使全网BRAS设备采用统一格式Nas-Port-Id来区分用户，且Nas-Port-Id在同一BRAS服务器为唯一值，防止相同区域用户共享账号。

3.3 设备自定义唯一号

RADIUS协议本身具备可扩展性，所有携带属性均由可变长度的属性-长度-值三元组表示，可以添加新属性值而不影响协议的现有实现。

运营商可以定义RADIUS扩展RFC2865中的26号属性，该属性由BRAS服务器、RADIUS以及运营商共同定义，扩展RADIUS识别性，防止私接BRAS攻击RADIUS服务器。

该属性值每台设备有一个唯一值，且只有在接入客户认证服务器时可以进行设定，客户认证服务器RADIUS根据BRAS服务器的地址来获取唯一值，并且与RADIUS扩展协议中定义的属性值进行对比，以提高BRAS服务器的合法性。

4 宽带认证服务器

宽带认证服务器作为用户认证流程的终结点，管理着几十万到几百万的用户，下属的宽带接入服务器从几百台到几千台，认证流程及计费流程在宽带认证服务器中进行，且所有用户的认证信息均保留在宽带认证服务器中，重要性在这个体系中处于最高级，整个系统由若干台网络设备、业务服务器组成，宽带认证服务器的安全决定了全网用户宽带信息安全及全网宽带接入服务器的信息安全。

RADIUS处于宽带用户认证的顶层，应具备足够完善的防攻击、防渗透策略，并具备完整的容灾备份处理能力：网

络设备应具有故障转移、对所有硬件设备接入网管系统进行监控等能力。典型的宽带认证服务器系统拓扑如图2所示，RADIUS系统主要包含三大组成子系统：核心网络设备、业务服务器集群、内部安全管理域。下面根据这三大组件来分别阐述RADIUS系统的安全性。

4.1 核心网络设备安全

核心网络设备的主要职责有隔离内部网络与外部网络及系统服务器之间的数据交换、系统服务器业务负载均衡与故障转移。

网络设备安全主要包括如下几点。

(1)网络设备均需具备容灾备份模式：当一台设备出现故障时，备份设备可立即接管所有业务，例如丢包率控制在5%以下。

(2)所有网络设备均需建立完善的监控机制，及时监控硬件和软件的状态。例如：当设备的配置更改时，发出告警或者通知相关责任人。

(3)禁用设备空闲端口，防止发生被人恶意通过接入网络设备发送ARP攻击等会导致网络设备瘫痪的操作。

(4)建立完善的网络设备管理流程，如需进行配置修改，需经过完善的审批流程，并制定完整的意外处理流程。

(5)定期升级设备固件，及时修复设备漏洞，保证内部网络安全。

(6)建立完善的灾难处理流程，定期进行灾难演习，保证设备容灾备份功能正常，完善灾难处理流程。

4.2 业务服务器安全

在RADIUS系统中的业务服务器一般包括：处理用户请求和计费的RADIUS服务器、负责与业务支撑平台进行对用户开/销户操作的接口服务器和其他附属业务服务器。

目前业界业务服务器一般采用Linux或者类Unix操作系统，从服务器硬件及系统软件、业务软件安全几方面进行阐述。

4.2.1 服务器硬件

服务器硬件主要包括服务器CPU、内存、相对应的主板固件（BIOS）等。

由于现代服务器均具有带外管理功能，因此服务器BMC管理网口应该接入RADIUS系统内网且与业务网络隔

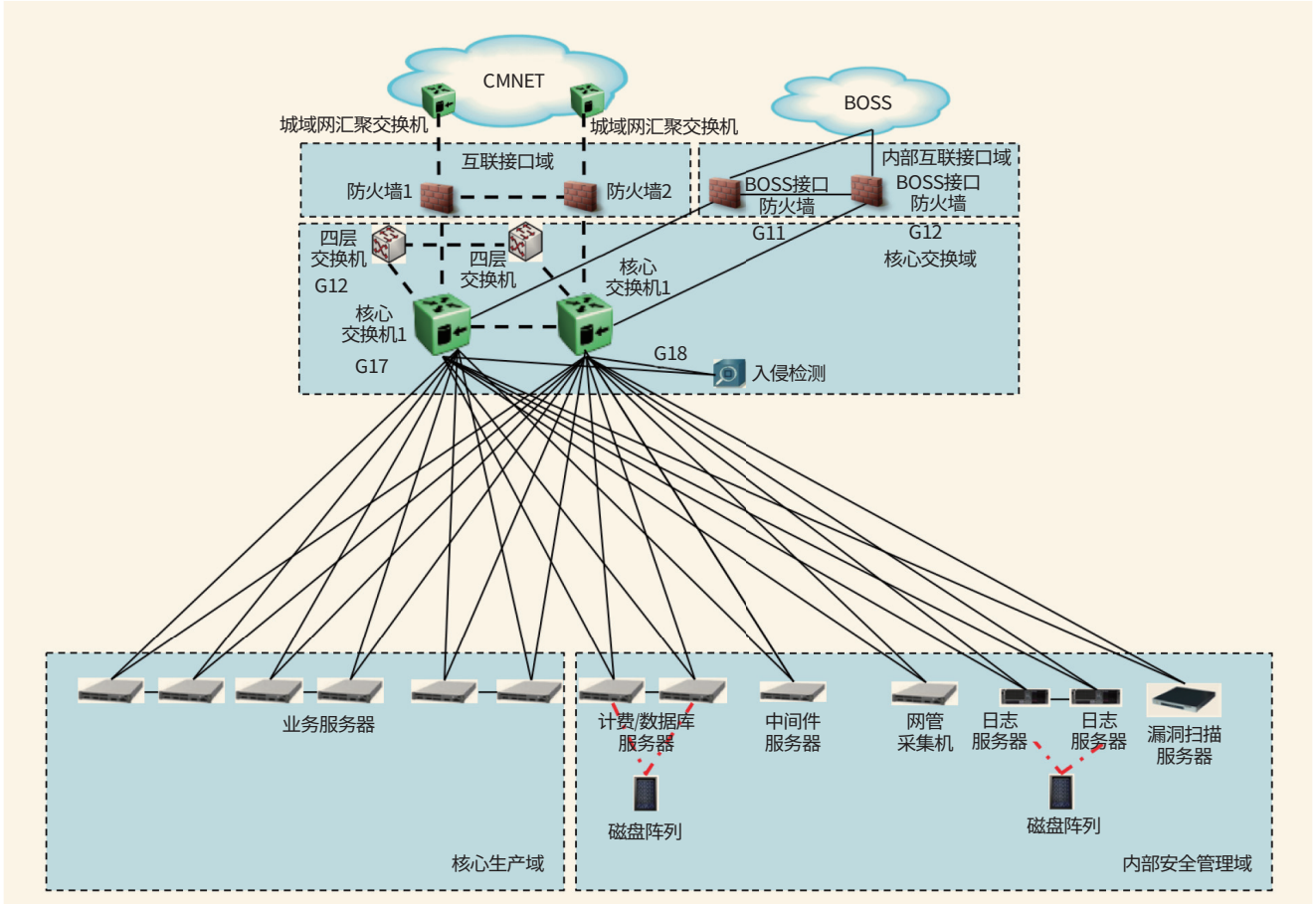


图2　典型宽带认证服务器网络拓扑结构

离，可以独立访问，在服务器故障时可以远程控制服务器，快速解决故障。

目前业界主流服务器均带有SNMP和IPMI接口来管理服务器硬件，应根据实际情况采用其中的一种来详细监控服务器的硬件。例如华为RH服务器的硬件监控可细化到服务器的每颗CPU、每条内存、每块硬盘、主板以及阵列卡的健康状态，还可以监控风扇的转速、出风口温度等指标，使用户可及时了解服务器的硬件运行状态，加强系统业务主机安全指标。

4.2.2 系统软件安全

系统软件就是部署在硬件服务器上的操作系统，目前业界采用较多的为Red Hat Linux或者Cent OS Linux发行版，前者由开源软件公司Red Hat发行，后者是其开源版本。

系统软件的安全主要集中在操作系统软件包的更新、系统软件安全配置等方面。

(1)业务服务器的操作系统关键服务，如SSH、FTP、NTPD、OPEN SSL等关键服务器软件应及时进行更新。

(2)定期使用安全扫描工具扫描系统漏洞，定期更新关键服务软件，避免服务器存在高危漏洞，包括但不限于SSH配置、FTP配置等的优化。

(3)关闭不必要的系统服务，例如关闭FTP、AUTOFS、DHCPD等服务，避免被恶意攻击。

(4)业务服务器不应与工程师设备直接连接，应通过安全认证过的堡垒机进行统一认证，并记录工程师的全部操作，禁止绕行设备，防止绕行攻击，且堡垒机服务器不能使用bash、csh等shell，应使用安全的shell程序且仅可执行有限的命令。

(5)业务服务器应具有安全、必要的依赖包，只需满足业务软件需求即可。

(6)开启SE Linux服务，避免服务器软件被恶意篡改。

4.2.3 业务软件安全

业务软件是运行在业务服务器上提供RADIUS服务的一组软件集合，提供宽带用户的认证、计费等基础服务，业务软件应具备比较完善的安全策略，主要包括如下内容。

(1)RADIUS业务软件需具备7×24×365不间断的运行能力，但大部分软件，尤其是庞大的软件系统更加容易出现Bug，因此业务软件应具备完善的健康检查机制，例如是否发生错误、发生错误的数量等健康信息，针对错误信息等打印足够详细的日志来帮助工程师分析定位问题原因，并不断优化。基于健康检查机制可以在错误出现次数过多的情况下，在业务闲时重启业务软件，保障业务软件的稳定运行。

(2)RADIUS业务软件应由专业的监控软件进行持续性监控，并且在业务进程意外宕机的情况下可以重启业务软件，防止业务中断。

(3)RADIUS业务软件应具备完善的业务统计能力，如可以报告正在处理的业务请求数、已经完成的业务请求数等业务统计能力，这些数据不仅可以供业务运维进行统计，亦可以将数据提交给专业的大数据平台进行处理，协助运营部门更好地运营宽带产品。

(4)RADIUS业务进程应只允许由运营商批准的宽带接入服务器进行用户认证请求，目前主流的做法是将宽带接入服务器登记到RADIUS业务进程，只允许列表中的BRAS进行认证请求，也可以参考3.3节制定更高的安全策略。

(5)用户密码不应以明文存储在用户服务器、业务进程日志中，应以加密字符串保存在服务器或者日志中。

(6)RADIUS协议共享密钥不应以明文存储在业务进程配置文件中，应以加密形式存储在配置文件或者数据库中。

(7)RADIUS服务器应可以识别用户唯一性。目前业界主流的做法是采用宽带接入服务器IP地址+RADIUS报文中Nas-Port-ID值与用户绑定来进行用户唯一性校验，防止用户将宽带信息共享给其他用户，避免造成运营商的经济损失，并且应支持解绑功能，防止因用户搬家或者BRAS故障端口信息重置影响用户认证。

(8)RADIUS服务器应记录所有在线用户信息，在用户下线后删除在线信息，且同一用户只能有一条在线用户信息，当用户在线时相同用户的其他请求将予以拒绝。

4.3 内部安全管理域安全

内部安全管理域与业务服务器在网络上进行隔离，只允许通过特定端口进行业务访问，在服务器内部限制登录IP，只允许安全堡垒机IP地址进行登录。

内部安全管理域主要包括数据库服务器、日志留存服务器、中间件服务器、安全防护服务器。安全域内的服务器硬件和操作系统安全与业务服务器类似，故不再详述，只针对这几类服务器安全进行阐述。

4.3.1 数据库服务器安全

数据库负责存储用户宽带信息、用户话单，作为用户认证阶段的数据落点，数据库的安全是重中之重。下面按照Oracle数据库进行阐述。

(1)数据库服务器主备模式

数据库应配置为主备模式，防止主机由于硬件问题导致数据库无法提供服务。建议使用Active Data Guard来进行Oracle数据库的主备机制，并在重大节日前进行安全演练，防止主备模式出现异常。

(2)限制用户登录

非dba权限用户，原则上不授予dba权限。业务用户仅对

自己业务数据有相应的读写权限。通过使用触发器，限制用户只能从指定IP访问，其他IP地址禁止访问。

(3)TNS Listener漏洞防护技术

通过数据库弱口令扫描产品和定期更换安全密码进行预防。

对TNS Listener进行密码设置，防止远程注册被黑客利用（阻止来自网络的非法注册）。

定期通过下载官方补丁或者使用含有VPATH的防火墙产品对已知漏洞进行修复。

通过数据局保险箱对数据库进行全库或者敏感字段加密。保证即便TNS Listener被攻破，核心数据依旧不会泄露。

(4)Oracle表空间加密

表空间加密保护整个表空间中的数据安全，如：数据文件或数据文件备份若被窃取，没有密钥不可能查看到其中的数据，这对于保护诸如军用级别的数据、his系统的病人数据等非常重要。

(5)保护敏感数据

使用Oracle Database Vault能够限制任何用户访问数据库中的特定区域，包括拥有管理（dba）权限在内的用户，Oracle Vault提供sys用户削权的一种选择。作为Oracle数据库的一个可选组件，Vault是需要额外的文件链接、注册和安装的。安装Vault之后，Oracle会去创建一个全新的用户dbvowner，原有的sys对一些数据的操作和访问权限都有进行控制的可能。

(6)数据存储

数据应存储在专业存储硬件中，建议使用RAID 5+1或者RAID 6+1来进行RAID配置，并将存储设备接入网管设备，随时监控设备状态，防止出现情况。

4.3.2 日志留存服务器

日志留存作为业务日志的最终节点，业务日志不仅包含用户认证流程，也可以写入用户密码，因此用户日志服务器应与外网隔绝，不允许通过SFTP/FTP/HTTP等手段下载日志文件。

若进行日志查询应通过指定的接口，接口应由运营商与认证系统协商规范，并且接口服务器应在防火墙配置为只允许有限的服务器IP地址访问。

4.3.3 中间件服务器

若业务服务器是业务流程的发起者，数据库是业务流程数据的落点，那么中间件服务器就是业务服务器与数据库之间的管道。中间件服务器接受业务服务器的业务请求，根据数据库中的用户数据来进行具体的业务逻辑，宽带认证服务器系统的全部业务处理均来自于中间件服务器，是业务处理的发动机。

中间件服务器作为业务处理的核心服务器，具有配套的各类服务器，下面从业务发起的方式阐述中间件服务器安全，如HTTP、TCP/UDP等。

不论何种业务接口形式，应遵循只对外公布必要的服务器端口、中间件服务器内部组件之间通信尽量采用IPC、Socket等服务器内部接口，如需要通过网络，内部组件应只监听127.0.0.1本地回环地址，不在内网地址进行监听的原则。

HTTP作为互联网使用最广泛的协议，是黑客攻击的重点。因此应尽量保证HTTP服务器的安全，尽量遵循以下原则：

(1)定期进行HTTP服务的漏洞扫描，出现漏洞尽快进行处理；

(2)建议使用HTTPS协议代替HTTP，内网服务器可以使用自定义SSL证书，并不会影响用户使用，因此成本低廉且安全，即便使用HTTP，也建议传输报文进行加密处理，防止报文内容被攻击而导致信息泄露；

(3)HTTP协议头不应带有服务器端Web容器类型和版本号，只允许HTTP的Get、Post操作，不允许Delete、Put等操作；

(4)不只在防火墙做访问限制，应在软件内部也限制源IP地址集，防止非法入侵；

(5)建议中间件软件通信进行加密传输，防止网络嗅探，用户信息被泄露。

4.3.4 安全防护服务器

安全防护服务器主要包括漏洞扫描服务器和4A安全接入服务器。安全防护服务器作为安全性较高的产品，由专业的安全公司工程师进行定期维护与升级。若采用安全防护服务器则应订阅升级邮件，定期完善安全策略，并对系统内所有服务器进行漏洞扫描，尽快修复高危漏洞。

5 结束语

宽带作为家庭用户接入互联网的最主要方式，其安全应给予重视。文中从理论与可行性上对宽带安全进行阐述，分别从认证时的三个组成部分：用户接入设备、宽带接入服务器BRAS、宽带认证服务器RADIUS进行说明，尤其对宽带认证服务器进行了比较深入的探讨和研究。通过采取有效方式，使用户宽带接入更加顺畅，合理利用运营商资源，防止宽带资源滥用，使宽带系统具有更高的健壮性，提高用户体验，提升运营商信誉。

参考文献

[1] C.Rigney and S.Willens,Remote Authentication Dial In User Service(RADIUS)[S]. RFC 2865.June 2000,https://tools.ietf.org/html/rfc2865[J]

[2] 连伟亮.家庭宽带光纤接入技术研究[J].无线互联科技,2017(18)