



信息通信领域产学研合作特色期刊
 第三届国家期刊奖百种重点期刊 | 中国科技核心期刊

ISSN 1009-6868
 CN 34-1228/TN

中兴通讯技术

ZTE TECHNOLOGY JOURNAL

www.zte.com.cn/magazine

2015年6月 • 第3期



创刊20周年纪念特刊



专题：移动互联网安全技术



中兴通讯技术

ZTE TECHNOLOGY JOURNAL

二〇一五年六月

第二十一卷第三期

总第二二三期

刊首 寄语

办有思想的刊物 做有文化的企业



侯为贵

中兴通讯股份有限公司
董事长

1995年,我们创办了《中兴通讯技术》杂志。希望通过办刊回报社会,促进通信产业发展;也希望通过办刊,凝聚业界精英,为公司的发展出谋划策。

20年来,刊物紧跟技术的步伐,同步公司的发展,一直朝着这样一个目标在努力:办成业界有广泛影响力的刊物。广义地说,《中兴通讯技术》的读者是通信运营商,是高校师生,是科研人员。但是,真正的目标读者只有那么一群人。从刊物的角度来说,影响了他们,就影响了世界。他们是谁呢?他们是通信前沿技术的探索者,是技术标准的制定者,是通信网络的管理者和建设者,是未来栋梁的高校学子。

刊物影响力来自于内容,内容的价值决定了刊物的影响力。通信行业在过去的20多年,一直处于快速变化过程之中。无论是技术还是市场,都有很多东西需要我们去研究,去探讨。正是这些内容,使刊物有了份量和厚度。今后,信息技术的发展将更加多元化和复杂化。在这样一个快速变化的环境下,刊物如何感知自己的责任,找准自己的位置,发挥最大的价值,显得尤为重要。我们需要有思想的刊物。

有思考,才有思想;有观点的碰撞,才有思想的花。好的刊物应该是有个性的刊物,是有观点和生命力的刊物,是真正能为行业发展创造价值的刊物。过去的20年,《中兴通讯技术》一直在努力,在聚焦前沿技术的同时,着力挖掘行业发展的真知灼见,将知识性和思想性融为一体。

随着信息技术的发展,新媒体时代悄然来临。

可以说,新媒体是以数字技术为基础,以网络为载体,以多客户端呈现为特点的信息传播媒介。相比传统刊物,它在交互性、及时性、渗透性等方面有着更大的优势,而且能够低成本运营。由此看来,我们面临的挑战将是,如何让传统媒体在新媒体的平台上实现从内容到功能的质的飞跃,如何发掘能让新媒体价值充分体现的信息内容。

不管媒体的内容和表现形式如何变化,一个原则不能变:内容永远为王;一个理念不能变:服务,即价值。

刊物的价值是多方面的,它的文化属性也显而易见。《中兴通讯技术》走过20年,伴随企业成长,助力企业发展,已经成为我们企业文化的一个重要载体。

企业都想做百年老店。我们纵观全球长盛不衰的知名企业,真正使其立于不败之地不是其技术、专利或产品,而是其文化。可以说,企业文化是企业的思想和灵魂,是企业发展的永久动力。企业文化渗透在企业经营和管理的方方面面。

企业文化各有特色。中兴通讯的企业文化是尊

重员工的文化,是中国传统文化在现代企业的延续和发展;中兴通讯的企业文化是尊重股东的文化,是注重股东回报与企业长期发展的平衡文化;中兴通讯的企业文化是服务社会的文化,是力求通过优质产品和服务提高人们生活品质的文化。《中兴通讯技术》就是企业服务社会的一个文化产品。

企业在不同程度上承载着国家责任和社会责任。国家倡导建立以企业为主体的国家创新体系,企业的舞台变大了,责任也更大了。我们办好学术刊物,也是想从一个方面促进企业需求和社会资源的匹配,促进科研成果向应用产品的转化。

20年来,《中兴通讯技术》杂志见证并记录了通信技术的发展轨迹,为行业发展尽了一份力,为企业发展做出了一份贡献。感谢所有编委、审稿人、作者以及社会各界对刊物的大力支持!也感谢编辑部员工为刊物发展付出了辛勤汗水!

办有思想的刊物,做有文化的企业,是我们不懈的追求。



办刊 回顾

如歌的岁月 如诗的篇章

——中兴通讯技术杂志社办刊 20 周年回顾

黄新明

(中兴通讯技术杂志社常务副总编)

20 年前,中兴通讯技术杂志社成立。回顾办刊历程,难忘曾经的风雨和彩虹。

1995 年 6 月发布招聘广告,7 月召开第一次编委会,9 月创刊号与读者见面。也许,这就是当年的“深圳速度”吧!有人说,《中兴通讯技术》杂志有典型的时代烙印和特有的气质。也许,因为它诞生在通信大发展的黎明时分,成长在深圳特区开拓创新的强大气场之中。

80 年代后期,改革开放大潮席卷中国,深圳位于潮头浪尖。此时的通信市场被国外“七国八制”的设备垄断,民族通信产业发展举步维艰。进入 90 年代,中兴通讯与国内同行共同努力,在数字程控交换机市场实现突破,“巨大中华”脱颖而出。1995 年,年销售额不足 3 亿元的中兴通讯以独特的境界和眼光,着眼行业现实需求和企业长远发展,创办《中兴通讯技术》杂志。

刊物的定位很明确,服务行业,服务市场。侯为贵董事长在第一次编委会上说:“希望刊物成为企业回馈社会的一个手段,并成为企业联系社会的一个桥梁。”

最初的 24 位编委,主要来自高校和科研院所,确定了“新、专、融、实”这一务实的办刊特色。“以人为本,荟萃通信技术领域精英;迎接挑战,把握世界通信技术动态;立即行动,求解通信发展疑难课题;励精图治,促进民族信息产业崛起。”这四句办刊宗旨,字里行间映射出企业办刊的初衷和期许。

虽说创刊时还没有公开刊号,但每期发行 15 000 册。在那样一个年代,激情燃烧的通信建设者们对现代通信技术的需求如饥似渴,而创刊号的专题就是当时最热点的数字程控交换技术,很“解渴”。

《中兴通讯技术》的专题运作要早于国内很多刊物,并一直延续至今,已成为刊物的核心竞争力。从 2G 时代的交换技术、接入网技术,到 3G 时代移动通信技术、IPv6 技术;从 4G 时代的 LTE 技术、云计算技术,到当前热点的 Pre-5G 技术、大数据

技术,可以说,从CT到ICT的演进过程,都囊括在刊物的专题之中。20年117期专题如实记录了当代通信技术发展的每一个脉动。一个企业,以推动民族通信事业的发展为己任;一本刊物,以促进现代通信技术的传播为使命。这,是一种情怀。

90年代开始,中国通信建设如火如荼。刊物开设“专题”、“新动态”、“电信辞库”、“产品荟萃”、“技术问答”、“专家访谈”等众多栏目,很好地满足了“技术跟随”的需要。2005年4G技术研发使中国企业首次进入世界领先队伍行列,刊物栏目减少为“专题”、“研究与开发”、“运营应用”、“系列讲座”。2010年中国成为最大的通信和互联网消费市场,中兴通讯产品在有线、无线、业务、终端等领域全面开花,产学研合作日益加强,刊物栏目则聚焦产学研,即“专题”、“研究论文”、“运营应用”、“开发园地”、“专家视点”。2015年,办刊20周年之际,为体现中国在通信领域已渐入“技术引领”的角色,刊物再一次减少栏目,力图将一个特色专题,打造成3个亮点栏目,即“专题”、“专家论坛”、“企业视界”,办“有思想的刊物”。“专题”聚集ICT前沿技术,“专家论坛”展现技术观点交锋,企业视界表达企业的技术理解。

几番产业升级,几度栏目变化。从中可以看出,在中国通信行业从极端落后到世界领先的巨变过程中,企业刊物视角的调整和对媒体责任的担当,同时也体现出了刊物同步公司发展,不断创新求变的勇气和精神。

回想当初,刊物曾刻意回避中兴通讯员工的论文,因为当时公司的实力和影响力都很弱小。但经过这20年,中兴通讯已经从一家小企业发展成为国际上销售规模排名第4的通信设备制造商,拥有6万多件技术专利。2014年中兴通讯已连续5年稳居全球企业国际专利申请量前三甲。现在的每期刊物专题中,已经不能没有中兴通讯的文章。

刊物的成长不仅体现在内容上,也体现在它的外观上。应该说,科技刊物也有它的诗情画意。如果把20年的刊物封面拼接起来,那就是一段影像。它不仅记录了封面设计的历程,更体现了科技之光的美。早期封面展示的是公司产品和技术;2001年获得正式刊号后,封面改为时尚色块;2005年,开始利用图片素材库设计封面;2009年,封面展示中兴通讯走向全球的展厅和展台。2010年更有了全新的设计思路,那就是在专题中找出最能代表该技术的图表元素,然后经过艺术加工,夸张表现,达到文图相配、见微知著的效果。此后的每期封面,都是独一无二,且富有美感,得到读者和同行的广泛称赞。从印刷方面来说,20年来,刊物从普通双胶纸单色印刷,到胶版纸双色印刷,再到铜版纸全彩印刷,2015年开始使用高档的纯质纸减少反光。不断的努力,是为了改善阅读体验。因为,这既是刊物发展的需要,也是对读者的一份尊重。

过去的20年,是中国科技期刊在改革中寻求突破的20年。从1995年开始,中国期刊业进入整改阶段。2000年中国科技期刊共4449种,到2014年增加到4944种,增长数量非常有限,而中兴通讯技术杂志社分别于2000年、2005年获得中、英文两刊的正式刊号,实属不易。2013年,按照国家要求,期刊社转企改制工作正式启动。作为第一批试点刊物,改制方案正在报批之中。当年,中兴通讯以“国有民营”新机制创造了奇迹;今天,它所创办的刊物,也同样是改革的先行者。

20年来,刊物成长的脚步是坚定的、踏实的。中文刊影响因子逐年递增,目前在无线电、电子学、电信技术刊物中排名第三;中英文两刊被国内国际16家知名数据库收录,并且均入选中国科技核心期刊;2005年中文刊荣获第三届国家期刊奖,成为中国“百种重点期刊”;目前中文刊每期国内发行8000册,英

办刊回顾

文刊每期海外发行5 500册,并通过网站、展会等多渠道与读者见面。真可谓,公司30载,享誉四海内外;刊物20年,情洒天南地北。

还记得创刊时,武汉大学图书馆在收到赠刊后,来函感谢,并告知已将本刊入库珍藏,供师生参阅;还记得河北省邮电管理局计划处领导在看到ZXJ10交换机专题后,来信称赞“ZXJ10是一种好的交换机。贵刊内容新颖,版式活泼,是不多见的好刊”;某军事院校还一次性订购100本刊物,作为当时的培训教材使用。20年后的今天,国内一家运营商集团的高层领导说:“《中兴通讯技术》是一本好刊,我每期都读,从这里获得不少新知识。跟员工交流常常用到这些内容”。依托刊物的平台,2009年中兴通讯成立了产学研合作论坛,把办刊和产学研合作紧密地结合在一起,相互促进,资源共享。

更有让办刊人激动的时刻,那就是在与公司领导和员工交流的时候,对方冷不丁地说,我正是在大学期间阅读《中兴通讯技术》杂志,才选择了中兴通讯。说话时,他们是那么平静,那么自然。这些年来,这样的场景,总在不断上演,着实让办刊人在自豪中享受一份陶醉。然而,这一切,又多么地来之不易。

创刊之初24位编委,还有6位在任,但编委队伍已发展壮大至中文刊56人、英文刊28人。正是他们的关爱和辛勤付出才有刊物今天的成就。翻看刊物,这些熟悉而又亲切的名字,频繁闪耀在眼前,因为他们既是专题策划人,又是作者,还是审稿人,在不同期次中担任不同的角色。他们,是中国通信事业的脊梁。忘不了,编委把编辑部的约稿函放在玻璃台板下提醒;忘不了,编委在深夜两点赶来参加编委会;忘不了,编委在病房中为刊物写稿;忘不了,在编辑部遇到困难时,编委一次又一次伸出温暖的双手……感谢编委!

3亿元销售规模时创办刊物,上千亿规模时还在关心着刊物,这就是中兴通讯股份有限公司的文化情怀。杂志社由当初的一个编辑部发展为合肥、深圳两个编辑部;由1种中文刊,发展到现在的3种中文刊、3种英文刊,其中两刊在合肥,享有公开刊号,4刊在深圳,作为宣传刊物;人员由当初的3个人,发展到现在的15个人。这一切,都是公司持续支持的结果。20年来,公司发展,一浪高过一浪,总编换了一任又一任,但对刊物的支持从来没有改变。即使在公司困难时期,也没有压缩办刊的编制和经费。正是公司的爱,浸润着刊物,让办刊人时刻提醒自己,不能懈怠,不能辜负。感谢公司!感谢历任总编!

20年来,杂志刊登的近2 000篇论文是作者智慧的结晶,也凝聚了审稿人对文章的贡献。“读编往来”中刊登的读者来信,无时不在鼓舞着每个办刊人勤奋工作。可以说,刊物的每一点进步和成长都得到了业界专家的鼎力支持、期刊管理部门的悉心呵护,还有刊物合办单位的共同努力。感谢他们!感谢所有关心和帮助刊物成长的朋友!

20年过去了,成就属于昨天。新起点,新征程。展望未来,信息技术的发展、公司实力的壮大、新媒体平台的出现必将为刊物的发展增添无限动力!

日出江花红胜火,春来江水绿如蓝。在国家强盛的新时代,在信息产业高速发展的春天,在数字化出版的蓝天下,办刊人一定不辱使命,在下一个20年谱写更加华美的篇章!



热烈祝贺《中兴通讯技术》创刊20周年！

中兴通讯
立足科技，创新未来。

——祝贺《中兴通讯技术》
创刊20周年



史立荣

中兴通讯股份有限公司 总裁

引领通信技术，
铸造中国辉煌！

——祝贺《中兴通讯技术》创刊20周年

赵厚麟
2015年5月3日 国际电信联盟
日内瓦



赵厚麟

国际电信联盟 秘书长



邬贺铨

中国工程院 院士

中兴通讯的名片
产业发展的写照
创新成果的园地
科技交流的平台

祝贺《中兴通讯技术》创刊 20 周年



李乐民

中国工程院 院士

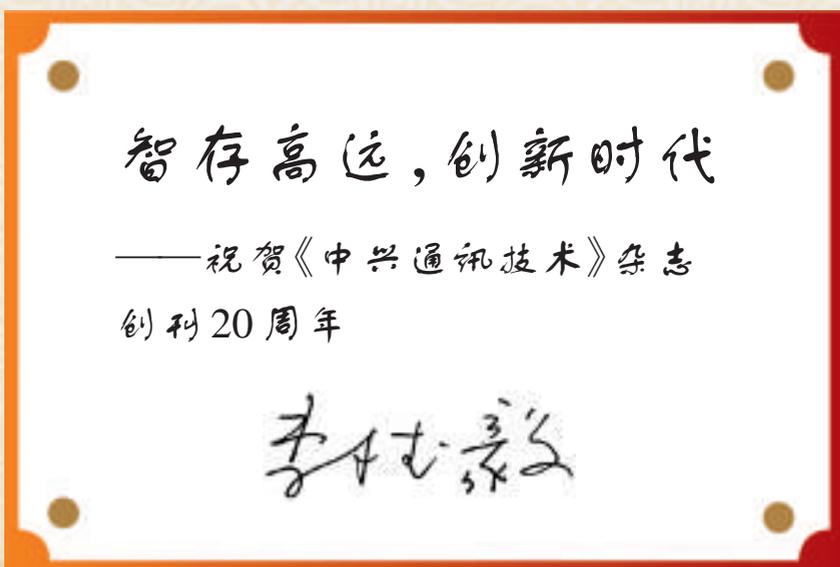
立足中国，放眼世界
依托中兴，服务行业
祝贺《中兴通讯技术》创刊 20 周年！
李乐民 2015 年 5 月 25 日

专家题词



张乃通

中国工程院 院士



李德毅

中国工程院 院士



梅宏

中国工程院 院士

廿载耕耘 今日基石
继往开来 明日辉煌

梅宏
2015.5.25



钟义信

北京邮电大学 教授
《中兴通讯技术》编委会 主任

中兴华夏得益于通信
领军世界有赖于智慧

——祝贺《中兴通讯技术》杂志创刊 20 周年

钟义信
15-05-25

扎实耕耘二十载,搭建业界平台,
务实推动创新,助力英才辈出。

——祝贺杂志创办二十周年

曹淑敏



曹淑敏

中国信息通信研究院 院长

衷心祝愿《中兴通讯技术》越办越好,成为
反映高新技术,服务行业创新的重要窗口。

北京交通大学 宁滨

2015.5.12



宁滨

北京交通大学 校长



乔建永

北京邮电大学 校长

聚焦关键学术问题 服务经济社会
发展 努力把中兴通讯技术办
成产学研协同创新平台的典范

乔建永

二零一五年六月



杨震

南京邮电大学 校长

群英荟萃百家争鸣，
廿载耕耘技术引领，
通信先锋信息殿堂，
继往开来再创辉煌！

——热烈祝贺《中兴通讯技术》创刊二十周年！

杨震

专家题词

祝贺《中兴通讯技术》创刊20周年

技术创新结硕果，
人才培养谱新篇。

重庆邮电大学 李银国 贺
二〇一五年五月十二日



李银国

重庆邮电大学 校长

集思中兴融万物
创新通讯赢未来

南京大学 潘毅
2015年5月20日



潘毅

南京大学 副校长



王保平

东南大学 副校长

廿年耕耘 成绩卓著
卅载创业 再铸辉煌

——贺《中兴通讯技术》办刊 20 年
暨中兴通讯 30 周年庆

王保平



韩杰才

哈尔滨工业大学 副校长

产学研深度融合，创造世界
一流品牌通讯企业！

——贺《中兴通讯技术》杂志
创刊二十周年！

韩杰才

专家题词

二十年海纳百川铸通讯名利
新起点百尺竿头创辉煌业绩

贺《中兴通讯技术》创办20周年

电子科技大学 杨晓波

2015.5.20



杨晓波

电子科技大学 副校长

突出新专融实特色
促进产学研用联合

贺《中兴通讯技术》创刊二十周年

杨银堂

2015.6.2



杨银堂

西安电子科技大学 副校长

编委阵容

《中兴通讯技术》第 6 届编辑委员会成员名单



- 主任** 钟义信（北京邮电大学教授）
副主任 侯为贵（中兴通讯股份有限公司董事长）
糜正琨（南京邮电大学教授）
马建国（天津大学电子信息工程学院院长）
陈前斌（重庆邮电大学通信与信息工程学院执行院长）

编委（按姓氏拼音排序）

- | | | | |
|-------|----------------------|-------|------------------------|
| • 艾波 | 中国联通学院党委书记 | • 洪波 | 中兴发展股份有限公司总裁 |
| • 曹淑敏 | 中国信息通信研究院院长 | • 纪越峰 | 北京邮电大学信息光子学与光通信研究院执行院长 |
| • 陈建平 | 上海交通大学教授 | • 江华 | 中兴通讯股份有限公司副总裁 |
| • 陈杰 | 中兴通讯股份有限公司高级副总裁 | • 蒋林涛 | 中国信息通信研究院科技委主任 |
| • 陈前斌 | 重庆邮电大学通信与信息工程学院执行院长 | • 雷震洲 | 中国信息通信研究院科技委副主任 |
| • 陈锡生 | 南京邮电大学教授 | • 李红滨 | 北京大学教授 |
| • 程时端 | 北京邮电大学教授 | • 李建东 | 西安电子科技大学副校长 |
| • 葛建华 | 西安电子科技大学通信工程学院副院长 | • 李乐民 | 中国工程院院士, 电子科技大学教授 |
| • 顾晓仪 | 北京邮电大学教授 | • 李融林 | 华南理工大学教授 |
| • 管海兵 | 上海交通大学电子信息与电气工程学院副院长 | • 李少谦 | 电子科技大学通信与信息工程学院院长 |
| • 郭云飞 | 解放军信息工程大学副校长 | • 李星 | 清华大学教授 |
| • 侯为贵 | 中兴通讯股份有限公司董事长 | • 马建国 | 天津大学电子信息工程学院院长 |

编委阵容

- | | | | |
|-------|------------------------|-------|-------------------------|
| • 孟洛明 | 北京邮电大学教授 | • 邬贺铨 | 中国工程院院士 |
| • 糜正琨 | 南京邮电大学教授 | • 徐安士 | 北京大学教授 |
| • 庞胜清 | 中兴通讯股份有限公司
高级副总裁 | • 续合元 | 中国信息通信研究院通信标准
研究所总工 |
| • 史立荣 | 中兴通讯股份有限公司总裁 | • 薛一波 | 清华大学 CPU&SOC 中心副主任 |
| • 孙枕戈 | 中兴通讯股份有限公司副总裁 | • 杨义先 | 北京邮电大学教授 |
| • 孙知信 | 南京邮电大学物联网学院院长 | • 杨震 | 南京邮电大学校长 |
| • 谈振辉 | 北京交通大学教授 | • 尤肖虎 | 东南大学教授 |
| • 唐雄燕 | 中国联通网络技术研究院
首席专家 | • 乐光新 | 北京邮电大学教授 |
| • 田文果 | 中兴通讯股份有限公司
执行副总裁 | • 张宏科 | 北京交通大学教授 |
| • 童晓渝 | 中电科软件信息服务有限公司
副总经理 | • 张平 | 北京邮电大学网络技术研究院
执行院长 |
| • 王京 | 清华大学教授 | • 张同须 | 中国移动通信集团设计院院长 |
| • 王文东 | 北京邮电大学软件学院副院长 | • 赵慧玲 | 中国电信股份有限公司
北京研究院总工程师 |
| • 王晓明 | 中兴通讯股份有限公司
微电子研究院院长 | • 赵先明 | 中兴通讯股份有限公司
执行副总裁 |
| • 王育民 | 西安电子科技大学教授 | • 郑纬民 | 清华大学教授, 中国计算机学会
理事长 |
| • 韦乐平 | 中国电信集团公司科技委主任 | • 钟义信 | 北京邮电大学教授 |
| • 卫 国 | 中国科学技术大学教授 | • 朱近康 | 中国科学技术大学教授 |

第 11—20 次编委会掠影



第 11 次编委会



2005 年 8 月 13—14 日,《中兴通讯技术》杂志第 11 次编委会在深圳市召开。

在创刊 10 周年之际,杂志荣获“第 3 届国家期刊奖百种重点期刊”称号,并进入“中国科技核心期刊”行列。会议指出,刊物可以在保持基本定位不变的前提下,尝试向 E 检索努力,会议通过了栏目调整的方案。

第 12 次编委会

2006 年 8 月 12—13 日,《中兴通讯技术》杂志第 12 次编委会在西安市召开。侯为贵董事长到会并致辞。

会议明确不能单纯为了进入 E 而改变刊物现有特色,刊物影响力是关键,要加大英文刊在海外的发行量,包括著名大学、科研机构和国际组织等。

第 13 次编委会



2007 年 8 月 18—19 日,《中兴通讯技术》杂志第 13 次编委会在宁波市召开。殷一民总裁到位并致辞。

会议肯定了中英文两刊的进步,以及对外交流活动和队伍建设取得的成绩。代表们听取了中兴通讯的国际化发展历程和成就的专题汇报,并对“IT 对传统电信业的影响”和“未来移动通信的发展趋势”两个专题展开了深入讨论。

第 15 次编委会



2009 年 8 月 15—16 日,《中兴通讯技术》杂志第 15 次编委会在贵阳市召开。侯为贵董事长到会并发言。

会议肯定了杂志社在扩大组稿队伍、调整刊物栏目、提高发行质量、提升管理水平方面所做出的努力和取得的成果,提出下年度工作重点将聚集英文刊海外组稿和海外发行。本次会议首次邀请海外专家参会。

第 14 次编委会



2008 年 7 月 26—27 日,《中兴通讯技术》杂志第 14 次编委会在哈尔滨市召开。

会议总结了年度办刊工作,汇报了中兴通讯在汶川抗震救灾中的积极行动和对北京奥运通信的支持。论坛期间,代表们对“宽带接入技术及承载网”、“网络融合及业务融合”和“中兴通讯产学研论坛筹划”进行了分组讨论。产学研合作第一次提上会议议程。

编委会回顾

第17次编委会



2011年8月13—14日,《中兴通讯技术》杂志第17次编委会在张家界市召开。

侯为贵董事长在会上分析了国内外通信市场发展现状,希望以刊物为纽带,促进产学研合作,使中兴通讯在技术上有更多创新,市场上更具差异化竞争力。会议指出中英文两刊可以走差异化的发展道路。会议分别就办刊和产学研工作的开展进行了汇报和研讨。

第18次编委会



2012年8月18—19日,《中兴通讯技术》杂志第18次编委会在郑州市召开。

编辑部汇报了年度办刊工作以及产学研合作取得的成绩。会议讨论通过了编委任期制度,新增邬贺铨、童晓渝、孙信信3位编委。尤肖虎、张平、曾文军等15位海内外专家针对移动互联网、通信网络智能化等行业热点做了精彩报告。邬贺铨院士首次参加编委会,并对刊物发展提出希望。

第16次编委会



2010年8月7—8日,《中兴通讯技术》杂志第16次编委会在青岛市召开。侯为贵董事长、史立荣总裁参会。

编辑部首次以PPT形式总结、回顾了15年办刊历程。会议对做出突出贡献的编委专家进行了表彰,并提出刊物要有更高的理想,要做“百年名刊”。

第20次编委会



2014年8月9—10日,《中兴通讯技术》杂志第19次编委会在银川市召开。史立荣总裁到会并介绍了中兴通讯M-ICT战略。

会议总结了编辑部各项工作以及产学研合作进展,对刊物专题运作机制、刊物定位、编委会议程进行了重新思考,提出了进一步提升的举措,确定中文刊聚焦观点文章,英文刊增加Review栏目。会议通过了新增两位编委会副主任的提议,并建议英文刊尽快以双月刊出版。

(第1—10次编委会掠影见2005年创刊10周年纪念特刊)

第19次编委会



2013年8月3—4日,《中兴通讯技术》杂志第19次编委会在呼和浩特市召开。

会议总结了杂志社一年来工作成果,汇报了两刊编委会运作情况,以及英文刊为进入EI等数据库采取的举措:加强国际化、网络化,提高学术性、成果性。会议宣布了新增编委名单。首次召开英文刊专题研讨会,取得积极成果。

中兴通讯成立 30周年大事记

- 1985 年** 2月,深圳市中兴半导体有限公司成立。
- 1986 年** 自主研发成功第一台交换机 ZX60。
- 1989 年** 11月,自主研发的 ZX-500 数字程控交换机面市,它被认定为国内具有自主知识产权的国产化第一台数字程控交换机。
- 1991 年** 12月,适应中国农话 C5 局端数字改造的小容量数字局用交换机 ZX500A 研制成功,并在江苏和江西两省实验局成功开通,开创了国产交换机进入农村市场的先河。
- 1993 年** 3月,航天系统 691 厂、深圳广宇工业(集团)公司与中兴维先通共同投资组建深圳中兴新通讯设备有限公司,注册资金 300 万元,首创“国有民营”的经营机制。
10月,南京研究所成立。
ZXJ10 局用交换机在江苏射阳镇开通实验局,11月获得邮电部颁发的人网许可证,作为国内自行研制的第三个人网机型,ZXJ10 在邮电部组织的专家评审中被认定为“是目前能与国际一流机型相媲美的最好机型”。



中兴通讯成立 30 周年大事记

1994 年

8 月,上海研究所成立。

1995 年

启动国际化战略,史立荣副总裁只身前往日内瓦参加 ITU 世界电信展。
创办《中兴新通讯》杂志。

1997 年

11 月 18 日,在深圳证券交易所 A 股成功上市。

1998 年

6 月,在美国设立研究机构(新泽西、圣地亚哥、硅谷共 3 家)。
10 月 17 日,获巴基斯坦交换总承包项目,金额为 9 700 万美元,是当时中国通信制造企业在海外获得的最大一个通信工程项目,令世界瞩目。
12 月,北京研究所成立。

1999 年

在安徽六安与中国联通签订了第一个 GSM 实验局,不久又在河北保定开通 1 800 M 实验局,由此开始进入无线领域。

2000 年

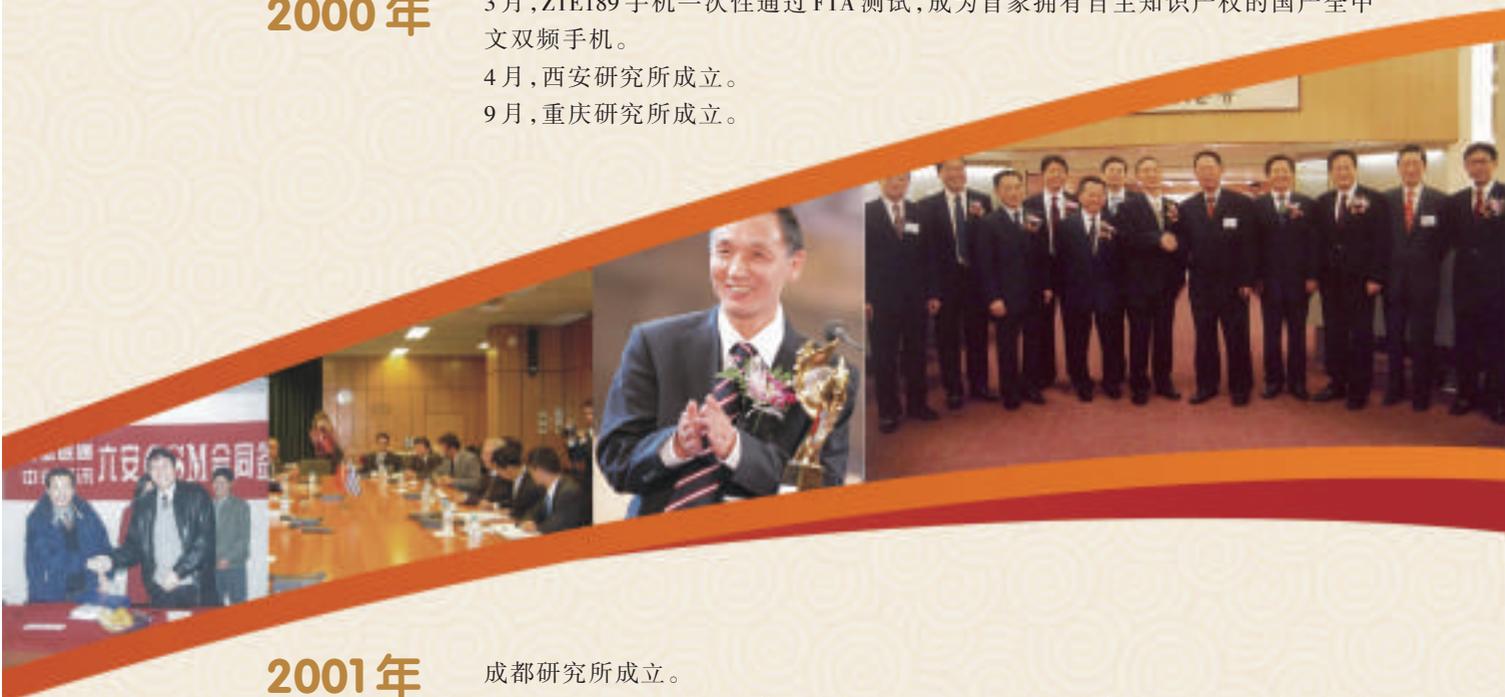
3 月,ZTE189 手机一次性通过 FTA 测试,成为首家拥有自主知识产权的国产全中文双频手机。
4 月,西安研究所成立。
9 月,重庆研究所成立。

2001 年

成都研究所成立。
5 月 15 日,CDMA 移动通信系统中标中国联通 110 万线合同,正式进入大规模商用阶段。
5 月,签订价值近亿元的重庆移动 GSM 六期扩容工程项目。GSM 设备覆盖全国二十几个省,并远销国外近十个国家。

2002 年

与英特尔(中国)有限公司签署合作备忘录,在未来 3G 无线通信、无线局域网等几个关键领域展开深层次合作。



- 2003 年** 自主研发 GoTa 数字集群通信系统,这是国际范围内首次由中国企业发布的具有自主知识产权的数字集群通信产品,拥有数 10 项核心专利。
中标希腊雅典奥运会项目,承建 16 个重点比赛场馆的 ADSL 宽带数据接入工程项目。
- 2004 年** 6 月,与突尼斯交通通信部签订 WCDMA 网络建设合同,这是公司为国际电信服务提供商建设商用 3G 网络的开始。
12 月,H 股在香港联合交易所成功上市。
- 2005 年** 12 月,与和黄英国公司签署 30 万部 WCDMA 终端合同,3G 终端首次大规模进入欧洲市场。
打通了国内第一个 TD 电话。
作为第一批 EPON 试点厂家参与中国电信宽带网络建设。
- 2006 年** 在青岛麦岛站开通业界首例 BBU + RRU 光纤基站解决方案,使 TD 规模组网成为可能,并使运营商降低 60% 的工程量,缩短 50% 以上的工程周期,大幅降低了 TCO。
- 2007 年** 2 月,与全球移动通信运营商英国沃达丰(Vodafone)正式签署合作协议,为沃达丰提供其品牌标准的手机。
11 月,天津研究所成立。
- 2008 年** 9 月,三亚研究所成立。
9 月,成为全球第六大手机厂商。
- 2009 年** 4 月,全球首家实现了 CDMA/LTE 双模系统。
9 月,CSL 宣布与公司在香港建立第一个 LTE 商用测试网络。
9 月,发布全球首个 10G EPON 试商用,À 开 10G EPON 时代的序幕。
GSM 全年销售额已达到 118 亿元,成为公司首个突破百亿的产品,全年新增市场占有率达到 20%,排名全球前三。
自主研发明星产品 ZXR10 T8000 获中国创新设计红星奖金奖,是国内自主知识产权程度最高的集群路由器,三大核心芯片均由中兴通讯自主研发。
- 2010 年** 与尼泊尔 Ncell 在珠穆朗玛峰南坡大本营开通全球海拔最高的 3G 站点。
CDMA 产品以 30% 份额居全球市场首位。
6 月,武汉研究所成立。



中兴通讯成立30周年大事记

2011年

7月,完成业界首次TDD LTE与2G/3G网络互操作。
为和记电讯在奥地利部署LTE/DC-HSPA+全国网。
为和在瑞典、丹麦独家建设LTE FDD/TDD双模商用网。
推出全球首个LTE商用一体化小型微站。
全球首款TD-LTE多模双待智能手机亮相大运会。
在南京成立全球云计算中心。
政企网全年国内增长率高达90%。

2012年

2月,发布全球最薄四核智能机Grand Era。
3月,长沙研究所成立。
10月,中标中国移动TD-LTE招标项目13 000载频,成为中国移动第一大LTE设备供货商。

2013年

3月,国际专利2012年度申请量达3 906件,位居全球第一。
5月,PTN产品ZXCTN 6500获Frost & Sullivan综合技术排名第一。
6月,光网络产品跃居全球第二。
6月,业界首次实现400 Gb/s信号超5 000 km超长距离传输。
6月,IPTV市场份额位列全球第二。
9月,连胜美国2宗337专利调查,已构筑5万件专利“长城”。
中国电信4G LTE网络主设备招标中,LTE产品进入90%招标省份,占据近40%市场份额,在无线、核心网的市场份额均排名第一。

2014年

3月,视频会议产品跃居全球前三。
推出“微品会”平台,引爆全员B2C2C的销售模式。
发布M-ICT战略。
二季度FTTH CPE出货量排名全球第一。
二季度PON产品排名全球第二,其中EPON产品市场份额稳居全球第一。
9月,携手蜀都客车发布全球首个无线充电城市微循环公交解决方案。
9月,天机手机被选为国礼赠送外宾。
承建全球首个轨道交通商用4G无线宽带多媒体集群网。
承载产品PTN市场占有率连续三年排名第一。
10月,同时获得移动支付、互联网支付和数字电视支付业务许可,成为国内首家一次性获得以上三张牌照的第三方支付机构。
12月,发布语音手机星星2号。

2015年

在迎来30岁生日之际,中兴通讯全球发布新的品牌标识。M-ICT(万物移动互联)时代,以CGO(Cool、Green、Open)为核心指导思想,积极布局国内外运营商市场、政企市场、全球终端市场以及无线充电等新兴蓝海市场,寻求企业新一轮的发展。



中兴通讯技术杂志社 办刊 20 周年大事记

1995—2000 年 (开拓创新的五年)

1995 年 6 月,《中兴新通讯》编辑部成立,编委会组建

1995 年 7 月,《中兴新通讯》正式创办,获省级刊号,季刊出版

1997 年 1 月,《中兴新通讯》改为双月刊

2000 年 7 月,《中兴新通讯》获正式刊号,国内外公开发行,同时更名为《中兴通讯技术》

2000 年 10 月,《中兴通讯技术》被《中文科技期刊数据库》收录

1995

2000

2005

2001—2005 年 (快速发展的五年)

2001 年 8 月,《中兴通讯技术》获安徽省优秀科技期刊二等奖

2002 年 9 月,《中兴通讯技术》获第三届华东地区优秀期刊奖

2002 年 12 月,《中兴通讯技术》被《中国核心期刊(遴选)数据库》收录

2003 年 6 月,《ZTE Communications》创刊,季刊出版,中兴通讯技术杂志社成立

2003 年 7 月,《中兴通讯技术》入选为《中国学术期刊综合评价数据库(CAJCED)》统计源期刊

2003 年 7 月,《中兴通讯技术》被《中国期刊全文数据库(CJFD)》全文收录

2003 年 12 月,《中兴通讯技术》荣获首届《CAJ-CD 规范》执行优秀期刊奖

2004 年 1 月,《中兴通讯技术》被收录为“中国科技论文统计源期刊”(中国科技核心期刊)

2005 年 1 月,《中兴通讯技术》荣获第三届国家期刊奖百种重点期刊

2005 年 10 月,《ZTE Communications》获正式刊号,国内外公开发行

2006—2010年（国际化发展的五年）

- 2006年6月,《ZTE Communications》被《中国期刊全文数据库(CJFD)》全文收录
- 2008年7月,《ZTE Communications》被美国《乌利希期刊指南》(Ulrich's Periodicals Directory)收录
- 2009年3月,《ZTE Communications》被美国《剑桥科学文摘(工程技术)》(CSA(T))收录
- 2009年5月,《ZTE Communications》被波兰《哥白尼索引》(Index Copernicus)收录
- 2009年11月,《中兴通讯技术》获安徽省优秀期刊奖
- 2009年11月,《中兴通讯技术》获第四届华东地区优秀期刊奖
- 2010年5月,《ZTE Communications》被《中国核心期刊(遴选)数据库》收录

2010

2015

2011—2015年（产学研合作的五年）

- 2011年1月,《ZTE Communications》被《中文科技期刊数据库》收录
- 2011年3月,《ZTE Communications》组建编辑委员会,刊物开始独立组稿,独立运作
- 2011年12月,《中兴通讯技术》获工信部优秀科技期刊奖
- 2012年7月,建立编委任期制,并发布《中兴通讯技术》杂志编委聘任制度文件
- 2012年12月,《中兴通讯技术》获年华东地区优秀期刊奖
- 2012年12月,《ZTE Communications》被英国 INSPEC 数据库收录
- 2013年2月,两本刊物引入 DOI 并启用数字优先出版
- 2013年6月,《ZTE Communications》被挪威 NSD 数据库收录
- 2014年8月,要求20万元以上的产学研项目为《ZTE Communications》提交一篇原创论文
- 2015年1月,两刊调整栏目,体现刊物观点性、思想性、原创性
- 2015年3月,《中兴通讯技术》被评为“RCCSE(中国学术期刊评价研究中心)中国核心学术期刊(A)”
- 2015年4月,明确数字化出版发展路径,提出建立刊物门户网站的设想
- 2015年6月,出版纪念创刊20周年特刊以及画册



信息通信领域产学研合作特色期刊
第三届国家期刊奖百种重点期刊
中国科技核心期刊
工信部优秀科技期刊
中国五大文献数据库收录期刊
ISSN 1009-6868
CN 34-1228/TN
1995年创刊

办刊宗旨

以人为本,荟萃通信技术领域精英;
迎接挑战,把握世界通信技术动态;
立即行动,求解通信发展疑难课题;
励精图治,促进民族信息产业崛起。

Contents 目次

中兴通讯技术 总第122期 第21卷 第3期 2015年6月

特稿

01 人工智能:信息技术的制高点 钟义信

专题:移动互联网安全技术

- 04 云计算环境下移动互联网安全问题研究 刘权,王涛
07 蜂窝移动通信系统的安全架构 徐晖,孙韶辉
11 移动终端高安全可信计算平台架构 刘建伟,程东旭,李妍
16 移动互联网服务的隐私保护机制 李晖,牛犇,李维皓
23 智能移动终端的位置隐私保护技术 杜瑞颖,王持恒,何琨
30 移动数字取证技术 丁丽萍,岳晓萌,李彦峰
34 基于Android移动客户端的互联网数据安全实证研究 何昱晨,石文昌
38 移动互联网安全测评关键技术研究 范红,杜大海,王冠

专家论坛

- 41 高移动无线通信干扰的物理层应对思考 陈文
45 对高铁宽带移动通信系统架构演进的思考 方旭明

企业视界

50 对无线新技术演进的思考 向际鹰

技术广角

55 HSPA+异构网中信道分离技术的时延补偿研究 李红豆,王柯,常永宇

综合信息

IDC:全球超六成制造商已使用云计算 (22) 全球未来网络暨SDN技术大会北京开幕 (29)
2019全球IP流量预计将达2 ZB 视频占80% (49)

期刊基本参数:CN 34-1228/TN*1995*b*16*64*zh*P* ¥ 20.00*15000*13*2015-06

Contents 目次

ZTE TECHNOLOGY JOURNAL Vol. 21 No. 3 Jun. 2015

Guest Paper

01 Artificial Intelligence: The Commanding Heights of Information Technology ZHONG Yixin

Special Topic: Security Technology in Mobile Internet

04 Mobile Internet Security in Cloud Computing LIU Quan, WANG Tao

07 Security Architecture of Cellular Mobile Communication System XU Hui, SUN Shaohui

11 A High and Trusted Computing Platform Architecture
for Mobile Terminal LIU Jianwei, CHENG Dongxu, LI Yan

16 Privacy Mechanism in Mobile Internet LI Hui, NIU Ben, LI Weihao

23 Location Privacy Protection Technology
on Smart Mobile Devices DU Ruiying, WANG Chiheng, HE Kun

30 Mobile Forensics Technology DING Liping, YUE Xiaomeng, LI Yanfeng

34 Internet Data Security Based on Android Mobile Clients HE Yuchen, SHI Wenchang

38 Key Technologies of Security Test for Mobile Internet FAN Hong, DU Dahai, WANG Guan

Expert Forum

41 Physical Layer Consideration for the Interference
in High Mobility Wireless Communications CHEN Wen

45 Evolution of Broadband Mobile Communication System Structures
for High-Speed Railway FANG Xuming

Enterprise View

50 Evolution of Wireless New Technologies XIANG Jiyong

Technology Perspective

55 Delay Compensation for HSPA+HetNet
Decoupling LI Hongdou, WANG Ke, CHANG Yongyu

敬告读者

本刊享有所发表文章的版权,包括英文版、电子版、网络版和优先数字出版版权,所支付的稿酬已经包含上述各版本的费用。

未经本刊许可,不得以任何形式全文转载本刊内容;如部分引用本刊内容,须注明该内容出自本刊。

邮购须知

本刊常年办理邮购订阅业务,欢迎订阅。订阅方法:从邮局汇款至编辑部,在汇款单上将订阅者的详细地址、收件人姓名及联系电话填写清楚,并在汇款单附言栏注明所购杂志期次及数量。



刘建伟

北京航空航天大学电子信息工程学院教授、博士生导师、党委书记，现担任中国密码学会理事、教育部高等学校信息安全专业教学指导委员会委员；主要研究领域包括：密码学、信息安全、网络安全；曾获国家技术发明一等奖1项，国防技术发明一等奖1项，山东省计算机应用优秀成果二等奖1项，山东省科技进步三等奖1项；承担国家级课题10余项，发表论文100余篇，已获授权发明专利17项，出版专著和教材5部，译著1部。

专题导读

随着智能手机和可穿戴电子设备的迅猛发展和广泛应用，人类进入了移动互联网的新时代。移动互联网的发展，彻底改变了人们的生活和工作方式，让人们可以在任何时间、任何地点，以任何移动终端接入互联网。移动互联网与传统行业的融合，催生了手机银行、移动电子商务、移动视频、移动游戏、移动传媒等新的业务模式，并创造了诸如阿里巴巴般的经济神话。微信、手机QQ、滴滴打车、手机淘宝等移动互联网新应用，正如雨后春笋般地出现在人们的手机屏幕上，令人们耳目一新，使人们切身体会到移动互联网给人们的生活带来的日新月异的变化。

当前移动互联网还在继续发展，其应用将延伸到教育、医疗、旅游、交通等众多新领域。此外，移动互联网与云计算、大数据、物联网等新技术结合，必将带来更多新的应用。移动互联网将极大地促进中国的信息化建设进程，加速中国进入“互联网+”的新时代。

在移动互联网环境下，TCP/IP协议族的脆弱性没有改变，移动终端操作系统的安全漏洞依然存在，网络攻击的手段不断翻新，手机病毒和木马呈现多态势，从而造成网银账户的失窃、电商网站屡遭黑客攻击、有害和垃圾信息大量传播等安全事件，这一切对移动互联网造成了极大的安全威胁，动摇着人们对移动互联网安全性的信心。

目前，移动互联网的安全问题已经引起各国政府和科研机构的高度重视，成为当前全球的一个研究热点。中国科技部、工信部以及自然科学基金委等部门均已设立了移动互联网安全研究的重大专项和研究课题，正积极开展研究以应对移动互联网面临的安全挑战。

移动互联网的安全问题不仅涉及网络安全、系统安全、信息安全、内容安全等问题，还与国家的政策、法律等方面息息相关。我们精心策划了本期专题，主要目的是与大家一起讨论移动互联网安全与隐私保护技术层面的问题。本期刊物收录的论文凝聚了作者多年的研究成果和工作经验，希望能与读者朋友分享。作为本期专题的策划人，在此对各位作者对本期专题的积极支持和辛勤工作致以衷心的感谢。

刘建伟

2015年5月10日

2015年第1—6期专题计划

1

自组织异构小基站网络

张平 北京邮电大学网络技术研究院 执行院长

2

移动云计算和云服务

唐雄燕 中国联通网络技术研究院 首席专家

3

移动互联网安全技术

刘建伟 北京航空航天大学电子信息工程学院 教授

4

软件定义光网络

迟楠 复旦大学信息科学与工程学院 教授

5

虚拟运营业务和网络

续合元 中国信息通信研究院通信标准研究所 总工

6

移动群智感知和协同计算

王文东 北京邮电大学软件学院 教授

[编者按] 人工智能一直处于技术创新的前沿,成为信息技术的制高点。在本刊创办20周年之际,编辑部特邀本刊编委会主任、人工智能著名专家、北京邮电大学钟义信教授就人工智能技术的定位及发展发表高见。钟教授认为,发展和应用人工智能技术是实现科技创新和应对复杂挑战的有效途径,需要中兴通讯这样的创新型企业大力研究人工智能技术,积极推动人工智能技术的快速发展和广泛应用。

人工智能:信息技术的制高点

——献给《中兴通讯技术》创刊20周年

钟义信/ZHONG Yixin



钟义信,北京邮电大学计算机学院智能科学技术研究中心教授;一直从事信息科学与人工智能的基础理论研究;先后提出并完成了全信息理论、知识生态学理论、智能的机制模拟理论和人工智能统一理论的建构;在相关领域出版了18部学术专著,发表了480多篇论文。

2015年是《中兴通讯技术》创刊20周年。20年来,《中兴通讯技术》和信息技术一起都取得了令人瞩目的进展。在20年这个时间节点上,我们需要思考:下一个20年信息技术将何去何从?是走向新型信息技术?还是走向人工智能?显然,前者是一个偷懒的敷衍说法,因为任何时候人们都可以把未来的某种技术叫做某种新型技术,而后者才是一个认真的科学答案。

1 人类智能和人工智能的概念

和其他生物物种不同,人类是一种智慧型生物。人类智慧包含两个相辅相成的部分:隐性智慧和显性智慧。隐性智慧负责发现和确定创新的方向,显性智慧负责在确定的创新方向上实现具体的创新求解。更具体地说,隐性智慧是人类发现问题和定义问题的能力,需要全局性的分析能力、想象能力和开拓能力,是一种内隐的创造性能力,因而不可被机器模拟;显性智慧是人类在隐性智慧所定义的问题框架内解决问题的能力,需要获取信息生成知识和运用知识

解决问题的能力,是外显的操作能力,因而可以被机器模拟。人类的显性智慧通常也会被称为人类智能,模拟人类智能(显性智慧)的科学技术就叫人工智能。

图1所示就是一个功能完整的人工智能科学技术模型。

模型中的隐性智慧表现在:面对环境定义的实际问题;为知识库提供的已有知识;预设的问题求解目标。这三者就是隐性智慧定义的工作框架。在这个框架下,人工智能系统所要执行的任务就是模拟人类智能(显性智慧)的能力,运用所提供的信息和已有知识解决所给定的实际问题,达到预定的求解目标。

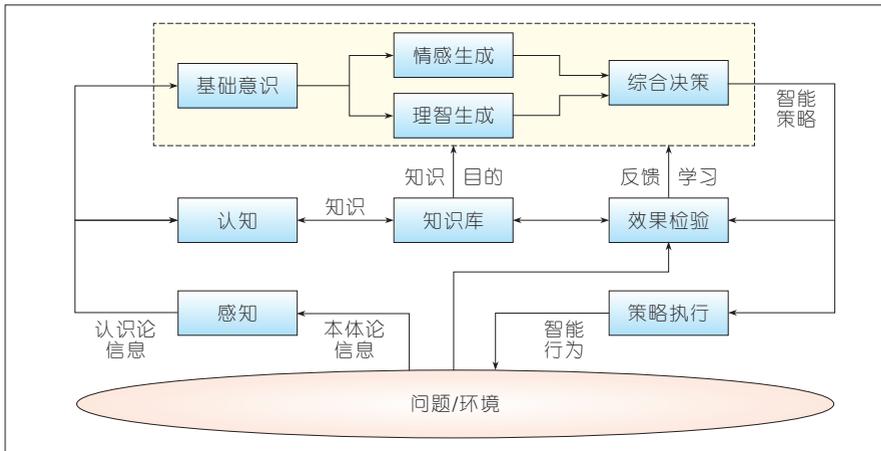
但是,图1所表示的人工智能系统模型比较复杂,适合科学研究。针对本文讨论的需要,我们把它加以简化,成为图2所示的简化模型。

模型表明了人工智能系统工作的基本过程:

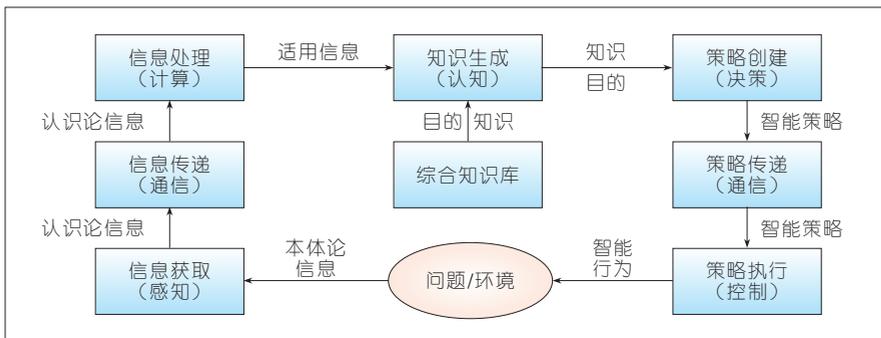
(1)人类主体(隐性智慧)首先设定工作框架,即定义要解决的实际问题,提供已有知识,预设求解目标。

(2)人工智能系统收集工作框架的信息,包括模型中的本体论信息。

收稿日期:2015-05-05
网络出版时间:2015-05-11



▲ 图1 人工智能系统模型



▲ 图2 人工智能系统的简化模型

(3) 通过信息获取(感知)单元, 把本体论信息转换为认识论信息。

(4) 通过信息传递(通信)单元, 把认识论信息传送到信息处理单元。

(5) 通过信息处理(计算)单元, 使认识论信息成为适用信息。

(6) 通过知识生成(认知)单元, 根据求解问题的需要生成专门知识。

(7) 通过策略创建(决策)单元, 把认识论信息、专门知识、求解目标转换为求解问题的智能策略。

(8) 通过策略传递(通信)单元, 把智能策略传递到策略执行单元。

(9) 通过策略执行(控制)单元, 把智能策略转换为智能行为, 反作用于实际问题。

(10) 如果智能行为反作用于实际问题的结果没有满意地实现预期的求解目标, 就把误差作为新的信息反馈到信息获取(感知)单元, 通过学习, 补充新的知识, 优化智能策略, 改

善执行效果, 减小求解误差。

完成第(10)步以后, 人类隐性智慧又会定义新的工作框架, 人工智能系统就开始新一轮模拟人类显性智慧能力的工作。如此循环往复, 螺旋上升, 不断地展开人类主体与人工智能系统之间和谐默契的合作, 不断改善人类生存发展水平。

以上步骤表明, 在人类与人工智能系统之间, 人类始终是主体, 人工智能系统则是人类求解问题的聪明工具。由于人工智能系统接受了人类所预设的求解目标和提供的专门知识, 就保证了人类主体与客体之间实现主客双赢的策略: 主体赢, 因为实现了主体的求解目标; 客体赢, 因为遵守体现在知识中的客观规律^[4]。

2 人工智能技术

以上论证说明: 人工智能技术可以在人类隐性智慧定义的工作框架

内模拟人类显性智慧(人类智能)生成知识, 创建主客双赢的策略解决各种复杂问题。而这是现今其他各类技术做不到的。

不过, 由于在人工智能系统工作的基本过程中, 第(1)步中客观存在各种不确定性, 人类给定的知识未必能够理想地体现客观规律, 也未必能够完全满足求解问题的需要, 第(2)步中人类预设的求解目标也不见得完全合理, 第(3)步中人工智能系统各个环节必然存在各种不理想性。因此, 人工智能系统对人类显性智慧能力的模拟不可能完全到位, 人工智能系统提供的问题解答也可能不如人类求出的解答。

如果说人工智能系统确实也有超人的地方, 那主要是它的工作速度、工作精度、持久能力等因素, 而不可能是显性智慧中的智慧品质。

至于一些人所宣传的机器超越人类甚至机器淘汰人类的说法, 是没有根据的。无论是人工智能系统, 还是其他各种机器系统, 它们共同的问题之一是: 机器没有生命, 没有目的, 不可能自主发现应当解决的实际问题, 不可能自主形成机器的智慧, 尤其不可能无中生有地形成超越人类和淘汰人类的荒唐愿望, 因此更不可能产生淘汰人类或灭绝人类的行为。

3 人工智能与信息技术的关系

图2的人工智能系统模型表明, 完整的人工智能技术系统必须具有如下环节: 信息获取(感知)、信息传递(通信)、信息处理(计算)、知识生成(认知)、策略创建(决策)、策略执行(控制)以及反馈学习优化等基本技术系统, 这正像“人”这个智能系统必须具有感觉器官(信息获取)、传输神经系统(信息传递)、思维器官(信息处理、知识生成、策略创建)以及执行器官(策略执行)。

其中传感(感受信息)、通信(传递信息)、计算(处理信息)、控制(执

行信息)等技术属于信息技术。可见,人工智能系统是一个全局整体,其中包含着传感、通信、计算、控制等信息技术环节;这正像人这个智能系统是一个全局整体,其中包含感觉器官、传输神经、丘脑和执行器官。

如果把人工智能系统称为完整的人工智能系统,而把其中的知识生成和策略创建称为核心人工智能系统,那么,则有:

完整的人工智能系统 = 核心人工智能系统 + 信息技术系统

其中,核心人工智能系统处于完整人工智能系统的核心,处理知识和智能层次的问题;信息技术系统处于完整人工智能系统的外周,处理信息层次的问题,同时担任核心系统与外部环境之间的两端接口:一端是从环境获取本体论信息(传感),另一端是对环境施加智能行为(控制)。

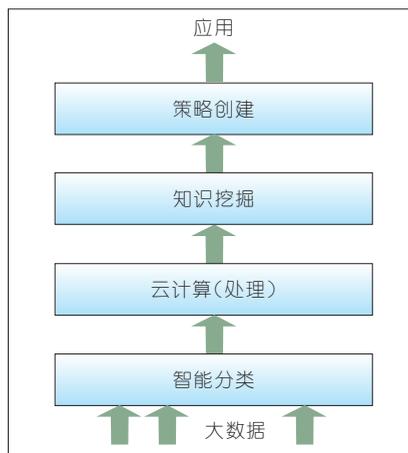
这就表明,信息技术系统提供给人类的服务主要是方便快捷的信息共享,而不可能提供如何认识事物本质的服务(因为这需要知识),更不可能提供如何解决问题的服务(因为这需要智能策略)^[1]。

4“新型”信息技术

近十多年来,先后出现了大数据、云计算、物联网、移动互联网以及各种互联网的应用技术。人们把它们称为“新型”信息技术或“新一代”信息技术。

深入分析可以发现,这些新型信息技术的核心技术正是核心人工智能系统的知识生成和策略创建技术。不妨以大数据技术为例加以说明。图3表示了大数据技术系统的工作流程。

由于有着多种来源、多种背景以及多种格式,大数据通常是病态结构或不良结构的大规模数据集,其中可能包含垃圾、病毒和黑客攻击程序。因此,如图3所示,大数据技术的第一个环节就是智能分类:把无用的数据识别分类出来加以过滤和抑



▲图3 大数据的工作流程

制,把有用的数据按照某些特征进行分类,再分门别类地送到恰当的云计算(和云存储)系统,进行相应的信息处理,为知识生成(知识挖掘)做好必要的准备。通过知识挖掘生成了足够的知识之后,才可以把这些知识(结合求解目标)转换成为用来解决问题的智能策略。其中,智能分类、知识挖掘和策略创建都是人工智能的基本技术。可见,如果没有这些人工智能技术,大数据就只能是数据,而不可能转换为有用的知识和可以用来解决问题的智能策略。

由此可知,大数据技术的核心就是人工智能技术,可以把它比较确切地称为面向大数据的智能技术。

真正的智能物联网模型不是别的,正是图2所示的模型。如图2所示,只要在综合知识库内设置“对物控制的目标”,那么“外部世界的物”的信息就经由传感器获得,经过通信系统传送到计算系统并在这里进行必要的处理即把信息变成适用的信息,接着由认知系统转换成为知识,然后由决策系统根据控制目标把信息和知识转换成为智能策略,智能策略再经通信系统传到执行系统之后转换成为智能行为反作用于所关注的“物”,使它的状态符合预设目标。

近来人们在密切关注着“互联网+”。其实,“互联网+”可以有两种不同的理解。一种理解是当前人

们所关注的互联网推广,这里的“+”就相当于信息化的“化”,就是互联网的各种应用。另一种更有意义的理解则把“互联网+”理解为互联网升级,就是把以计算机为终端的现有互联网升级为以人工智能系统为终端的智能互联网。

应当认为,互联网推广即把互联网应用到各行各业是完全必要的,这是信息化建设的正常要求。但是,从信息化建设的发展大势来看,互联网升级即把当前常规互联网升级为智能互联网则更为必要,这将为中国信息化建设注入更为强大的新活力,是转变经济发展方式的需要,是国民经济产业升级的需要。

综上所述,大数据技术、云计算技术、智能物联网技术,其实都是人工智能技术的相关具体应用。可以这么说,如果没有人工智能技术,单凭信息技术很难有效地应对大数据和物联网以及未来更多更复杂的技术挑战。

5 结束语

我们认为人工智能技术不会排斥信息技术,因为信息技术是人工智能技术系统的有机组成部分。强调人工智能技术的作用实际上也就强调了信息技术的作用,强调了信息技术的升级。

从现在开始的未来20年,中国和世界经济发展都进入深水区,面临越来越复杂的严峻挑战。发展和应用人工智能技术(而不是停留在一般信息技术的水平)是实现科技创新和应对这些挑战的有效途径。因此,需要像中兴通讯这样的创新型企业和国家各级决策层次大力宣传人工智能技术,积极推动人工智能技术的发展和应用,使中国的现代化建设走上健康发展的轨道。

参考文献

- [1] 钟义信.信息科学原理(第5版)[M].北京:北京邮电大学出版社,2013
- [2] 钟义信.高等人工智能原理[M].北京:科学出版社,2014

云计算环境下移动互联网安全问题研究

Mobile Internet Security in Cloud Computing

刘权/LIU Quan
王涛/WANG Tao

(工业和信息化部赛迪智库信息安全研究所, 北京 100846)
(Information Security Institute, CCID think tank, MIIT, Beijing 100846, China)

云计算和移动互联网是近年来发展十分迅速的IT领域,云计算颠覆了传统的IT资源管理和运营模式,实现了资源的按需使用和灵活配置,移动互联网前所未有地扩展了互联网的应用深度和广度。云计算和移动互联网具有天然的互补性,移动互联网内在要求应用随时随处可用、跨终端、跨平台且具有一致的用户体验,云计算的特性恰恰满足这些要求。在云计算环境下,移动互联网的安全问题更值得重视,一方面,云计算环境下移动互联网的一些固有问题会更加突出,另一方面,云计算环境催生移动互联网产生新的安全问题。因此需要采取有针对性的措施来提升云计算环境下移动互联网安全防护能力。

1 云计算概念与特点

1.1 云计算概念

云计算是通过互联网提供的一种动态可伸缩的虚拟化资源计算模式^[1]。广义云计算是指服务的交付和

收稿日期: 2015-03-19

网络出版时间: 2015-05-06

基金项目: 中国工程院重大资助项目(2013-ZD-10)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0004-003

摘要: 基于云计算的特点和移动互联网存在的安全问题,提出了云计算环境下移动互联网应用的新特点,指出了由此带来的新的安全问题,如通过移动互联网对云服务的攻击、云服务可用性面临严峻考验、企业的业务流程和业务数据面临更大风险等,并指出移动互联网一些固有安全问题更为突出,如个人隐私泄露、不良信息传播、个人信息滥用、综合信息挖掘等;从终端安全、网络通信安全、云端安全等方面,提出了提升云计算环境下移动互联网安全防护能力的对策与建议。

关键词: 移动互联网;云计算;信息安全

Abstract: In this paper, according to the characteristics of cloud computing and information security issues of mobile Internet, we discuss the new characteristics of mobile Internet application in cloud computing and new information security issues in cloud computing environment, such as attacks on cloud services via mobile Internet, severe challenges to the availability of cloud services, and the high risk of business process and data face risks. Some existing information security issues of mobile Internet are more serious in cloud computing environment, such as personal privacy leakage, proliferation of bad information, misuse of personal information and information mining. We propose countermeasures and suggestions to enhance mobile Internet security in cloud computing from aspects such as terminal security, network security and cloud security.

Keywords: mobile Internet; cloud computing; information security

使用模式,即通过网络以按需、易扩展的方式获得所需服务^[2],这种服务可以是和软件、互联网相关的IT服务,也可能是其他非IT服务。狭义云计算IT基础设施的交付和使用模式,指通过网络以按需、易扩展的方式获得所需资源。

1.2 云计算特点

一是资源的动态调拨与调整。实现云计算的基础是虚拟化技术,通过将主机、存储设备、网络、操作系统、数据库等各类资源的虚拟化,实现资源的动态调拨与调整,既实现了资源的高效利用,又实现了按需求提供资源。

二是一切皆服务。云计算实现了IT资源的集中与统一管理,在基础设施、平台及应用3个层次实现了由购买资源到购买服务的转变,即基础设施即服务(IaaS)、平台即服务(PaaS)及软件即服务(SaaS)^[2-3],用户只要按需租用虚拟资源、购买相应服务即可。

三是一切尽在云端。云计算提供的基础设施、平台和应用都在云端统一管理^[4],用户侧的需求被极大简化。与此同时,IT资源使用模式的转变,使得数据的所有权与管理权产生了分离,用户数据被转移到云端。除此之外,随着企业应用云计算的不断深入,企业的业务流程也被迁移到了

云端。

2 移动互联网特点及其安全问题

2.1 移动互联网概念

移动互联网是一种通过移动智能终端,采用移动无线通信方式获取业务和服务的新兴业态,包含网络、终端、软件、应用和数据5个层面。网络层包括多种无线通信技术的接入设施;终端层包括智能手机、平板电脑等;软件层包括操作系统、中间件、数据库和安全软件等^[2];应用层包括数字娱乐、生活服务、社交网络、商务财经等多种类别的应用与服务;数据层包括存储在移动终端、应用提供商、运营商等处的用户、系统、设备等的各类相关数据。

2.2 移动互联网特点

一是实现了随时随地接入互联网。移动互联网与传统互联网的本质区别,就是通过应用无线通信技术,使得接入互联网的终端具备了移动性,只要有网络信号支持,就可以实现随时随地接入互联网,随时随地地访问各类资源和服务。

二是终端类型多种多样。随着技术的不断发展和应用场景的不断丰富,移动互联网接入终端的类型也种类繁多。除了智能手机、平板电脑等之外,其他创新型接入终端不断产生,如形式各异的可穿戴设备。另外,随着移动互联网应用的深度、广度不断扩展,接入终端也不再仅仅是直接和人交互的,如汽车厂商应用移动互联网技术,推出了“互联网汽车”,在全球名声大噪的特斯拉电动车,更是将移动互联网作为其核心竞争力之一。

三是网络中的数据由静态向动态发展。传统互联网将现实中静态的数据搬到了互联网上,在传统互联网上发布的文本、声音、视频等各类信息,数据之间缺乏明显关联,本质

上是静态的和离散的。移动互联网将现实中动态的、连续的数据转移到了互联网上。由于用户随时随地可以接入移动互联网,用户数据具备时间和空间上的动态连续性,例如,可以不断收集用户地理位置和终端操作数据,这些数据具备时间上的因果关系和空间上的轨迹。同时,移动终端收集数据种类的丰富程度和粒度的精细程度都是传统互联网难以比拟的,使得移动互联网上的数据具有横向间的复杂关联。

四是向众多传统行业渗透力强。众多传统行业,其关键要素难以接入传统固定互联网,而应用移动互联网则可使这些要素轻松接入互联网,使这些行业对互联网的应用程度极大提升,产生根本性的变化。如物流行业,众多车辆只有依靠移动互联网才能实现精细管理与调度,又如医疗行业,通过应用移动互联网,可实现对人体生理指标的连续监测,大大提升服务效率和医治效果^[5]。

2.3 移动互联网面临的安全问题

目前,移动互联网面临的安全威胁主要包括以下几方面:

一是智能终端安全无法保证。移动智能终端面临比传统计算机更严峻的安全问题,由于用户安全防范意识薄弱、终端本身存在安全漏洞,导致用户手机终端受攻击的概率比传统PC机高得多。由于移动智能终端的随身性和私密性,用户还面临着隐私泄露等安全问题。

二是移动网络的不可靠性。在移动互联网环境下,传统网络中存在的明显的网络边界不再存在,用户可以随处接入并且可以跨区漫游^[6],因此像安全域划分、防火墙部署这样的边界防护机制在移动互联网环境下不再适用,使得移动互联网较传统网络具有更大的不可靠性。

三是业务的安全威胁。移动互联网固有的随身性、身份可识别等特性带来了更多的安全隐患,如多种途

径的对信息系统的攻击、敏感数据泄露、资费盗取、垃圾信息泛滥、非法内容的传播、产品和内容盗版等问题。尤其移动办公、移动支付、社交网络等对移动互联网信息安全提出了更高要求。

四是运营支撑安全问题严重。运营支撑涉及的安全内容包括用户身份及鉴权、流量控制、安全审计、资费管理、非法内容过滤与舆情管控、版权内容保护与访问控制等。移动互联网具有移动性大、业务种类丰富、用户身份与权限管理复杂^[7]等特点,网络安全监控和管理的工作也更加繁重。

3 云计算环境下移动互联网新特点及带来的安全问题

3.1 云计算环境下移动互联网应用新特点

移动互联网与云计算的结合,一方面拓展了移动互联网的应用范围,同时也增强了移动互联网应用功能。云计算环境下移动互联网应用呈现以下新特点:

一是云存储与数据分享广泛应用。云存储是最适于移动互联网应用的,国内的众多互联网巨头都积极推动其云存储业务向移动互联网普及,如百度、腾讯、360等推出的云存储服务都在移动互联网上使用^[8]。用户在云存储上存储的数据种类十分丰富,包括视频、照片、通讯录、通话记录、网上交易信息、位置记录、应用备份等。同时,数据分享十分便利,用户只需指定特定数据的访问权限,即可轻松地将其共享给使用同一服务的特定人群。除了用户间的数据分享,云服务之间的数据分享也十分容易,如百度的云存储服务,即可实现与其旗下应用市场、健身应用等之间的数据分享。

二是越来越多的移动互联网应用向云端转移。早期移动互联网应用大多是下载到移动终端安装的本

地程序,随着应用的功能复杂度不断提升,移动终端的处理能力、存储空间等难以满足应用要求,同时,移动终端的种类多样化,本地应用的维护和升级都十分困难。此外,移动互联网速度快速提升,终端系统和浏览器等对云服务的支持不断完善,促使移动应用向云端转移。一方面是一些本地的应用在后台利用云计算提供的服务,例如杀毒软件的云查杀、社交软件的云同步等,另一方面是一些应用从本地应用转换为云应用,通过云端的高效处理能力提供良好的用户体验,例如微软和谷歌公司都提供云办公软件^[1],在移动终端用浏览器即可随时使用。

3.2 云计算环境下移动互联网面临新的安全问题

一是通过移动互联网对云服务的多种攻击。移动终端上的病毒和恶意软件等会窃取云服务的账号、密码以及用户数据等。黑客通过对无线通信信号的嗅探,窃取云服务信息或破坏云服务。通过移动互联网对云服务的分布式拒绝服务(DDoS)攻击也日益频繁。基于移动互联网的攻击对云计算服务的威胁不断增大。

二是移动互联网使云服务可用性面临更加严峻的考验。移动互联网终端数量众多,一旦发生众多用户同时访问云服务的情况,将使云服务的可用性面临严峻考验。例如,2014年双十一期间,天猫一天的订单数近3亿,其中约一半来自移动互联网,后台云服务负载是平时的数十倍;2015年春节期间,腾讯的摇手机抢红包活动一晚就有上百亿人次参与,高峰时一分钟内摇手机8亿多人次,其背后的云服务压力可想而知。

三是企业的业务流程和业务数据面临更大风险。云计算环境下,企业通过不断将业务迁移到移动互联网上,通过无线网络获得移动办公便利的同时,也将业务流程和业务数据暴露在移动互联网中,面临诸多风

险。第一个方面是移动终端对高安全性的身份认证技术支持不够好,使得仿冒用户、破解终端与云服务的通信等更加容易;第二个方面是移动终端较易丢失,云服务容易被他人冒用;第三个方面是无线通信安全性较差,容易受到攻击或截取信息。

3.3 云计算使移动互联网固有安全问题更为突出

一是云应用使得对个人信息的收集和分析规模空前,影响更为严重。移动终端随时随地收集大量个人相关信息,各类云应用通过收集这些信息,经过分析,可以获得个人的隐私信息、活动范围、生活习惯、消费习惯、社会关系等大量有价值信息。终端上不同的云应用可能会互相交互分享各自获得的信息,以获取单个应用不可能得到的信息。这些信息若被滥用,会造成个人经济损失、隐私泄露等问题^[9]。

二是云存储等服务使个人相关信息集中存储,隐私泄露问题更加严重。云存储的应用使移动互联网产生的用户数据向云端转移^[9],集中存储,其中包含大量用户隐私数据,如照片、账号密码、通讯录、通话记录、交易记录等,一旦云端的安全措施不足或出现防护漏洞,就可能大量用户隐私数据泄露,相较于未应用云计算一般只会有个别或少量用户隐私数据泄露,其影响范围会大大增加,后果更加严重。

三是云应用收集大量用户信息并进行综合分析,威胁国家利益。云计算应用不仅对个体的信息收集更加全面,同时云计算的数据集中效应使得云平台可以获得大量个体的信息,通过对这些数据的综合分析,可以获得关于国家、社会的一些全局性、深层次的信息^[10],如大范围人员流动情况、经济运行数据、工业发展趋势等,这些信息具有极大价值,若被敌对势力利用,可能会威胁社会稳定和国家利益。

四是云平台使得通过移动互联网的不良信息传播更加快速,影响国家安全。移动终端可以通过拍照、摄像、录音等方式十分方便地记录信息,若反动、违法、色情等不良信息,一旦通过移动互联网上传到云平台并加以分享,可以迅速被大量用户获取,使得不良信息的传播呈现爆炸式,往往在监管部门感知和处理之前,已经扩散,造成不良后果。

4 提升云计算环境下移动互联网安全防护能力的对策与建议

4.1 提升终端安全防护水平

终端安全是移动互联网安全的核心,提升终端安全防护水平,对云计算环境下移动互联网安全具有重要意义。通过安装杀毒和防护软件,提高终端对病毒、恶意软件等的安全防护能力。对应用权限进行检测和限制,采用严格的资源访问控制策略,对应用私有资源进行隔离和保护。积极采用电子签名、反跟踪调试、代码加密等应用加固技术,防止逆向工程、非法篡改、动态注入、协议分析、漏洞挖掘等攻击,确保云服务账号密码等相关信息不被窃取,减少通过移动终端对云服务发起的DDoS等攻击。及时修补终端软硬件漏洞,加强操作系统、浏览器、硬件的安全性,提高访问云服务的安全性,防止利用系统漏洞窃密或攻击云服务。

4.2 加强网络通信安全

移动互联网由于网络制式众多、终端计算能力较弱、软件限制等,以及安全性较低的2G和Wi-Fi网络还在普遍应用,网络通信安全保护能力较传统网络更低。移动互联网下的大量云应用没有采取加密等强化网络通信安全的措施,例如通过不加密的HTTP协议访问云服务等。为保障

➔下转第15页

蜂窝移动通信系统的安全架构

Security Architecture of Cellular Mobile Communication System

徐晖/XU Hui
孙韶辉/SUN Shaohui

(大唐电信科技产业集团, 北京 100191)
(Datang Telecom Technology and
Industry Group, Beijing 100191, China)

在移动通信发展过程中安全技术是一个重要的研究领域, 移动通信技术发展的过程, 也是移动通信网络安全机制不断完善的过程。第4代移动通信系统最大限度地继承了UMTS的网络安全架构和机制, 并根据新的安全威胁和安全风险确定了新的安全架构和安全机制。

1 2G/3G 移动通信系统的安全架构

1.1 GSM 系统的安全特征

移动通信系统从GSM开始采用数字技术对用户语音、数据和信令进行加密保护, 并在网络中引入了身份鉴权技术来识别用户的身份。

GSM系统引入了用户识别模块(SIM)卡的技术, 实现了人机分离, SIM卡中存储签约用户的用户数据、安全数据和鉴权加密算法等。SIM卡与移动设备之间有一个开放的接口, SIM卡只有置入移动设备才能进行通信, 在用户接入网络时, 移动设备通过接口读取SIM卡中的用户数据, 并

收稿日期: 2015-02-27
网络出版时间: 2015-05-06
基金项目: 国家高技术研究发展(“863”)计划(2014AA012706)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0007-004

摘要: 总结了移动通信系统中的信息安全问题, 对GSM、UMTS和LTE移动通信系统的安全体系、安全目标、安全机制和安全缺陷等问题进行了详细分析; 对未来移动通信网络进行了展望, 认为未来移动通信网络是多种接入网络融合的通信网络, 是开放的、弹性的、可编程的网络, 其更加开放和灵活的网络架构不可避免地会引入新的安全风险。

关键词: 移动通信网络; 安全架构; 安全机制

Abstract: This paper summarizes the problem of information security in mobile communication systems, security architecture, security objectives, security mechanism and security flaws for GSM, UMTS, and LTE systems. This paper proposes that the future mobile communication system will be characterized by multi-RATs coordination, and it will be open and programmable. Such an open and flexible architecture will introduce new security risks.

Key words: mobile communication network; security architecture; security mechanism

将该数据发送给GSM网络, 请求接入网络。

在GSM系统中, 为用户提供了以下的安全功能^[1]:

(1) 对用户的身份进行了保护, 使窃听者无法确定用户的身份。

(2) 采用了A5/1的64位加密技术保护用户面和控制面, 使窃听者在无线链路上无法收听到通信内容。

(3) 采用鉴权机制, 对接入网络的用户身份进行认证, 防止未经授权的用户接入网络。

虽然GSM系统采用了一定的安全措施, 但是仍然存在着较大的安全风险, 其安全缺陷包括:

(1) GSM系统中的鉴权是单向的, 即只有网络对用户的鉴权, 用户不能对网络进行鉴权, 因此非法设备可以利用这个缺陷伪装成合法的网络设备欺骗用户。

(2) GSM系统使用的密钥长度是64位而且密钥生成算法固定, 比较容易在很短时间内被破解。

(3) GSM系统没有实现数据的完整性保护, 使信令容易被篡改。

(4) GSM系统只实现了空中接口的加密。

1.2 3G 移动通信系统的安全架构

基于2G系统的基础, 3G UMTS系统的安全架构保持了与GSM网络的安全兼容性, 确保2G/3G的互操作与切换, 在最初设计3G安全的时候, 第3代移动通信合作计划(3GPP)制订了指导方针, 即保留2G系统中必须的或者应增强的安全特征, 改进2G系统存在和潜在的弱安全特征和为新业务提供安全保护功能。为此, 3GPP制订了相应的安全目标^[2]:

(1) 为了防止用户产生的信息不

被滥用或者盗用,UMTS系统应该保护用户产生的信息或者与之相关的信息。

(2)为了防止网络提供的资源和服务不被滥用或盗用,UMTS系统应该保护归属网络和拜访网络提供的资源和服务。

(3)UMTS系统应该保证其安全方案可以在世界范围内使用,至少必须有一种加密算法能够在世界范围内使用。

(4)为了保证用户可以在世界范围内的不同服务网络之间漫游和互操作,UMTS系统应该保证其安全方案的标准化。

(5)UMTS系统应该保证其提供给用户和运营商的安全保护水平高于已有的网络。

(6)为了抵制各种攻击,UMTS系统应该保证可以根据新的威胁和新的服务要求对其安全能力进行扩展和增强。

为了实现安全目标,3GPP针对3G移动通信系统提出了新的安全体系架构^[9],如图1所示。新的安全体系架构可以分为3个层次5个方面:

(1)网络接入安全(第I类)。这部分安全主要解决用户接入UMTS接入网的安全,为用户提供安全接入UMTS接入网的机制,并保证无线链路的安全。这一部分的功能主要包括实现网络与用户之间的双向鉴权、控制面和数据面的机密保护和控制

面的完整性保护。

(2)网络域安全(第II类)。这部分主要解决核心网的安全问题,保证网间控制信令安全传送并抵御对核心网的攻击,实现了核心网内各个实体的身份鉴权、数据机密性保护和完整性保护等安全功能。

(3)用户域安全(第III类)。这部分主要解决了移动终端的安全问题,保证对移动终端的安全接入。实现全球用户识别模块(USIM)对用户的认证和终端对USIM的认证等安全功能。

(4)应用域安全(第IV类)。该安全能力主要确保用户应用与服务提供商提供的应用之间的信息安全传送。

(5)安全特性的可视性及可配置能力(第V类)。用户通过这个安全能力获知其是否正在使用安全特性,以及运营商提供的业务是否基于该安全特性。

相对于GSM系统,UMTS系统主要做了如下的改进^[9]:

(1)双向认证。UMTS系统的安全机制沿用了GSM系统的基本思想,并进行了增强。GSM系统采用的是网络对用户的单向认证,而UMTS系统增强为网络和用户之间的双向认证,不但基站需要对终端(MS)进行认证,而且终端MS也需要对基站进行认证,保证了基站和终端都是可信的实体。

(2)算法改进。UMTS仍然采用对称密钥密码体系,速度快,相对GSM系统对算法进行了改进,将GSM系统中使用的64比特长度的密钥增加为128比特,密钥破解难度大大增加。网络侧执行安全操作的节点从不可靠的基站转移到无线网络控制单元(RNC),进一步增强了系统的安全可靠性。

(3)接入链路信令数据的完整性保护。UMTS系统为信令提供机密性和完整性保护,对用户数据提供机密性保护。

(4)接入网的数据机密性保护延伸至无线接入控制器RNC。在UMTS系统中安全执行实体为用户终端(UE)和RNC。在核心网内部,如GPRS服务支持节点(SGSN)、拜访地位置寄存器(VLR)、归属地位置寄存器(HLR)等节点之间,使用基于因特网协议安全(IPsec)的安全机制,可以实现对消息来源的认证,以及消息的完整性保护、加密、重放保护等。

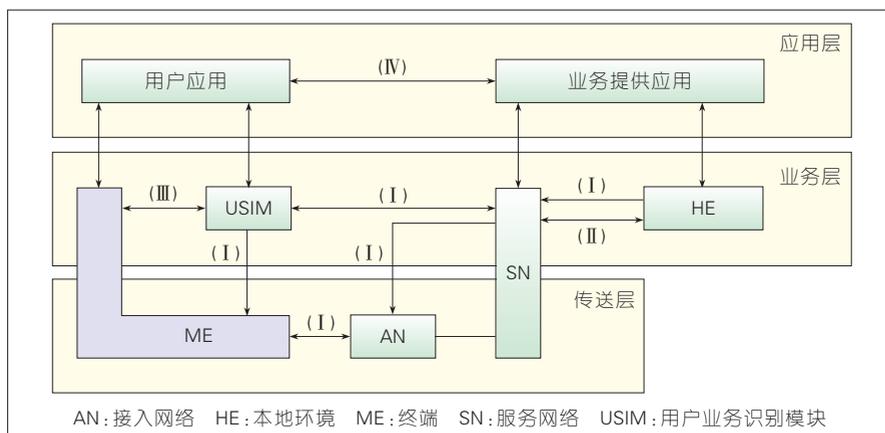
(5)UMTS系统可以让用户查看其所用的安全模式及安全级别。

(6)UMTS的安全机制还具有可扩展性,可以为将来引入新业务提供足够的保护。

但是,UMTS通信系统的安全机制仍然存在一些安全隐患,例如UMTS系统没有对非接入层进行安全保护,易泄露用户信息,同时UMTS系统没有实现终端对VLR的认证,易遭受重定向攻击,而且UMTS系统没有实现核心网实体间的认证和机密性保护,攻击者可以通过截取VLR与HLR之间的信息获得密钥信息。

2 LTE移动通信系统安全架构

LTE系统在UMTS系统的安全基础上进行了很大的改进,大大加强了网络的安全性。在UMTS系统中RNC负责执行安全保护功能,由于RNC安装在机房里,可以认为RNC位于安全的物理环境,所以UMTS系统只有一



▲图1 3G UMTS安全架构

层安全保护措施,保护 UE 到 RNC 之间的通信安全。但是在 LTE 系统中接入网只有基站(eNodeB)一层节点,而且 eNodeB 负责执行安全功能,在 LTE 系统部署中 eNodeB 是安装在室外的,受到攻击的可能大大增加了,因此 LTE 系统设计了两层安全保护,第一层是接入层安全,即演进型通用陆地无线接入网(EUTRAN)中的无线资源控制(RRC)层和用户层安全,第二层是非接入层安全,即 UE 与演进型分组核心网(EPC)之间的安全,如图 2 所示。LTE 系统这种设计的目的是使接入网安全和核心网安全的相互影响最小,从而提高了 LTE 系统的安全性,从部署的角度,运营商可以将 eNodeB 放置在易受攻击的位置,但是不存在高风险,而且可以在多种接入技术连接到 EPC 的情况下,更容易对整个系统的安全性进行评估和分析^[9]。

LTE 系统沿用了 3G 系统的安全架构^[6],包含 5 个安全特性组,如图 3 所示。与 3G 系统相比,LTE 系统主要有以下改进:

(1)在 AN 和 SN 之间实现了双向安全保护功能,保证了接入网(AN)和服务网络(SN)之间的数据的安全传输。

(2)在终端和 SN 之间进行双向安全保护,实现了终端 UE 和 SN 之间的非接入层安全。

(3)在归属网络本地环境(HE)和 SN 之间进行双向安全保护,实现了对服务网的认证。

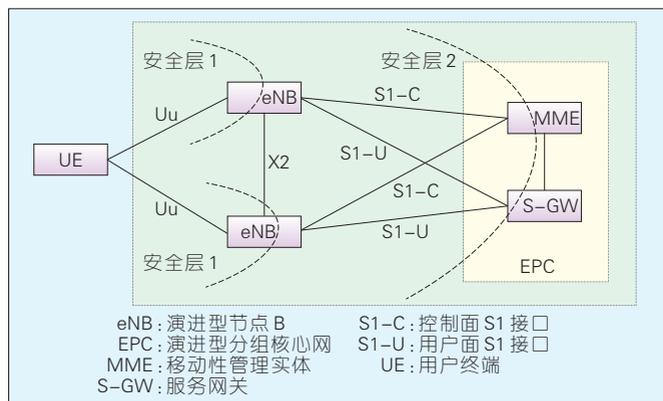


图2 LTE安全层次

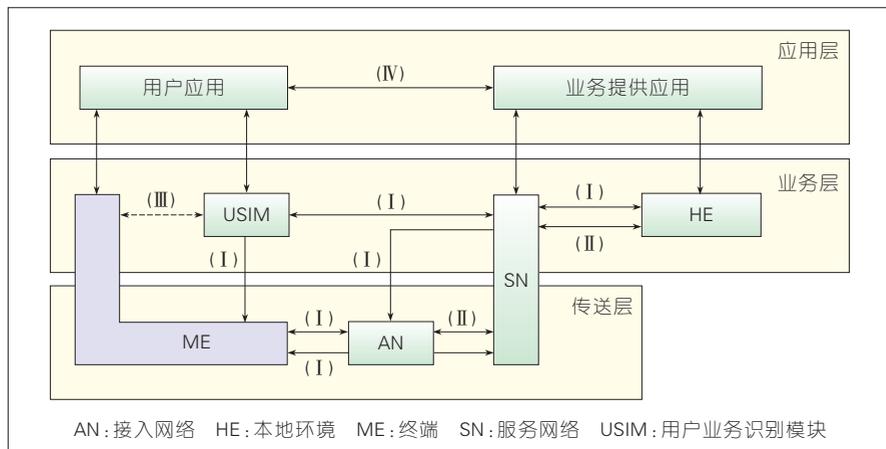


图3 LTE系统安全架构

除了两层安全设计外,LTE系统采用了多个层次的密钥,保证不同层次和不同用途的密钥是相互独立的,在安全机制中使用的密钥是通过推生成成的新密钥,这样做的好处保证了密钥的安全性和新鲜性。

与UMTS系统相同,LTE系统的安全算法是网络 and 用户在安全模式建立过程中通过协商决定的。当安全算法确定后,LTE会对信令进行机密和完整性保护,同时对用户面数据进行机密性保护。目前LTE系统机密性和完整性保护的算法有NULL、SNOW 3G(128位流加密)、AES(128位块加密)、ZUC(128位流加密)4种。其中ZUC算法^[7-9]是中国提出的用于移动通信系统的安全算法并于2011年9月被3GPP正式接纳为LTE的安全算法。

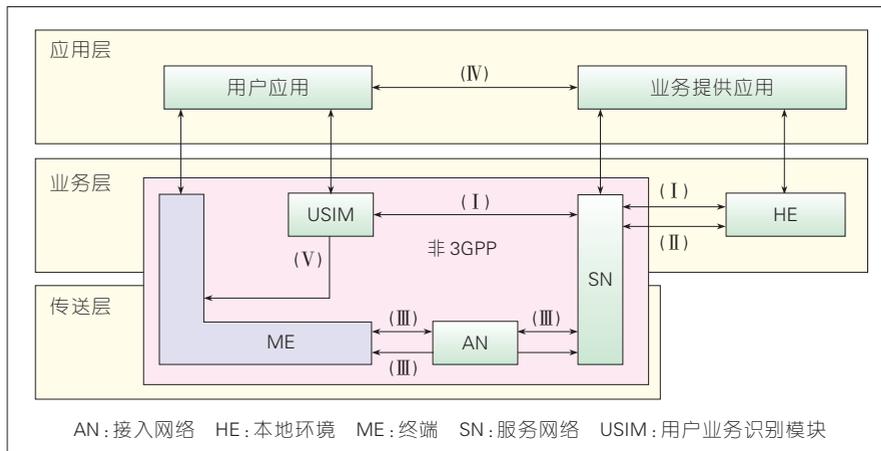
同时在LTE系统中考虑了非3GPP接入技术的融合问题,因此在

LTE系统也考虑了与非3GPP系统融合的安全架构^[10-11],如图4所示。

与3G系统和LTE系统的安全架构相比,非3GPP(如Wi-Fi等)接入LTE网络的安全架构主要改进是增加了非3GPP域安全。当所有的安全特征被运营商认为足够安全,该非3GPP接入被认为是可信的非3GPP接入。当一个或多个安全特征被运营商认为不够安全时,该非3GPP接入将被认为是一个不可信的非3GPP接入。

与UMTS相比,LTE系统对安全做了进一步增强,大大加强了其网络安全。在安全架构方面,LTE在沿用UMTS系统安全架构基础上,增加了接入网与核心网、终端与核心网之间的安全保护;在安全层次方面,LTE增加了终端和核心网之间的安全保护;LTE系统具有更复杂的密钥体系,保证了密钥的安全性;LTE系统增加了终端对网络的鉴权,鉴权向量变为5元组向量,提升了密钥的重要性,避免了SQN序列号重同步缺陷等;中国ZUC算法已经成为了LTE安全算法,同时也提高了LTE系统的安全性能。

另外LTE系统引入了很多新的业务和新的特性,如家庭基站(HeNB)^[12]、机器通信^[13]等新特性,为此LTE系统针对这些新特性对安全进行了扩展和增强,使其具备更高的



▲图4 非3GPP接入LTE网络的安全架构

安全保护。

3 未来移动通信网络安全发展趋势

随着智能终端的快速普及以及网络流量的增长,移动通信技术的演进需求也更加明确及迫切。一方面传统的无线通信性能指标如网络容量、频谱效率等需要持续提升,以进一步提高有限且日益紧张的无线频谱利用率;另一方面更丰富的通信模式以及由此带来的用户体验的提升也是移动通信发展的方向。

未来移动通信网络架构的发展趋势是网络IT化、功能软件化、硬件通用化,解决目前软硬件垂直一体化的封闭体系架构和烟囱群式的网络和业务模式,形成开放的、弹性的网络,实现跨网、跨层、跨域、跨技术、跨厂家全局视野,从而达到资源的最佳利用。未来的移动通信网络将是融合了不同的接入技术、不同网络类型的开放的、弹性的、可编程框架,实现软硬件解耦、全网集中控制、开放可编程。

在未来移动通信网络架构下,业务安全系统能够从网络中获取更加丰富的信息,甚至可以直接采取安全操作如对网络流量进行镜像、阻断和过滤等,可以增强网络安全。但是新的功能实体、协议、接口将成为新的攻击面,传统安全威胁的形式也会发

生改变,如业务可能直接通过与核心网的接口^[14]对网络资源进行非法操作。另外作为网络集中化控制的控制器是网络的核心,其可靠性和安全性非常重要,存在着负载过大、单点失效、易受网络攻击等问题。如果控制器被攻击,那么控制器覆盖的网络将会瘫痪^[15]。

同时未来的移动通信系统将是多种无线通信技术及异构网络共存和融合的网络,使得异构融合的无线网络通信系统的安全接入问题变得更加复杂和重要。目前的多少安全机制不能够完全适用于异构融合的移动通信网络。同时由于新业务带来的新的安全需求也使异构网络面临一系列新的安全问题。

4 结束语

随着网络架构的演进,新业务的出现、新通信协议的引入及用户新安全需求的涌现,移动通信网络将面临更多的安全威胁和安全风险。当前各种移动互联网应用层出不穷,在移动互联网发展过程中移动安全问题越来越多,已经引起用户越来越多的关注,移动互联网的安全威胁要远远大于传统的互联网。移动网络接入安全、移动系统安全和移动应用安全等方面面临着巨大的挑战。本文详细分析了移动通信系统的安全架构、安全机制及存在的安全问题,为移动

通信网络安全的研究和产业发展做出贡献。

参考文献

- [1] 谢进柳. 3GPP安全架构演进探讨[J]. 保密科学技术, 2012, 12(7): 24-29
- [2] 3GPP TS 33.120. Security principles and objectives [S]. 2010
- [3] 3GPP TS 33.102. 3G Security: Security architecture [S]. 2010
- [4] 陈自力, 林德敬, 林柏钢. 第二、三代移动通信系统安全体系的分析与比较[J]. 通信技术, 2003, 22(6): 97-100
- [5] 张长青. TD-LTE系统安全机制分析[J]. 电信网技术, 2014, 32(1): 35-38
- [6] 3GPP TS 33.401. 3GPP System Architecture Evolution (SAE): Security architecture [S]. 2012
- [7] 3GPP TS 35.221. Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications [S]. 2014
- [8] 3GPP TS 35.222. Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification [S]. 2014
- [9] 3GPP TS 35.223. Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data [S]. 2014
- [10] 3GPP TS 33.402. 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses [S]. 2012
- [11] 林东岱, 田有亮, 田呈亮. 移动安全技术研究综述[J]. 保密科学技术, 2014, 18(3): 4-25
- [12] 3GPP TS 33.320. Security of Home Node B (HNB) / Home evolved Node B (HeNB) [S]. 2012
- [13] 3GPP TS 33.187. Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements [S]. 2012
- [14] 周苏静. 浅析SDN安全需求和实现[J]. 电信科学, 2013, 29(9): 113-116
- [15] 王淑玲, 李济汉, 张云勇, 房秉毅. SDN架构及安全性研究[J]. 电信科学, 2013, 29(3): 117-122

作者简介



徐晖,大唐电信科技产业集团无线移动创新中心教授级高工;主要研究领域为移动通信核心网、物联网及安全方向;已主持和参加基金项目10余项,获得中国通信标准化协会科学技术奖3项。



孙韶辉,大唐电信科技产业集团无线移动创新中心总工,北京航空航天大学兼职博士生导师,北京理工大学兼职教授;长期从事无线移动通信关键技术研究 and LTE标准制订工作;已主持和参与基金项目10余项,发表学术论文近50篇。

移动终端高安全可信计算平台架构

A High Security and Trusted Computing Platform Architecture for Mobile Terminal

刘建伟/LIU Jianwei¹
程东旭/CHENG Dongxu¹
李妍/LI Yan²

(1. 北京航空航天大学, 北京 100191;
2. 中国航天科技集团公司卫星应用
研究院, 北京 100086)

(1. Beihang University, Beijing 100191,
China;

2. China Aerospace Science and
Technology Corporation Satellite Application
Research Institute, Beijing 100086, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0011-005

摘要: 针对移动终端日益增长的高安全等级业务需求, 提出一种基于可信平台模块(TPM)芯片的面向移动终端的高安全、高可信计算平台架构。基于当前多种移动终端可信功能拓展架构, 提出了TPM芯片在移动终端可信链路中发挥核心作用的软硬件集成方案; 进一步设计了集成TPM芯片的原型平台, 对移动终端的高安全可信属性进行原理验证, 并对此可信计算平台进行了要点分析。

关键词: 可信计算; 集成式可信平台模块; 移动终端

Abstract: Aiming at the increasing growth of high security level business requirements for mobile terminal, a high security, trusted computing platform architecture for mobile terminal based on trusted platform module (TPM) trusted chip is proposed. Based on the analysis of expanded architecture for trusted function of a wide variety of current mobile terminals, a software and hardware integration scheme is given. In this scheme, the TPM chip plays a key role in the trusted link of mobile terminal. Furthermore, a prototype platform integrated TPM chip has been designed and used for principle verification of highly secure and trusted attribute of mobile terminal. A key point analysis has been done for this trusted computing platform.

Key words: trusted computing; integrated trusted platform module; mobile terminal

目前, 随着移动终端互联的发展, 各种无线移动数据业务持续增长, 尤其是智能手机、平板电脑、PDA等手持设备成为了个人信息终端, 一类高安全等级业务如手机支付、电子转账汇款、移动电子商务、移动电子政务等方兴未艾。但是, 病毒、木马、黑客攻击等各种安全威胁层出不穷, 对移动终端面向高安全等级的应用带来了严重威胁^[1]。在信息安全领域, 可信计算组(TCG)提出了一整套可信计算概念^[2-3], 要求可信平台中集成可信平台模块(TPM)芯片, 作为整个系统可信度量的根, 再逐级构建可信链路, 将信任关系扩展到整个PC系统。目前, 基于TPM芯片扩展移动终端、嵌入式终端以及计算机网络的可信概念也被提出来^[4-5], 用于解决信息安全领域日益增加的可信计算需求。因此, 基于TPM芯片构建面向身份的可信计算平台架构, 是移动

终端用来安全等级的有效途径。

1 移动终端各种可信增强架构对比

人们为了解决移动终端安全可信问题, 提出了多种可信增强方案, 大多数方案都以软硬件相结合的方式提高系统的安全性

1.1 嵌入式处理器内嵌可信分区架构

方案1为嵌入式处理器内嵌可信分区架构。基于ARM单芯片应用处理器内核的嵌入式处理器在移动终端设备中应用广泛, 为了提升ARM处理器的安全可信性能, ARM公司在某些Cortex系列处理器核中设计了内嵌可信分区的TrustZone架构^[6], 该架构隔离了单芯片系统(SoC)硬件和软

件资源, 构成安全子系统分区和普通存储分区, 为利用TrustZone技术的移动设备提供了一个可信执行环境。

但是, 为了追求最佳性能, ARM处理器核的结构非常复杂, 致使其通常不具备芯片级安全防护能力, 也不具备证书认证、数据加密等安全应用所需密码算法引擎。并且基于TrustZone架构的可信应用难以移植到其他嵌入式处理器环境中, 使得可信应用十分受限。

1.2 便携式TPM架构

方案2为便携式TPM架构。TCG组织制订的可信PC平台规范^[7-9], 要求TPM芯片集成在PC主板上, 通过改造主板BIOS, 构造TPM可信链路, 但是, 集成式TPM可信平台方案初期

收稿日期: 2015-02-28

网络出版时间: 2015-04-28

基金项目: 国家重点基础研究发展(“973”)计划(2012CB315905); 中国航天科技集团公司卫星应用研究院创新基金项目(2014CXJJTX10)

成本高,用户可选余地少。因此, Intel 于 2002 年提出了便携式 TPM 的概念,便携式 TPM 也具有可信根安全存储、各种密钥生成以及数字签名验证等功能,便携式 TPM 最初设想是通过 USB 接口或 PC 卡接口与 PC 连接,构建灵活的可信 PC 平台。因为 PC 平台可信规范不适用于移动终端设备环境,为了解决移动终端安全可信问题,人们将便携式 TPM 方案移植到了移动终端中^[10]。基于便携式 TPM 的移动终端可信架构如图 1 所示。

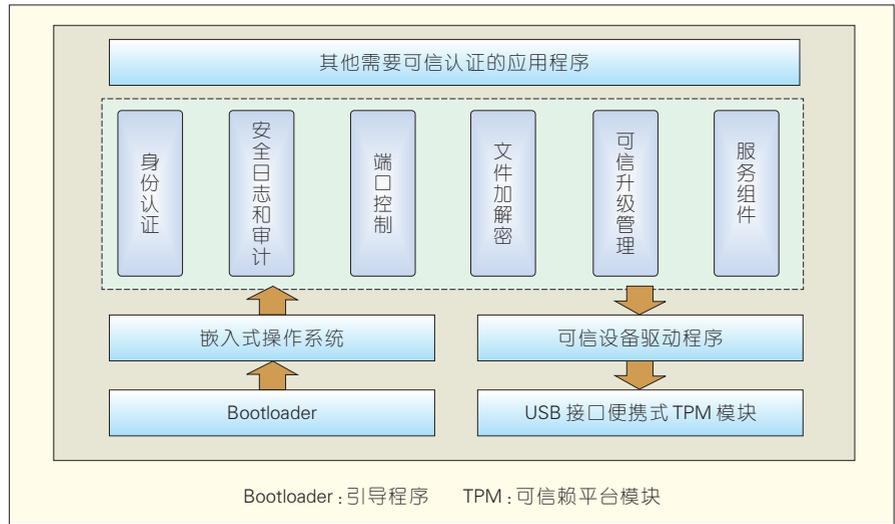
该方案中,移动终端上电后,引导程序(Bootloader)加载嵌入式操作系统代码,系统启动并加载可信升级管理部件,开始调用设备驱动程序访问便携式 TPM 模块,便携式 TPM 与嵌入式操作系统之间需要执行安全认证协议,构建可信计算环境。

由于移动终端启动过程中,嵌入式操作系统需要主动发起可信服务,而便携式 TPM 处于被动调用地位,理论上该方案仅能构建有限安全的可信环境,不适用于需要高安全可信的移动终端应用场景。

1.3 移植 PC 可信 TPM 应用架构

方案 3 为移植 PC 可信 TPM 应用架构。移动终端设备借用 PC 平台可信架构实现可信应用是很自然的推广^[11]。移植 PC 可信 TPM 应用架构如图 2 所示。图 2 给出了 TPM 芯片集成到移动终端电路系统中的原理框图,嵌入式处理器通过低引脚数(LPC)接口、内部集成电路(I2C)或者串行外设接口(SPI)低速总线接口与 TPM 芯片连接,嵌入式处理器与系统其他组件的连接关系保持不变。

此架构需要嵌入式处理器支持 Bootloader 代码通过 LPC、I2C 或 SPI 等低速总线被直接读出,需要改造 Bootloader,使其支持可信度量操作。移动终端上电后,TPM 芯片对 Bootloader 代码进行度量,并将度量值报告给 TPM。随后,TPM 将控制权移交给 Bootloader,由它对嵌入式操作系



▲ 图 1 基于便携式 TPM 的移动终端可信架构

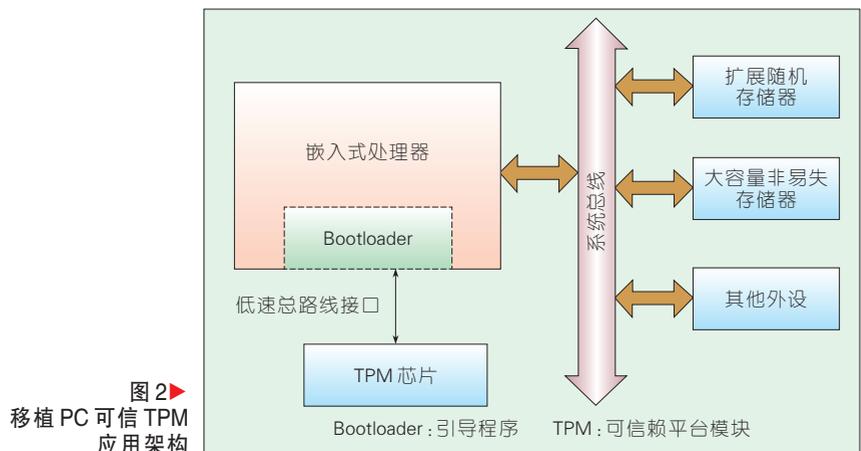


图 2 移植 PC 可信 TPM 应用架构

统代码进行度量并将度量值报告给 TPM。随后,逐级进行可信度量,直到可信链扩展到整个嵌入式系统。

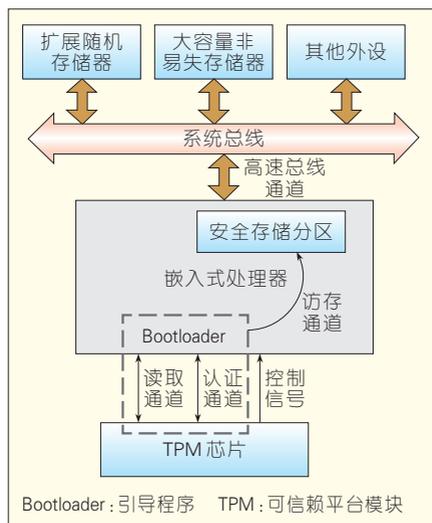
移动终端与 PC 平台相比,安全风险更高。如手机移动终端,丢失风险大;经常升级系统和安全应用程序,甚至更新 Bootloader;手机故障维修时,甚至会被更换手机主板芯片,任意读取手机闪存(Flash)中的敏感数据等。鉴于移动终端安全应用风险更高,本文基于 TPM 芯片提出了更加安全可信的“方案 4”移动终端计算平台架构。

1.4 高安全可信移动终端计算平台架构

方案 4 为高安全可信移动终端计

算平台架构。方案 4 要求 TPM 芯片对移动终端电路系统拥有绝对的控制权,要求进一步增强 Bootloader 的功能,Bootloader 能够对 TPM 芯片进行身份认证。对嵌入式处理器的部分功能和接口提出扩展要求,如要求嵌入式处理器具有安全存储区。与方案 3 相比较,显著提升了移动终端可信计算平台的安全可信性能。

高安全可信移动终端计算平台架构如图 3 所示。移动终端上电后,TPM 获得系统控制权,通过图 3 中控制信号复位嵌入式处理器,通过数据读取通道访问 Bootloader 代码,完成可信度量后,向 TPM 报告度量值。同时,释放对嵌入式处理器的复位操作,Bootloader 获得控制权,通过认证



▲图3 高安全可信移动终端计算平台架构

通道完成对TPM的身份认证。接着,通过高速总线通道读取嵌入式操作系统代码进行可信度量,并将度量值报告给TPM。随后,加载嵌入式操作系统程序,并将控制权移交给它。最后,逐级进行可信度量,直到可信链扩展到整个嵌入式系统。

基于图3架构,本文提出了轻量级的Bootloader认证TPM芯片的安全协议。在移动终端设备生产初装过程中,将配套TPM芯片的存储根密钥(SRK)哈希值写入安全存储区,并且该安全存储区仅Bootloader代码可以访问。针对TPM的身份认证过程非常简洁高效,即TPM通过认证通道将自身的SRK哈希值传给Bootloader,Bootloader从安全存储区读回初装的SRK哈希值,且比对一致后确认TPM芯片身份可信(如未被非法替换)。此外,是能够标识TPM芯片唯一身份数据的哈希值都可以写入安全存储区,作为身份认证过程的比对数据。

2 基于TPM芯片的移动终端高可信度量协议

TPM芯片是一款集成了密码算法引擎,真随机数发生器,能够存放密钥、可信度量值的非易失存储器,具有抵抗各种物理攻击能力的SoC芯片。本文通过在移动终端硬件平

台上集成TPM芯片,以此作为移动终端可信链的源头,构建移动终端高安全可信度量协议,实现整个移动系统软硬件模块逐级可信,为最终的高安全等级应用提供可信的身份、安全的认证证书以及密码学相关应用支持。

图4所示为移动终端在高安全可信计算平台架构下,系统上电后,移动终端启动过程中,可信链的传递过程^[12-13]。首先,在集成TPM芯片的移动终端电路系统设计中,要求TPM芯片先上电,并使它拥有整个电路系统的控制权,具体操作步骤如下:步骤1。由TPM中的可信度量根的核心(CRTM)代码读取Bootloader代码并进行可信度量,将报告传给TPM,TPM将控制权转移给Bootloader(操作a),在执行步骤2之前,Bootloader执行轻量级认证程序,对TPM芯片进行身份认证(操作b),确认TPM芯片未被摘除或非法替换。步骤2。Bootloader执行嵌入式操作系统代码的可信度量,并将度量值报告给TPM,然后加载嵌入式操作系统,并将控制权转移给嵌入式操作系统(操作c)。步骤3。嵌入式操作系统完成可信服务管理程序的可信度量,将度量值报告给TPM,并启动可信服务管理程序(操作d)。可信服务管理程序主要包括调用TPM密码服务的

驱动程序以及可信服务应用编程接口(API)接口程序,并负责度量其他需要可信认证的应用程序。步骤4。可信服务管理程序完成多个需要可信认证应用的度量,并将度量值报告给TPM,TPM芯片内部执行可信软件栈比对可信链路中的所有可信度量值,只有当所有度量值都正确,才认为完成了整个可信链路的逐级传递,使得来源于TPM的可信属性逐级扩展到整个移动终端。

最后,可信服务管理程序驻留系统内存中,执行主动度量功能^[14-15],即对运行中需要可信认证的应用程序进行不定时的可信度量,确保这些程序被木马或病毒修改运行代码后能够被及时发现,并执行补救措施。因为需要访问其他可信应用的程序运行空间,要求嵌入式操作系统赋予可信服务管理程序足够的特权等级。

3 构建FPGA硬件平台进行可信架构原型验证

为了验证和评估高安全可信移动终端计算平台架构的可行性和安全性,基于Altera公司的Stratix IV E系列的EP4SE530H40型现场可编程门阵列(FPGA)搭建了原型验证平台。鉴于此款FPGA集成了超大容量逻辑单元(531200 Logic Elements),我

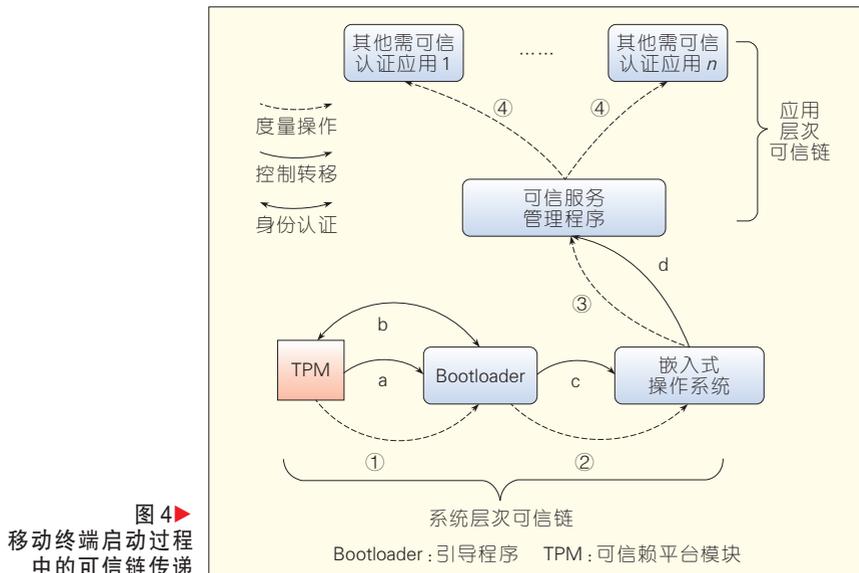


图4 移动终端启动过程中的可信链传递

们将 TPM 模块和移动终端主处理器系统都集成到该款 FPGA 中(嵌入式处理器选用 32 位精简指令集(RISC) CPU——NiosII CPU 软核),如图 5 所示。图中虚线框部分为硬件模拟的 TPM 模块,TPM 模块的随机数发生器(RNG)采用 M 序列伪随机数发生器来代替,非易失存储器采用预先加载初始数据的静态随机存取存储器(SRAM)知识产权(IP)核来代替,不影响仿真验证的真实性。

移动终端主处理器系统中的安全存储区也采用预先加载初始数据的 SRAM IP 核组件,访问控制逻辑确保只有 Bootloader 程序能够访问安全存储区。TPM 模块通过扩展访问接口能够控制移动终端主处理器系统的时钟复位电路,能够读取 Bootloader 代码,能够与总线从设备接口模块互通数据。基于图 5 原型验证平台我们实现了方案 4 的可信移动终端电

路基本功能,验证了基于 TPM 芯片的移动终端高可信度量协议,实现了可信链的逐级传递,并扩展到整个系统。如果进一步采用基于 FPGA 的部分动态重配置技术,能够对整个移动终端主处理器硬件系统进行完全的可信度量^[6]。

4 移动终端高安全可信计算平台要点分析

关于移动终端高安全可信计算平台的设计和应用要注意以下要点。

首先,设计上注意 TPM 芯片在上电初始必须首先运行,必须控制移动终端主嵌入式处理器的运行。

其次,Bootloader 必须对 TPM 芯片进行身份认证,因为 TPM 芯片存在被非法替换的风险。如果移动终端是智能手机,现在专业的维修人员在对手机进行硬件维修时,能够轻易的更换手机主板上的芯片。

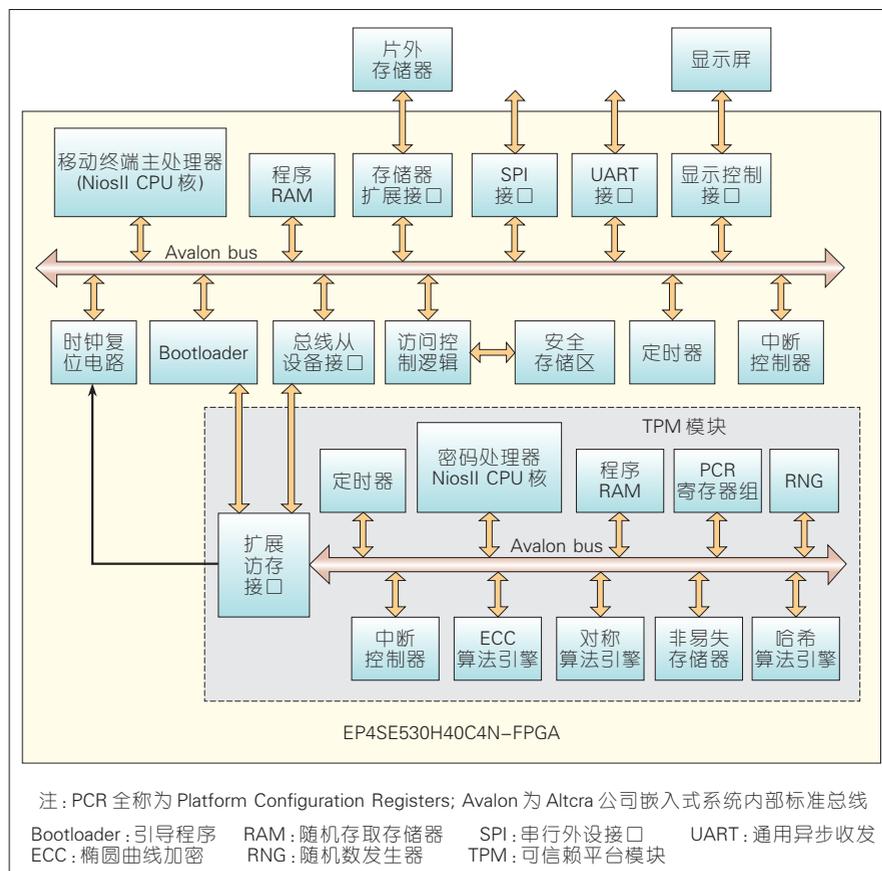
再次,关于高安全可信移动终端计算平台系统升级操作,需要保证安全可信并在用户授权情况下稳妥进行。如果升级 TPM 芯片,需要经过当前 TPM 芯片的授权,再经过 Bootloader 程序认证,才能将新 TPM 芯片的平台唯一标识数据的哈希值写入安全存储区,随后才能进行 TPM 芯片的升级更换操作。如果升级 Bootloader 程序,须经 TPM 授权,将要更新的 Bootloader 的度量值写入 TPM 非易失存储区,再由原 Bootloader 程序将自身加载到主程序 RAM,在主程序 RAM 获得执行后在线更新写入新 Bootloader 代码。再进一步,如果升级嵌入式操作系统代码,只需要经过 TPM 授权,将其度量值写入 TPM 的非易失存储区,再执行升级操作即可。

为了达到尽可能高的安全可信性能,移动终端的嵌入式处理器需要进行适当的可信增强改进,面向移动终端应用的 TPM 芯片也需要小型化和低功耗设计。

最后,虽然移动终端高可信设计初始阶段成本较高,但是,一旦制订并完善了移动终端可信计算平台行业规范,形成可信增强嵌入式处理器接口应用标准,则整个高安全可信移动终端计算平台的成本就会大幅下降。另外,采用移动终端集成 TPM 芯片的可信增强方案,也便于政府相关部门通过 TPM 芯片对可信安全业务进行监管。同时,政府相关部门作为可信的第三方,也便于安全可信认证协议的实施。

5 结束语

本文在分析多种移动终端可信增强架构的基础上,提出并验证了移动终端高安全可信计算平台架构的软硬件系统设计可行性,并给出了基于该架构的可信链传递协议,确保基于该架构具有足够高的安全可信软硬件基础,在此基础上构建的可信应用能够很好满足一类高安全等级业务需求。该架构在具有多处理器核



▲图 5 基于 FPGA 验证高可信移动终端架构

的移动终端设备上的适用性需要进一步的研究和完善,其上的主动度量技术也是下一阶段重点研究方向。

参考文献

- [1] 梁克非. 对智能移动终端进行信息安全等级保护可行性初探 [C]. 第二届全国信息安全等级保护技术大会, 2013-06-21, 中国, 安徽, 合肥. 2013:135-137
- [2] TCG Specification Architecture Overview [S]. Specification Revision 1.4, 2007
- [3] TPM 2.0 Mobile Reference Architecture [S]. Level 00 Revision 142, 2014
- [4] KIM M, JU H, KIM Y, PARK J, PARK Y. Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing [J]. IEEE Transactions on Consumer Electronics, 2010, 56(1):1254-1269
- [5] LI M, LIU J, HAN L. A USB Flash Disk-Based Model of Mobile TPM with Mass Storage [C]//Proceedings of the Management and Service Science, 2009. MASS '09. International Conference. Sept. 20-22, 2009, Wuhan, China: IEEE, 2009: 1-3
- [6] ARM. TrustZone Website [DB/OL]. [2015-01-31]. <http://www.arm.com/zh/products/processors/technologies/trustzone/index.php>
- [7] TPM Main Part 1 Design Principles [S]. Specification Version 1.2, Revision 116, 2011
- [8] TPM Main Part 2 TPM Structures [S]. Specification version 1.2, Level 2 Revision 116, 2011
- [9] TCG PC Client Specific TPM Interface

- Specification (TIS) [S]. Specification Version 1.3, 2013
- [10] 管骁翔, 高宏, 刘文煌. 基于便携式TPM的可信计算研究 [J]. 计算机工程与应用, 2006, 42(36):70-71
- [11] 刘海雷, 王震宇, 马鸣锦, 刘鑫杰. 嵌入式可信终端TPM接口的研究与实现 [J]. 计算机工程与设计, 2008, 29(13):3316-3318
- [12] TANG K, XU X, GUO C. The Secure Boot of Embedded System Based on Mobile Trusted Module [C]//Proceedings of the Second International Conference on Intelligent System Design and Engineering Application. Jan.6-7, 2012, Sanya, Hainan, China: IEEE, 2012: 1331-1334
- [13] LI J, ZHANG H G, ZHAO B. Research of reliable trusted boot in embedded systems [C]//Proceedings of the 2011 International Conference on Computer Science and Network Technology. Dec. 24-26, 2011, Harbin, China: IEEE, 2011: 2033-2037
- [14] LIU C, FAN M, FENG Y, WANG G. Dynamic Integrity Measurement Model Based on Trusted Computing [C]//Proceedings of the 2008 International Conference on Computational Intelligence and Security, Vol 1. Dec. 13-17, 2008, Suzhou, China: IEEE, 2008: 281-284
- [15] 邓锐, 陈左宁. 基于策略嵌入和可信计算的完整性主动动态度量架构 [J]. 计算机应用研究, 2013, 30(11):261-264
- [16] GLAS B, KLIMM A, MULLER-GLASER K, BECKER J. Configuration Measurement for FPGA-based Trusted Platforms [C]//Proceedings of the 2009 IEEE/IFIP International Symposium on Rapid System

Prototyping. June 23-26, 2009, Paris, France: IEEE, 2009:123-129

作者简介



刘建伟, 北京航空航天大学电子信息工程学院党委书记、教授、博士生导师, 中国密码学会理事, 中国电子学会高级会员; 研究方向为无线网络、密码学、信息安全、通信网络安全、信道编码与调制技术等; 已发表论文 100 余篇, 出版专著和教材 5 部、译著 1 部。



程东旭, 北京航空航天大学电子信息工程学院在读博士研究生; 主要研究方向为网络安全和可信计算。



李妍, 中国航天科技集团公司卫星应用研究院工程师; 研究方向为卫星通信网络、通信协议分析。

←上接第 6 页

访问云服务的网络通信安全,需要在移动互联网普及应用 HTTPS、VPN、IPSec 等安全协议,减少通信过程中信息泄露,加强对中间人攻击等网络攻击的抵御能力。

4.3 强化云端的安全防护与安全管理

通过移动互联网对云端进行攻击日益频繁,需要加强云端安全设施及防护能力。强化安全管理,确保信息加密、信息隔离,防止隐私泄露和信息滥用。加强云端安全防护能力,采用专业的云漏洞扫描技术发现漏洞或弱点,及时修补,应用新一代的入侵检测防护系统,智能区分正常流量与异常流量,加强抵御 DDoS、SQL 注入、撞库等攻击的能力。移动互联网也对云服务的可用性提出了更高要求,需要加强云端技术水平和维护水平,提升云端架构的灵活性和资源配置与利用能力,保证服务能力和资源消耗的平衡。制订并实施合理的

云服务等级协议,提高云服务质量。

5 结束语

IT 资源集中化和服务化是大势所趋,云计算必然在未来更为普及,移动互联网同样如此,会成为获取云服务的主要管道。云计算环境下移动互联网的安全问题也会不断暴露、发展、翻新。如何保障云计算环境下移动互联网安全,将成为学术界和业界共同关注的重大领域。

参考文献

- [1] SHIAU W L, HSIAO C M. A Unified Framework of the Cloud Computing Service Model [J]. Journal of Electronic Science and Technology, 2013, 11(2):40-50
- [2] FAN X P, CAO J N, MAO H X. A Survey of Mobile Cloud Computing [J]. ZTE Communications, 2011, 9(1):4-8
- [3] KEVIN Y. Cloud Computing: Concept, Model, and Key Technologies [J]. ZTE Communications, 2010, 8(4):21-26
- [4] 何永江. 基于云计算的移动互联网服务提供模式 [J]. 邮电设计技术, 2011, 28(10):39-42
- [5] 柏秋云. 大数据的价值与挑战 [J]. 科技信息, 2013, 35(17):479
- [6] LIU Y, WU J P, ZHANG Z, XU K. Research achievements on the new generation Internet architecture and protocols [J]. Science China,

2013, 56(11):1-25

- [7] 刘辛越. 云计算、云计算与密码安全体系 [J]. 信息安全与通信保密, 2012, 17(11):25-26
- [8] 黄伟. 新技术新业务发展提出新要求 网络建设与技术引入需持续推进 [J]. 世界电信, 2012, 25(12):54-58
- [9] 房秉毅, 张云勇, 徐雷. 移动互联网环境下云计算安全浅析 [J]. 移动通信, 2011, 35(9):25-28
- [10] LUO S M, WANG Z K, WANG Z P. Big-Data Analytics: Challenges, Key Technologies and Prospects [J]. ZTE Communications, 2013, 11(2):15-21

作者简介



刘权, 工业和信息化部赛迪智库信息安全研究所研究员、所长; 主要从事信息安全和信息安全战略、规划、政策等方面研究工作; 已发表学术论文 100 余篇。



王涛, 工业和信息化部赛迪智库信息安全研究所高级工程师; 主要从事信息安全政策、电子认证产业及技术等咨询和研究工作; 已发表学术论文 10 余篇。

移动互联网服务的隐私保护机制

Privacy Mechanism in Mobile Internet

李晖/ LI Hui¹牛犇/ NIU Ben²李维皓/ LI Weihao¹(1. 西安电子科技大学, 陕西 西安 710071;
2. 中国科学院信息工程研究所, 北京 100093)(1. Xidian University, Xi'an 710071, China;
2. Institute of Information Engineering,
Chinese Academy of Sciences, Beijing
100093, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0016-007

摘要: 探讨了考虑背景信息的位置和查询隐私保护方案, 如基于背景信息的虚拟位置 k -匿名方案、同时保护位置和兴趣的隐私保护方案、基于交互的隐私保护方案, 还探讨了基于用户隐私链拆分的实名认证和身份隐私保护策略; 认为在避免可信第三方参与, 敌手能够获取到背景信息的前提下, 能够实现对用户身份、位置和查询隐私的保护, 达到信任机制和隐私保护的有机结合将是未来隐私保护发展的趋势。

关键词: 移动互联网; 身份隐私; 位置隐私; 查询隐私

Abstract: In this paper, we discuss the location and query privacy mechanism which considering the background information, such as the k -anonymity based on background information, the privacy mechanism that preserves the location and interest and privacy preservation mechanism based on interaction. The real-name authentication based on user privacy chain separation and identity privacy mechanism are also discussed. In order to avoid the trusted party, and the background information can be obtained by an adversary, it will be the tendency that the user's identity, location and query can be kept private, and trust mechanism and privacy protection can be combined.

Keywords: mobile internet service; identity privacy; location privacy; query privacy

1 移动互联网面临隐私保护威胁

移动互联网服务的广泛普及、大数据技术的普遍应用在为人们带来便利的同时, 也对用户隐私保护带来了巨大的挑战。众多的移动互联网服务大量采用用户名-口令认证机制, 为记忆方便, 用户普遍对不同的应用采用相同的用户名和口令, 使得一旦某个服务商数据库泄露就威胁到用户在其他服务商的信息。国家对移动互联网信息传播实名管控的需求与用户身份隐私形成矛盾, 如何提高用户身份认证的安全等级, 免除用户记忆口令的负担, 兼顾实名管控和用户身份隐私的保护成为移动互联网用户身份管理的主要挑战。

另一方面, 微信、大众点评、百度地图等移动服务要求用户的位置信息和兴趣信息, 不可信的服务对这些

信息的滥用或者泄露对于用户权益带来极大的损害, 在享受移动互联网服务方便性的同时, 保护用户的身份、位置和兴趣的隐私成为移动互联网领域亟待解决的问题。

2 移动互联网位置和查询隐私保护的主要方法

基于位置服务中常见的安全及隐私威胁主要包括 5 种攻击方式: 单点攻击、基于上下文的攻击、多点攻击、多点配合上下文攻击以及直接攻击可信第三方。一般而言, 这几种攻击方式要求攻击者的能力依次增强, 要求攻击者能够获取越来越多的用户信息, 从而更高概率地获取用户隐私信息。

对于攻击者而言, 他们可以通过多种途径获取多种额外的信息, 例如, 用户密度信息, 请求发送的概率分布, 地图上兴趣点的分布情况等, 这些可以统称为背景信息, 此类信息一般为公开信息, 可以通过互联网轻易获取, 亦可通过攻击相关的可信第三方来获取。例如, Google Maps 的服务器上保存着历史用户的各种查询记录, 分布情况等重要信息, 一旦该服务器被攻击, 用户的所有信息将暴露于攻击者眼前。

各种基于位置服务中的服务提供商本身其实就是潜在的攻击者或者隐私信息的泄露者。层出不穷的泄密事件说明传统上认为是可信的服务提供商完全有可能被来自内部

收稿日期: 2015-02-28

网络出版时间: 2015-04-28

基金项目: 国家自然科学基金项目 (61170251, 61272457); 国家高技术研究发展 (“863”) 计划 (2012AA013102, 2012AA01A401); 数字版权保护技术研发工程项目 (1681300000119)

或者外部的攻击者攻陷,从而导致用户隐私信息的泄漏,因此,如何在服务提供商不可信的前提下保证用户隐私信息不被泄露就成为了一个很严峻的问题。

针对上述问题,来自全球工业界和学术界的科研人员已经提出了许多解决方案,这些方案可以根据不同标准分为不同的类别,以下介绍两种常见的分类方法:

(1)第一种分类主要根据用户对隐私信息的类型进行分类,可分为位置隐私、查询隐私。

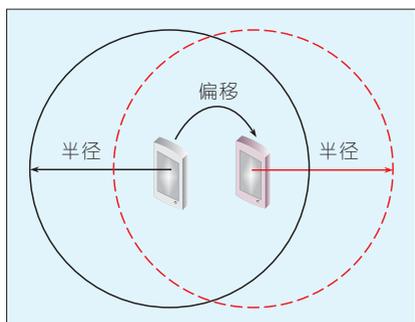
其中位置隐私用以保护用户当前以及历史位置信息,使得攻击者难以获取用户位置相关的信息,从而难以实现对用户的追踪等。

查询隐私旨在保护用户所查询的内容,从而不泄露用户的个人喜好等信息。然而,用户的位置与所查询的内容并不完全独立,甚至在大多数情况下两者存在一定的关系,从而使得单纯保护某一种隐私的方案难以真正保护用户的隐私,故而也需要同时保护用户的位置隐私和查询隐私。

(2)第二种分类主要是为了实现不同场景下的隐私保护问题,现将当前主流的隐私保护方案分为5类:位置偏移、混淆技术、时间和空间隐匿、添加虚假信息以及其他方案。

(a)位置偏移

位置偏移示意如图1所示。黑色手机为真实用户,其请求服务半径为1英里,当他需要发送基于位置服务的服务请求时,用偏移后的位置取代其真实位置,然后构建新的服务请求



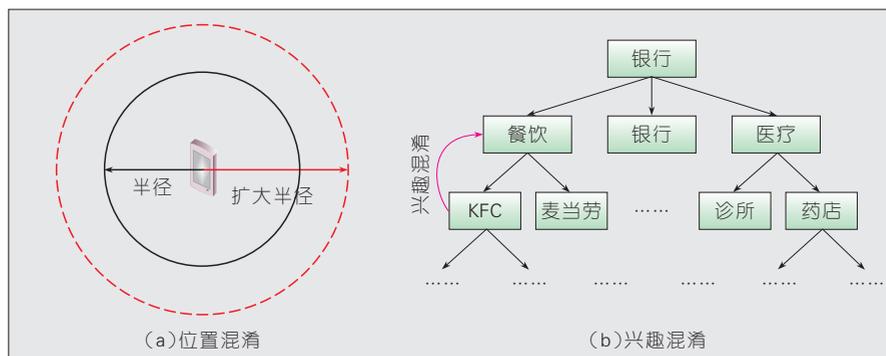
▲图1 位置偏移示意

信息并发送给服务运营商,从而达到保护其位置隐私的目的。此种方法算法复杂度很低,很容易在智能终端上实现,而且系统开销,尤其是通信开销基本上没有增加。然而由于所请求的服务数据和真实需要的服务数据之间存在一定的偏差,从而导致服务质量的降低。而且在此类方案中,服务质量的优劣和隐私保护效果的好坏成为了一对矛盾,服务质量越高,隐私效果越差,反之亦然。

(b)混淆

适用于位置隐私的保护和查询隐私的保护。对于位置混淆,用户可以通过对其查询半径进行模糊,例如,增大其查询半径或者刻意缩小其查询半径,甚至结合偏移的方案,通过位置偏移+查询半径变化的方案,使得攻击者更难推断其真实信息,如图2(a)所示;对于查询隐私混淆,将用户的兴趣集合进行划分,如图2(b)所示,当用户真实的查询请求为KFC的时候,为了对其查询信息进行混淆,可以用更大的一个集合“餐饮”代替,从而将自己的真实请求信息混淆于更大的集合之中,达到保护查询请求的目的。

此类解决方案的优点在于易于实现,由于只需要对相关参数进行修改,例如增大查询半径,所以很容易完成隐私保护。由于对查询半径的调整以及查询内容的混淆,会导致额外的系统开销,例如,用户需要获取一些不必要的服务信息,这样的操作也会引起服务质量的下降。



▲图2 基于混淆的隐私保护

(c)时空隐匿

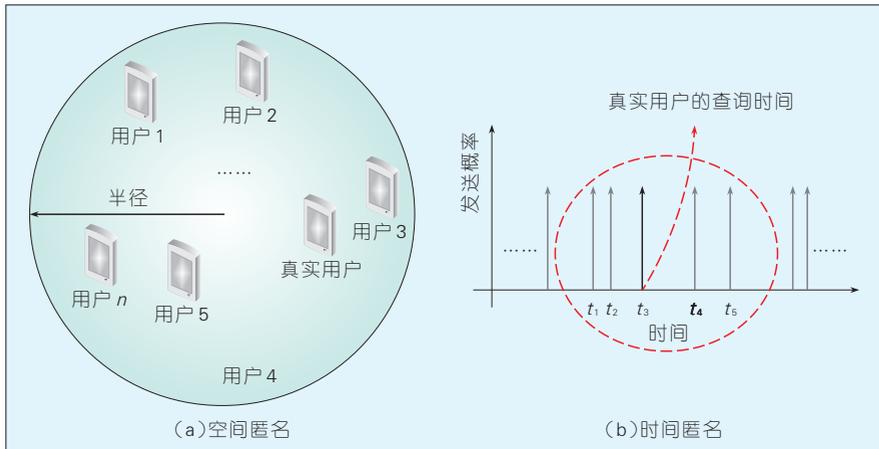
其核心思想在于收集/等候足够多的用户信息,通过统一提交请求,达到保护各个用户隐私信息的目的。真实用户将其请求发送至一个可信的第三方,该第三方同时收集周围其他用户的多个请求,如图3(a)收集多个用户的请求,然后将多个请求进行合并,一起发送给服务提供商,从而使得提供商难以获取各个用户的隐私信息。在图3(b)中,假设用户的真实请求发送于时间点 t_1 ,可信第三方出于时间隐匿的目的,等候一段时间以收集更多的请求信息。此处收集的信息可能来自多个用户,也可能来自该用户的多条请求信息,然后将多个请求一并发送给服务提供商,达到隐匿真实请求的目的。

一般情况下,此类方案可以达到较高的隐私保护级别,但具有较大的系统开销,以及较长的等待时延,最重要的问题在于对于可信第三方的依赖。

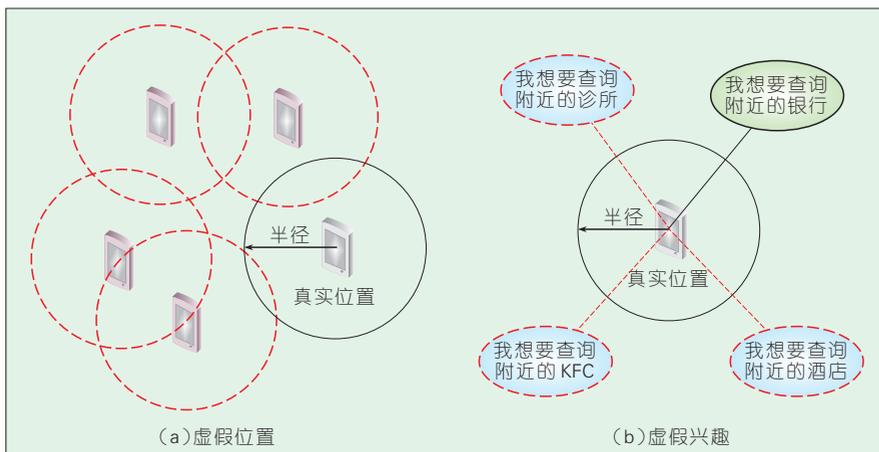
(d)虚假信息

包括基于虚假位置的位置隐私保护和基于虚假请求信息的查询隐私保护。其核心思想在于通过构造虚假的位置或者虚假的请求从而有效的实现 k -匿名或者 l -多样性的隐私保护级别。

如图4(a)所示,为了保护用户的真实位置,通过合理构造出若干个虚假的位置(例如 $k-1$ 个),最终将这个 k 个位置构成的集合一并发送给服务提供商,其隐私保护的效果取决于攻



▲图3 时空隐匿的隐私保护



▲图4 虚假位置和兴趣的隐私保护

击者是否能够有效从 k 个位置中区分出哪个是用户的真实位置。

类似的,图4(b)中给出了基于虚假查询请求的查询隐私保护策略,用户在向服务提供商发送请求之前,先构造若干个虚假的请求,一并发送给服务提供商,从而实现隐私保护。

在此类方案中,是否能够有效的构造虚假信息成为了隐私保护是否有效的关键,尤其是在面对拥有各种各样的背景信息的攻击者的时候,虚假信息可能会被有效过滤,从而难以达到用户期望的隐私保护效果。

基于虚假信息的隐私保护方案比较容易实现,也能够提供较高级别的隐私保护。由于需要引入额外的虚假信息,而额外的虚假位置或者虚假查询请求会带来相应的服务数据,

所以随着虚假信息数目的增加,系统的性能会大幅度的降低。另外大多此类方案都没能同时保护用户的位置隐私和查询隐私,这也会使得整个系统的隐私保护效果会由于攻击者所拥有背景信息的数量增加而下降。

(e) 其他

位置服务中还有其他相关的一些隐私保护方案,主要包括基于密码学工具的方案。通过对用户所上传的信息进行相关处理,例如加密等方法,借助于私人信息检索(PIR)等技术,从而使得用户在能够享受服务数据的同时又不将自己的查询请求泄露给服务提供商。当然,此类系统也可能借助于第三方的匿名服务器等,从而更程度的保护用户隐私信息。

此类方案一般能够较程度的

为用户提供隐私保护效果。然而,由于匿名服务器(可信第三方的一种)的存在,使得整个系统难以承受单点失效攻击。此外,一些复杂的密码学运算仍然难以高效的应用在其上,这样会导致额外的计算负担,降低系统的可用性。

从移动用户的身份信息、位置信息以及兴趣信息三方面对隐私保护问题进行总结,分析了现有科研成果所采用的主流技术及相应的优、缺点,在此基础上进行了分类。现有移动互联网中隐私保护方案分类如表1所示。

从表1提及的现有方案中可以看到,当前解决方案大都基于可信第三方,用户的身份认证一般由可信第三方或者服务提供商进行认证。CliqueCloak^[1]和 Casper^[2]利用可信第三方实现匿名区域大小可调的 k -anonymity。Footprint k -anonymity^[3]利用移动用户的历史信息,通过在相遇用户之间构成一个虚拟的 Mix-Zone 来完成对用户兴趣信息和身份信息的混淆,从而实现 k -anonymity。CacheCloak^[4]引入了缓存和预测的概念,通过缓存的用户历史轨迹等信息,预测用户下一步的移动,为用户提供实时的服务。但是当用户身处全新环境时,该方案的预测准确性会大幅降低。Xu 和 Cai^[5]提出了 Feeling-based pyramid 解决方案,该方案将地图进行划分,并根据用户的感兴趣程度赋予不同的权重,通过分析历史信息,用信息熵的概念实现 P -popular trajectory (PPT)。该方案能够有效的保护用户的位置信息和兴趣信息,但其具有较高的计算资源消耗。Pan^[6]等人提出了 ICliqueCloak,虽然该方案可以在连续场景下同时保护用户的位置信息和兴趣信息,但同样的运算复杂度较高。

与此同时,有一些隐私保护技术并不依赖于第三方机构的技术(TTP),其基本思想主要集中于用户和其他用户之间交互信息,通过对等

▼表 1 现有移动互联网中隐私保护方案

方法	文献出处	可信第三方	k -anonymity	混淆	移动设备	身份泄漏	位置泄漏	兴趣泄漏	连续场景
CliqueCloak	TMC'06	Y	Y	Y	N	N	N	Y	N
Casper	VLDB'08	Y	Y	N	N	N	N	Y	N
P2Pcloaking	GIS'06	N	Y	N	Y	N	N	Y	Y
Footprint k -anonymity	Infocom'08	Y	Y	N	N	Y	N	Y	N
CacheCloak	Mobicom'09	Y	N	Y	Y	Y	Y	Y	N
Feeling-based pyramid	CCS'09	Y	N	Y	N	N	N	N	N
CAP	ICDCS'09	N	N	Y	Y	N	N	Y	N
Dummy-Q	Infocom'11	N	N	Y	Y	N	N	Y	Y
ICliqueCloak	TKDE'12	Y	Y	N	N	N	Y	Y	Y
MobiCrowd	Mass'11	N	N	Y	Y	Y	Y	N	N
EPS	Globecom'13	N	Y	Y	Y	Y	N	N	N
DLS	Infocom'14	N	Y	N	Y	N	N	Y	N

网络(P2P)或者基于相遇的解决方案实现匿名集的构造,从而保护用户隐私。Chow^[7]等人提出了一种基于P2P的解决方案,通过用户的相互协作,用近距离通信标准(Wi-Fi或蓝牙技术)实现用户之间的信息交换,在考虑用户的最大移动距离基础上,实现连续场景下的 k -anonymity,以保护用户的位置隐私。然而由于用户的移动模式和近距离通信的通信距离限制,使得真实用户的位置会以较大概率落在匿名集的中心区域。另外,用户仍需将自己的真实身份和兴趣信息发送给服务运营商,所以该方案难以同时保护用户的身份信息和兴趣信息。CAP^[8]是一个基于四叉树和不同的网格步长的希尔伯特曲线型(VHC)的P2P解决方案,根据道路密度,CAP用一个大小可调的希尔伯特曲线对地图进行填充,用四叉树的存储结构,在有效实现 k -anonymity的基础上大幅度降低系统的计算和存储开销。Pingley^[9]等人提出了DUMMY-Q方案,通过在本地构建一个兴趣信息池,利用虚假兴趣信息选择算法高效的实现 k -anonymity,从而有效抵御来自主动攻击者的推理攻击。但高额的兴趣信息池维护开销对手机用户而言难以负担。Shokri^[10]等人提出

了一种基于群组的用户隐私保护方案,当前用户通过将所需查询在群组内转发,由某一用户替代其向服务运营商发送服务请求,从而实现当前用户身份信息,位置信息和兴趣信息的保护。但该方案的问题在于代替当前用户进行发送请求的用户没有足够的动力来进行此类操作,加之移动设备的资源受限性,该方案难以在移动互联网中广泛应用。

3 考虑背景信息的位置和查询隐私保护方案

3.1 基于背景信息的虚假位置 k -匿名方案

通过巧妙的设计虚假位置生成算法,在充分考虑攻击者可能拥有的背景信息的基础上有效实现 k -匿名。同时,此方案能够有效的提供较大的隐匿区域,而且可以避免真实用户落在所提交 k 个位置中处于最中间区域的问题。

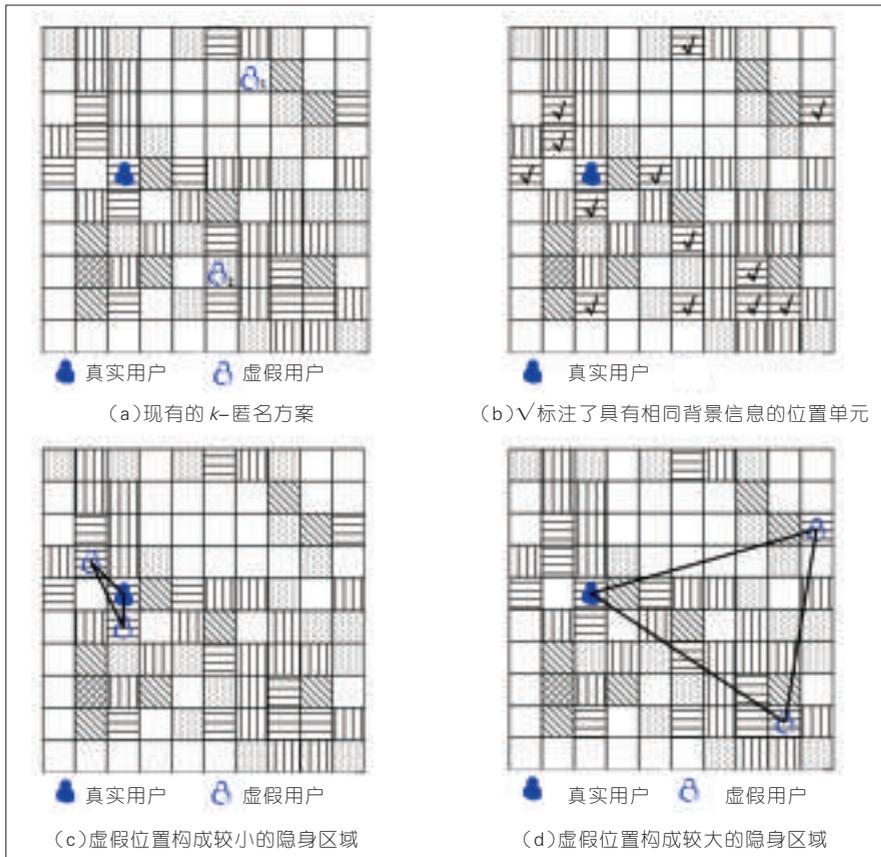
基于背景信息的虚假位置 k -匿名如图所示。将本地地图划分为若干个网格,不同的网格形状框代表了不同的历史请求概率,也就是用户历史上在该网格内发送基于位置服务请求的概率。蓝色小人儿代表真实

用户,空心儿小人儿代表最后参与 k -匿名的虚假用户位置。我们的思路包括两部分,第一部分见图5(a)、图5(b),其主要目的在于通过比对每个网格与当前用户所处网格的历史请求概率,旨在选择出一组潜在的网格去分配虚假用户,从而保证攻击者难以通过此类背景信息对最终提交的 k 个位置进行有效过滤。图5(c)、图5(d)代表了两种极端,在图5(c)中,真实用户与虚假用户相距较近,这样攻击者甚至无需猜测,便能获取真实用户的大体位置,使得真实用户的位置隐私难以有效保证,显然这是不可取的。图5(d)给出了一种相对比较优良的选择结果,即最终参与匿名的几个位置(包括了一个真的和两个假的),两两之间相距足够远,且具备相等或者近似的服务请求概率,从而大大降低攻击者猜测出用户真实位置的概率,大幅度提高用户的位置隐私级别。

我们对所提出方案的有效性和安全性进行了验证,具体细节^[11]可参看,同时对于背景信息的进一步利用可参考^[12]。

3.2 同时保护位置和兴趣的隐私保护方案

同时保护位置和兴趣的隐私保护方案^[13]用于同时保护用户的位置隐私和查询隐私,并提供个性化的隐匿区域大小选择。该方案通过对传统的背景信息进行细分,在选择虚假位置的时候,不但考虑选择 $k-1$ 个查询概率相似的位置,同时兼顾查询隐私的保护,通过合理选择 $l-1$ 个相似的查询内容,来确保位置隐私到达 k -匿名级别的保护,和查询隐私的 l -多样性级别的隐私保护。另外,本方案由于在设计初期就允许用户对隐匿区域的大小进行选择,并通过隐匿区域的随机偏移保证真实用户的位置可能落在该区域内的任何位置,从而有效的避免真实位置位于隐匿区域中心部分的攻击。

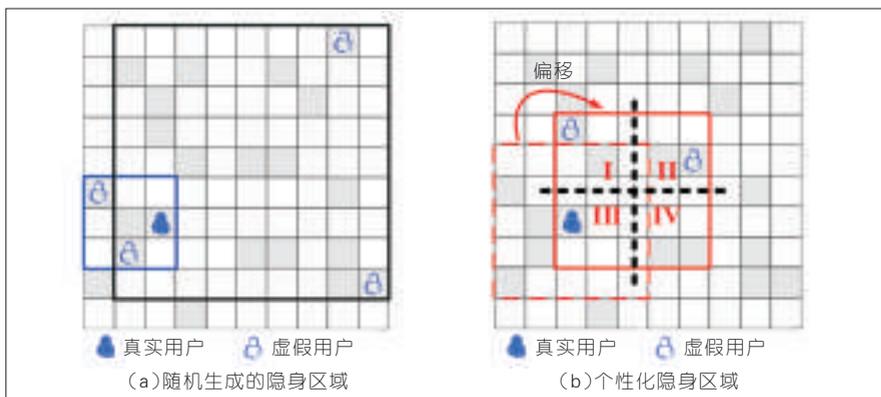


▲图5 基于背景信息的虚假位置 k -匿名

由于隐匿区域的大小往往决定了系统开销的大小,故而本方案首先赋予用户自主的隐匿区域大小调节能力,从而让用户根据自己的需求合理调节该区域的大小,进而调节可以忍受的系统开销。

具体而言,用户设定合适的隐匿区域,如图6(b)中的红色虚线框,故而需要在该隐匿区域内进行虚假位

置分布。然而考虑到上文提到的“用户处于中心区域的攻击”,我们首先对该虚线框进行一个随机偏移,偏移至图中红色实线框处,然后进行相关虚假用户分布工作。在具体分布时,根据需求达到的位置 k -匿名中的参数 k ,首先用四分法对该区域进行划分,如图6(b)所示, $k=3$,故而将该区域划分为4部分,除了真实用户所处

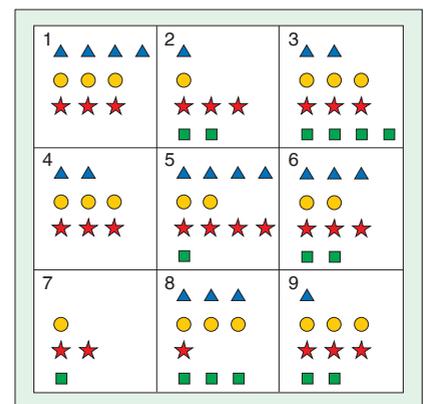


▲图6 区域隐匿示意

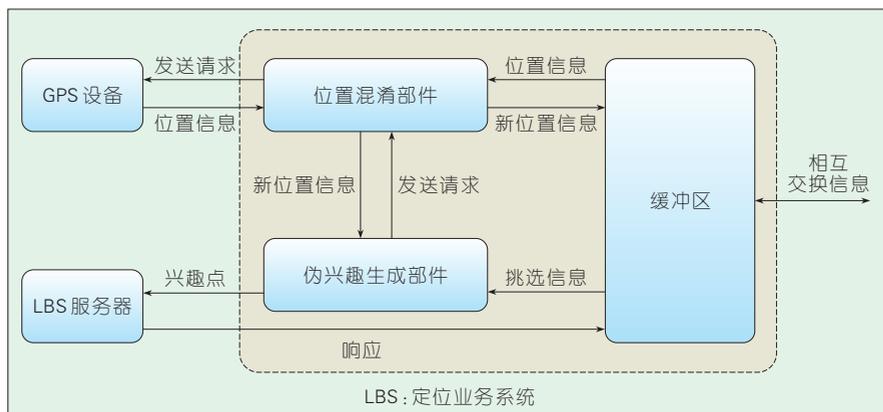
的区域外,随机选取其他3个区域中的2个作为备选,最后开始着手考虑对查询请求内容的 l -多样性需求。具体的方法如图7所示,图中每种颜色的符号代表不同的历史查询请求,例如附近的酒店信息,附近的医院信息等,我们在每个细分后的区域内对各类查询请求进行统计,遵循相似的规律来构造剩下的 $l-1$ 个查询内容,即所选择的 $l-1$ 个请求内容需要与当前用户的真实请求内容的查询概率接近,从而确保 l -多样性的效果。通过以上步骤,最大限度的实现本文所设定的目标。

3.3 基于交互的隐私保护机制

本方案目的在于设计一个通过用户交互来实现信息混淆的隐私信息保护方法,思路相对较简单。每个用户维护一个本地缓冲区,用以随机记录其所处位置和所发送请求,当遇到其他用户时,随机从缓冲区内抽取一条信息进行交换,如此往复,使得每个用户的缓冲区内的信息足够混乱。在真正需要向服务提供商发送请求时,可以从本地缓冲区内随机搭配出若干个组合,结合真实的位置和请求内容一起发送给服务提供商,以达到 k -匿名的保护效果。系统架构如图8所示,智能终端利用位置混淆部件、伪兴趣生成部件以及缓冲区对信息进行处理,将处理后的请求信息发送给定位业务系统(LBS)服务器



▲图7 兴趣分布统计示意(每种颜色的符号代表不同的历史查询请求)



▲图8 基于相遇的位置和查询隐私保护方案

以便获取服务^[14]。

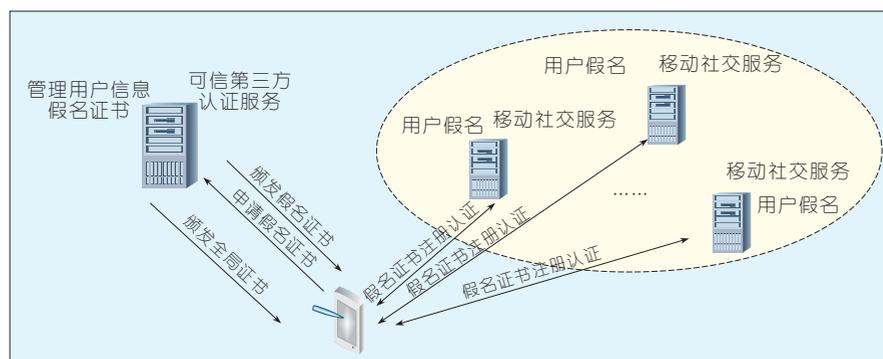
4 基于用户隐私链拆分的实名认证和身份隐私保护策略

Zhu^[5]等人提出通过将用户与证书之间的注册链条打断,并将各部分交由不同的实体进行管理的方案来实现对用户的身份信息的保护,进而实现用户个人信息的安全、有效更新,防止来自用户和服务运营商双方的欺骗和共谋等攻击。主要思想是打断用户查询/发布数据资源时提供的“用户真实身份-用户数据”对应关系,通过引入“假名”(或者多个假名的假名集)的方法实现基于用户隐私链拆分的实名认证和身份隐私保护策略。通过构造相应的“假名集”,将用户隐私链分为“用户真实身份-假名集-用户数据”,可信认证服务器是一个权威的第三方认证服务器,其和各种不同的服务提供商分别管理用户隐私链的一部分。其中,可信认证服务器维护“用户真实身份-假名集”,服务提供商维护“假名集-用户数据”,从而实现实名认证和用户身份隐私的保护。

服务提供商对用户的认证过程可基于移动终端进行。在移动终端上保存假名证书和假名对应的密钥,安装认证模块,该模块可以是应用(APP)程序,也可以是手机用户识别模块(SIM)卡或者手机内部拥有的硬

件安全模块。图9是我们基于SIM卡实现的一种兼顾实名与用户身份隐私的互联网服务认证方案。SIM卡中实现有数字签名模块和认证用户识别应用发展工具(STK)应用,可信认证服务方可使用公安部eID服务,具体步骤如下:

- 用户向可信认证服务器提供真实身份,申请“全局证书”,该证书包含可信认证服务器对用户的真实身份的签名,用作用户向可信用户申请假名证书时认证的凭证。
- 凭借“全局证书”,用户可向可信认证服务器申请多个假名证书,构建假名集合。
- 用户在向不同服务提供商系统注册时,可以使用不同的假名证书证实自己的身份。这样,服务提供商系统维护假名-用户数据。并利用假名证书实现服务提供商系统的登录认证,保证了不同的服务使用不同的假名。



▲图9 用户隐私链拆分保护策略

服务提供商对用户的认证过程如下:

- 用户提交注册或登录请求。
- 服务提供商通过短消息向用户SIM卡发送认证挑战。
- SIM卡上的认证STK应用会截获并处理认证挑战短消息,并通过STK功能将相关注册或交易请求信息显示在手机屏幕上。
- 用户确认信息无误后,认证STK应用对认证挑战进行数字签名生成相应的认证信息,并将此信息发回服务提供商。
- 服务提供商用户假名证书验证签名的正确性。

这一方案服务提供商不存储用户的真实身份信息,而且不同的服务提供商使用不同的假名,支付等关键交易采用数字签名认证,提高了安全级别。如有需要,通过假名证书,可信认证服务可追踪用户真实身份。

5 结束语

本文分析了现有移动互联网位置、兴趣和身份隐私保护方案,介绍了几个基于分布式架构的位置和查询隐私保护机制,并给出了一个兼顾实名和身份隐私保护的实名认证方案,但是这个方案需要可信认证服务提供商。未来在下面几个方面还有许多问题需要解决。

第一,考虑到智能终端的大规模使用,传统的基于可信第三方的方案无论从性能角度还是安全性角度来讲都有比较大的局限性,所以应该尽

可能的避免可信第三方的使用。另外由于智能终端的资源受限性,例如较低的计算能力,有限的存储空间以及相对较弱的通信能力,故而应该尽可能的降低所涉及隐私保护方案的复杂度,并提高已有资源的利用率。

第二,需要充分考虑攻击者可能拥有的各类背景信息。我们的实验结果证明,现有大多方案的隐私保护效果在攻击者拥有背景信息的前提下都会大幅下降,即使少部分方案已经将背景信息考虑进算法设计过程中,然而由于对于背景信息分析的不全面性,导致攻击者仍然能够通过将各类相关背景信息进行融合,如采用数据挖掘等技术,从而增大获取用户隐私信息概率的目的。因此,在未来的研究方向中,需要考虑更加符合用户现实生活的各类背景信息。

第三,目前仍然没有一种行之有效的隐私保护效果衡量方法。由于用户需求的多样性,例如,身份隐私,位置隐私,查询隐私,轨迹隐私,数据隐私等,以及用户在不同应用中对于各类隐私信息的个性化设置等因素,导致对隐私保护效果的衡量工作难以统一的进行,这也使得很难去评价当前已有算法的效果。因此,设计统一的隐私度量方案或者度量平台显得尤为重要。

第四,将信任机制与隐私保护有机结合。如果有足够高的信任,可以降低隐私泄露的风险,提高服务质

量,降低系统开销。如何确立最佳的平衡点和建立大规模用户的信任评估模型和系统还亟待开展研究。

参考文献

- [1] GEDIK B, LIU L. Protecting Location Privacy With Personalized k-Anonymity: Architecture and Algorithms [J]. IEEE Trans. Mobile Computing, 2008, 7(1):1-18
- [2] MOKBEL M F, CHOW C-Y, AREF W G. The New Casper: Query Processing for Location Services Without Compromising Privacy [C]// Proceedings of the VLDB, 2006:763-774
- [3] XU T, CAI Y. Exploring Historical Location Data for Anonymity Preservation in Location-Based Services [C]// Proceedings of the INFOCOM, 2008:547-555
- [4] MEYEROWITZ J, CHOUDHURY R R. Hiding Stars with Fireworks: Location Privacy Through Camouflage [C]// Proceedings of the MobiCom, 2009: 345-356
- [5] XU T, CAI Y. Feeling-Based Location Privacy Protection for Location-Based Services [C]// Proceedings of the CCS, 2009:348-357
- [6] PAN X, XU J, MENG X. Protecting Location Privacy against Location-Dependent Attack in Mobile Services [J]. IEEE Trans. Knowledge and Data Engineering, 2012, 24 (2): 1506-1519
- [7] CHOW C-Y, MOKBEL M F, LIU X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service [C]// Proceedings of the GIS, 2006:171-178
- [8] PINGLEY A. Cap: A context-Aware Privacy Protection System for Location-Based Services [C]// Proceedings of the ICDCS, 2009:49-57
- [9] PINGLEY A. Protection of Query Privacy for Continuous Location Based Services [C]// Proceedings of the INFOCOM, 2011:1710-1718
- [10] SHOKRI R, PAPADIMITRATOS P, THEODORAKOPOULOS G, HUBAUX J P. Collaborative Location Privacy [C]// Proceedings of the IEEE MASS, 2011:500-509
- [11] NIU B, LI Q, ZHU X, CAO G, LI H. Achieving k-anonymity in Privacy-Aware Location-Based Services [C]// Proceedings of the INFOCOM, 2014: 1805-1819
- [12] NIU B, LI Q, ZHU X, CAO G, LI H.

Enhancing Privacy through Caching in Location-Based Services [C]// Proceedings of the INFOCOM, 2015: 1309-1321

- [13] NIU B, ZHU X, LI W, LI H, WANG Q, LU Z. A Personalized Two-Tier Cloaking Scheme for Privacy-Aware Location-Based Services [C]// Proceedings of the ICNC, 2015: 2301-2316
- [14] NIU B, ZHU X, LEI X, ZHANG W, LI H. EPS: Encounter-Based Privacy-Preserving Scheme for Location-Based Services [C]// Proceedings of the GLOBECOM, 2013: 1106-1117
- [15] ZHU Z, CAO G. APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services [C]// Proceedings of the IEEE INFOCOM, 2011: 1889-1897

作者简介



李晖,西安电子科技大学教授;主要研究领域为密码学、无线网络安全、云计算安全、信息理论与编码理论;已主持承担基金项目15项,获发明专利授权20余项;已发表学术论文170余篇,出版教材2部。



牛淼,中国科学院信息工程研究所助理研究员;主要研究方向为移动互联网隐私保护;已发表论文20余篇,其中被SCI/EI检索20余篇。



李维皓,西安电子科技大学在读博士研究生;主要研究领域为移动互联网隐私保护;已发表论文3篇,其中被EI检索3篇。

综合信息

IDC:全球超六成制造商已使用云计算

IDC日前公布的最新调查结果显示,全球六成以上制造商已使用云计算。根据IDC 2014年全球技术和行业研究调查结果显示,在美国有41%的制造业受访者称,他们正在通过公有云访问IT资源。

全球大多数制造商目前正在使用公有云(66%)或者私有云(68%),并至少有两种应用。受访者称,对于新的和替代性的IT投资来说,“也可以采用云”仍然是

公有云领域最常见的策略;有61.6%的受访者称他们企业对于全新IT服务的态度是“也可以采用云”,这个比例比替代IT现有职能的受访者略低一些(56.8%)。

对于IDC 2014年CloudView调查的制造业受访者来说,云服务和云基础架构在年度IT预算分配中所占的份额将在未来两年内增长27%。而制造商将越来越多地依赖于企业和行业云来访问信息技术资源以及运营支持。

(转载自《中国信息产业网》)

智能移动终端的位置隐私保护技术

Location Privacy Protection Technology on Smart Mobile Devices

杜瑞颖/DU Ruiying
王持恒/WANG Chiheng
何琨/HE Kun

(武汉大学计算机学院, 湖北 武汉 430072)
(Computer School, Wuhan University,
Wuhan 430072, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0023-007

摘要: 从位置隐私保护理论模型和位置隐私保护方法两个方面入手, 对智能移动终端上的位置隐私保护研究现状进行了探讨, 重点研究当前模型和方法的优缺点以及各自的适用场景; 结合智能终端和移动互联网的发展趋势, 指出当前位置隐私保护技术存在的问题, 对未来的研究方向提出了建议。

关键词: 基于位置服务; 位置隐私; k -匿名; 隐私保护; 隐私模型

Abstract: This paper discusses the status of the location privacy protection technology. It describes the characteristics and applications of the current schemes in terms of the theoretical model and method. In light of current developments in smart devices and mobile Internet, it points out existing problems of location privacy preservation and some directions for future work.

Keywords: location based service; location privacy; k -anonymity; privacy preservation; privacy model

近年来, 移动互联网的出现以及3G/4G、Wi-Fi 等各类移动通信技术的发展和普及, 使得智能手机和可穿戴设备等智能移动终端成为人们生活不可或缺的一部分。随着智能移动终端的成本越来越低, 硬件软件的功能越来越强, 人们已能随时随地连接网络并发送和接受信息, 工作和生活方式发生了前所未有的变化。

智能移动终端的实时在线、随身携带、情景感知的特点, 使得其可以提供大量的个性化服务, 基于位置服务(LBS)就是这些服务的典型代表。基于位置服务已经广泛地应用在人们的日常生活中, 并且还在不断地扩展服务的应用范围。在基于位置服务中, 用户通过智能终端上的应用(APP)向服务提供商提交自己的位置信息, 服务提供商则根据服务类型进行反馈, 如返回最近的餐馆、有空位的停车场等信息。以手机终端为例, 根据中国互联网络信息中心(CNNIC)于2014年8月发布的《中国移动互联网调查研究报告》^[1], 截至

2014年6月底, 中国手机网民规模为5.27亿, 其中约有46.9%的手机网民使用手机地图。手机地图用户中有57.6%的用户使用定位功能, 有40.8%的用户使用查询周边美食餐饮服务功能, 有24.4%的用户使用签到或位置信息分享功能。手机地图这类APP收集了大量用户的位置信息, 并发送给服务提供者或发布到网络上, 这无疑是个个人隐私的重要威胁。

位置隐私作为智能移动终端中的一个重要安全威胁, 近年来受到全球研究机构的广泛关注。在智能移动终端广泛普及的今天, 对手能够通过移动应用或移动网络收集更多用户位置信息^[2], 从而更容易掌握用户的生活规律(如上下班时间、喜欢去的超市等)与个人隐私(如家庭住址、最近是否去医院等), 并实施进一步的目的(如贩卖个人信息、实施偷窃等)。棱镜门等事件使人们逐渐重视对个人隐私的保护, 位置隐私将成为

用户使用个性化服务的决定性因素之一。为了解决这一问题, 目前已经提出了一些位置隐私保护理论模型, 一些位置隐私保护方法也得到了广泛应用。本文将对这些理论模型和保护方法进行分析和总结, 并对出现的问题和面临的新挑战提出一些有效建议。

1 位置隐私保护理论模型

通常在基于位置服务应用中, 人们关心的隐私数据包括位置、身份和查询数据3个方面。我们可以形式化地表示位置服务中的查询请求: $(id, location, query)$ 。其中, id 表示用户的身份, $location$ 表示用户的位置坐标 (x, y) , $query$ 表示查询内容。位置和身份是用户的直接隐私, 能够标识到确定的个体对象, 例如家庭住址、身份证号等; 查询数据是用户的间接隐私, 虽不能直接确定用户的身份, 但内容却可以反映出用户的生活环

收稿日期: 2015-03-06

网络出版时间: 2015-04-28

基金项目: 国家自然科学基金
(61173154、61272451)

境,例如工资水平、健康状况等。目前,没有任何一种隐私保护理论模型可以适用于所有的应用场景,本节将重点讨论 k -匿名、差分隐私模型和博弈论这3类传统的隐私保护模型。

1.1 k -匿名

k -匿名模型由 Samarati 和 Sweeney 于 1998 年^[1]提出,它要求发布后的数据中存在一定数量的不可区分的个体,使攻击者至少不能从其他 $k-1$ 条记录中判别出隐私信息所属的具体个体。 k -匿名方法断开了个体与数据库中具体对象之间的联系,在一定程度上保护了敏感数据的隐私。本文给出的 k -匿名定义。

定义 1(k -匿名): $T(A_1, \dots, A_n)$ 是一个数据表, QI_T 是与其相关联的准标识符,当且仅当对任意一个准标识符 $QI \in QI_T$, $T[QI]$ 中的每一个值序列都至少出现 k 次,那么就可以称 T 满足 k -匿名。

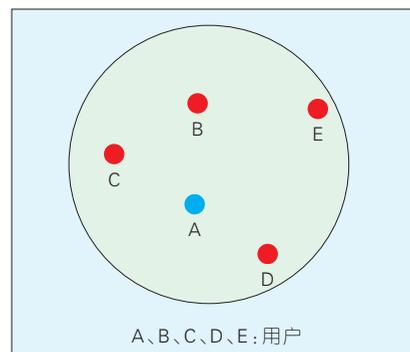
为了用形式化的语言准确地理解 k -匿名的定义,我们需要理解标识符 (Identifiers)、准标识符 (Quasi-Identifiers) 和敏感属性 (Sensitive-Attributes) 的概念。标识符属性是指可以直接标识个体身份的属性,如姓名、身份证号、驾照号码等,通过这些属性值能直接确定具体的个体。敏感属性指的是个人隐私属性,指个体不希望其他用户知晓的信息,例如工资水平、身体状况、家庭住址等。准标识符属性与标识符属性类似,也可以确定个体的身份,不同的是它需要进行间接的推测。通常情况下,准标识符属性不是单独出现的,而是一个属性组合。本文给出准标识符的具体定义。

定义 2(准标识符): 给定实体集合 U 、数据库表 $T(A_1, \dots, A_n)$, $f_c: U \rightarrow T$ 以及 $f_g: T \rightarrow U'$, 其中 $U \subseteq U'$ 。表 T 的准标识符 QI 为属性组 $\{A_1, \dots, A_i\} \subseteq \{A_1, \dots, A_n\}$, 其中 $\exists P_i \in U$ 且满足 $f_g(f_c(P_i|QI)) = P_i$ 。换言之,准标识符属性是指那些同时存在于数据

发布表和外部数据表中,通过对这两种数据表进行联接推测就可以获得个体隐私信息的一组属性。

Marco Gruteser^[4]最先将 k -匿名模型应用到位置隐私保护上,提出位置 k -匿名 (Location k -Anonymity) 的概念。位置 k -匿名利用 k -匿名的思想将用户的准确位置信息替换成一个空间区域,在该空间区域内至少存在 k 个不同用户,这样使得提出位置服务请求的用户在该空间区域内至少不能与其他 $k-1$ 个用户区分开来,从而保护了用户身份隐私。结合 k -匿名的定义,在位置 k -匿名模型中,标识符指用户的终端标识符(如电话号码等),敏感信息包括用户的身份信息 and 位置坐标等,可能的准标识符属性有时间、地点、查询内容等。图 1 是一个 $k=5$ 的位置 k -匿名的例子,共有 5 个用户 A、B、C、D 和 E。如果用户 A 需要请求位置服务,则与其他 4 个用户组成一个空间区域。经过位置匿名之后,每个用户的坐标都用这个空间区域表示。这样位置服务器和攻击者都只知道在此区域内有 5 个用户,但具体是哪个用户在哪个位置发起的服务请求无法确定,因为用户出现在每个位置的概率都是相同的。一般情况下, k 值越大,匿名程度就越高。

在文献[3]中作者指出隐私保护的涵义不仅仅是匿名,并通过实例说明了匿名数据同样会泄漏用户的身份。这是因为发布的数据中包含一些“准身份”信息,虽然单独查看这些



▲ 图 1 位置 k -匿名模型 ($k=5$)

“准身份”信息不能获得用户的身份,但将这些“准身份”信息链接到一起之后就能以很大的概率推测出用户的身份。同时,如果同一个 k -匿名组内的不同用户拥有相同的敏感信息,那么攻击者仍然可以从一条查询记录中推测出某个具体用户的真实隐私信息。为了解决 k -匿名模型存在的这一问题, Machanavajjhala 等人^[5]提出 l 区分 (l -diversity) 来隐藏同一个 k -匿名组内的用户的敏感信息。 l 区分要求一个 k -匿名组内除了至少有 k 个不同的用户外,仍需要保证该匿名组内有 l 个不同的兴趣点。Li 等人^[6]则进一步指出, l 区分对同一个 k -匿名组内的用户的敏感信息的保护还不够完善,因此提出 t 接近来实现更强的隐私保护。

1.2 差分隐私模型

差分隐私模型由 Dwork 于 2006 年提出^[7]。差分隐私保护通过添加噪声来改变原始数据,从而起到保护隐私的目的,对于一个严格定义下的攻击模型,其具有添加噪声少、隐私泄露风险低的优点。作者指出在一些情况下,例如一个医学实验的数据库,攻击者的目标仅仅是判断一个用户是否在发布的数据中。这样以 k -匿名为代表的隐私模型就无法判断用户的隐私是否真正得到了保护。差分隐私对敏感数据的计算处理结果对于具体某个用户的是不敏感的,单个用户在数据集中或者不在数据集中,对处理结果的影响微乎其微。本文对差分隐私的定义。

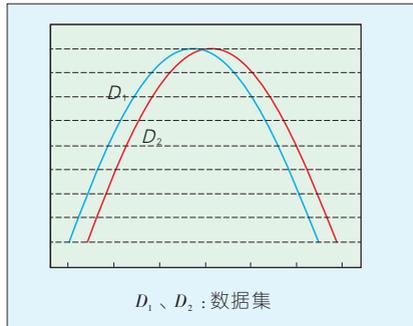
定义 3(差分隐私): 对于两个数据集 D_1 和 D_2 , $Range(K)$ 表示一个随机函数 K 的取值范围, $\Pr[E_i]$ 表示事件 E_i 的泄露风险,若随机函数 K 提供 ϵ -差分隐私保护,则要求两个数据集的差别至多为一条记录,并且对于所有 $S \subseteq Range(K)$, 有:

$$\Pr[K(D_1) \in S] \leq \exp(\epsilon) \times \Pr[K(D_2) \in S] \quad (1)$$

最后计算出的泄露风险 $\Pr[E_i]$ 取

决于随机化函数 K 的值。

图2给出了两个数据集 D_1 和 D_2 满足 ϵ -差分隐私的泄露风险曲线。



▲图2 ϵ -差分隐私的泄露风险曲线

在定义3中,有两点需要注意:首先,随机函数 K 的选择与攻击者所具有的先验知识无关,只要可以满足定义中的要求,就能够保护数据集 D 中任意数据的隐私;其次,在满足 ϵ -差分隐私保护时, ϵ 越小,添加的噪声越大,隐私保护的级别也就越高。因此,可以像 k -匿名中通过调整 k 的大小来实现不同的隐私程度一样,设置不同的 ϵ 值也能实现隐私保护等级的划分。

后续研究文献[8-10]进一步扩展了差分隐私模型的适用范围。其中 Andrés 等人^[8]的研究尤其值得注意,作者将差分隐私模型扩展到位置隐私保护领域。McSherry 和 Talwar^[9]、Dwork 和 Lei^[10]分别研究了满足差分隐私模型的数据发布方法,但均停留在理论的层面,还没有实际可用的隐私保护方案。

1.3 博弈论

基于博弈论的隐私保护模型用来解决多个终端的利益分配以及隐私保护程度与服务质量的权衡问题。例如,在 k -匿名模型中,不同的用户会有不同的隐私需求,而在参与匿名区域构建时,会消耗自身智能终端的资源。因此,需要在隐私需求与资源开销之间建立利益关系,使得各个参与方都可以有满意的服务体验,获得最大的利益。Freudiger 等人^[11]考

虑到自私节点对位置隐私的影响,以博弈论为基础分析了非合作情况下的位置隐私保护,但作者提出的系统模型仅针对以假名更换为基础的位置隐私保护机制。

有效的位置隐私保护机制背后的位置模糊算法必须考虑3个基本的元素:用户的隐私需求、对手的能力和知识、由于混淆真实位置而带来的服务质量下降的最大容忍度。Reza 等人^[12]提出了博弈论框架使得设计者能够从给定的服务中找到最优的位置隐私保护机制,而且满足用户对服务质量的要求。这种基于位置的隐私保护机制被设计以提供以用户为中心的位置隐私,因此是智能移动终端上实施的一种理想选择。

上述3个理论模型在位置隐私保护领域的研究都取得了一定成果,但也有较为明显的问题,这主要集中在以下两点:一是对安全需求定位不清,一些研究重点保护用户的身份,而另一些研究重点保护用户的位置,缺乏一个整体的安全需求分析,并且这些安全需求都集中在用户位置信息发布之后,而没有考虑位置信息在智能移动终端上的完整生命周期;二是对对手能力划分不明,一些研究将对对手能力固定在某些策略上,缺乏一个分层的对手能力划分,另一些研究虽然考虑了多种对手能力,但缺乏一个统一的对手模型。

2 位置隐私保护技术和方法

位置隐私保护技术是让位置服务提供商和非法人员不能或者无法轻易获得用户的真实位置相关信息(坐标、身份、兴趣爱好等)的防护方法。当前的位置隐私保护技术可以大致分为3类:位置模糊、身份隐藏和信息加密。位置模糊类方法通过扩大或者改变用户的真实位置,即用模糊的位置代替精确的位置,利用降低用户位置信息的准确度来达到位置隐私保护的目;身份隐藏类方法保留了用户的准确位置信息,这样就

保证了服务质量,而将用户的身份信息通过一定的技术方法隐藏起来;信息加密类方法采用加密手段在位置信息使用过程中隐藏用户隐私,使得非法攻击者即使得到了用户的敏感数据,也无法破解出原有的真实信息。另外,针对连续查询和特殊的应用场景,也存在一些专门的位置隐私保护方法。

2.1 位置模糊

位置隐私保护的主要目的就是保护用户在享受位置服务时的真实位置信息,因此首先想到的方法就是在将查询请求发送到服务提供商之前对位置信息进行模糊处理。目前存在3种位置模糊方法:虚假位置、地标技术和模糊空间。

(1) 虚假位置

虚假位置^[13]指用户用几个虚假的位置代替自身所处的真实位置来发送服务请求。在这类位置隐私保护方法中,用户不仅向位置服务器发送自己的真实坐标,而且以一定的策略生成一组假位置同时发送出去,这些假位置可以起到掩护真实位置的目的。真假位置在位置服务提供商是无法区分的,服务器必须查询出所有相关位置的服务请求,返回候选结果集,然后由用户根据自身的真实位置来判断所需的服务结果。显而易见的是,这种方法增加了服务器的查询处理开销,同时要求用户有判断结果准确性的能力。

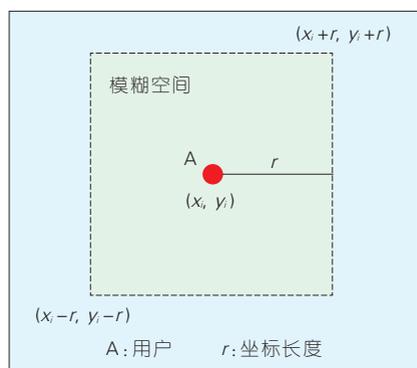
(2) 地标技术

为了解决虚假位置技术对服务器性能的影响问题, Hong 和 Landy^[14]提出了地标技术,它是虚假位置技术的一种特殊形式。与虚假位置技术不同的是,用户采用一个标志性的地理位置来代替其真实位置,位置服务器通过对这个标志性地理位置的处理来提供服务。这样攻击者就只能得知用户在这个标志性的地理位置附近出现过,而无法确定其精确的位置,从而保护了用户的位置隐私。可

以看出,地标位置与真实位置的距离远近会直接影响到基于位置服务的质量。

(3) 模糊空间

模糊空间^[15]指用一个空间区域来代替用户的具体位置坐标。区域的形状不限,普遍选择圆形或者矩形;区域的大小也不限,一般根据用户的隐私保护需求和服务质量要求确定。模糊空间位置隐私保护技术如图3所示。当前用户A的真实位置坐标为 (x_i, y_i) ,如果采用距离该坐标



▲图3 模糊空间位置隐私保护技术

长度为 r 的正方形作为模糊空间,则用户的位置就变换为了一个二维空间区域 $[(x_i-r, y_i-r), (x_i+r, y_i+r)]$ 。与虚假位置方法类似,位置服务器只知道用户在这个模糊空间内,而无法得知真实的位置信息。同样地,由于模糊空间降低了用户的位置精度,服务质量会根据区域的大小成反比例下降,并且该方法也面临服务器处理开销增大的问题。

2.2 身份隐藏

目前存在4种身份隐藏方法:匿名、假名技术、混合区方法以及盲签名技术。

(1) 匿名

如果攻击者不知道用户是谁,那么即使他得到了用户的真实位置,能够造成的危害也会小很多,因此如何隐藏用户的真实身份是当前研究的热点之一。其中,匿名化处理是比较直接的办法,它关注的是将用户的位

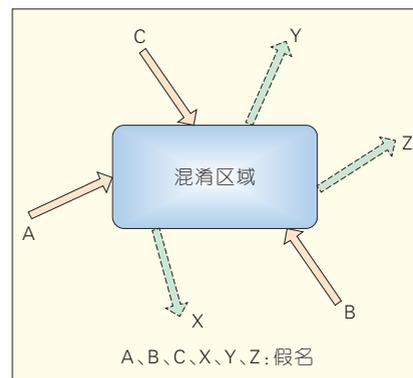
置信息与真实身份信息(如身份证号、电话号码等)分开,切断了位置和身份之间的联系。前面理论模型中提到的位置 k -匿名技术^[14]就是一种常用的匿名化处理方法。通过使一个空间区域内 k 个用户的身份不可区分,即使某个用户的位置信息被恶意的位置服务器或者攻击者获得,它们也无法推测出到底是哪个用户发起的哪个位置服务请求。

(2) 假名技术

假名技术是身份匿名的一种特殊形式,它的主要思路是让用户在发送位置服务请求时采用虚假的用户身份来代替真实的用户身份,这样也就使得服务提供商无法收集用户身份与位置的关联关系。即使非法攻击者通过特殊的技术手段获得了用户的位置信息,由于用户的身份是虚假的,这样就大大降低了真实用户面临的安全风险。Duckham和Kulik^[16]提出了一种基于假点的用户身份隐藏方案,此方案通过把一些虚拟用户以相同的概率插入到真实用户的位置周围来达到隐私保护的效果。

(3) 混合区方法

在假名技术的基础上,Beresford和Stajano^[17]提出混合区(mix zone)的方法,用于保护连续发布位置信息时的用户身份隐私。该方法将用户访问过的空间区域分为两种类型:应用区域和混淆区域。在应用区域中,用户可以提出位置服务请求和接收服务信息;在混淆区域中,用户禁止使用基于位置服务,几乎没有任何通信。为了更好地保护用户的位置隐私,用户在离开混淆区域时需要更换自己的假名。混合区位置隐私保护技术如图4所示。实例中给出了一个拥有3个用户的混淆区域。3个用户在不同时刻进入到混淆区域,使用的假名分别是A、B和C。当他们离开该区域后,立即更换假名为X、Y和Z。因为攻击者无法预测用户在混淆区域内停留的时间,并且用户在混淆区域中没有使用位置服务,增加



▲图4 混合区位置隐私保护技术

了将同一个用户前后使用的假名关联起来的难度。这样非法人员就无法继续追踪目标,从而达到保护用户身份信息的目的。

(4) 盲签名技术

在身份隐私保护技术中,盲签名技术也十分具有代表性,其核心思想是用户对要签名的内容进行盲化并发送给签名者,签名者对其签名后发送给用户,用户去盲后能得到正确的签名,从而保护用户要签名的内容不被签名者获取。Qi等人^[18]利用盲签名技术实现用户身份的隐私保护,提出了一种用户身份重混淆协议。Liao等人^[19]指出Qi方案中的盲签名方案并不能有效地消除一个合法移动设备上匿名ID和真实用户ID之间的关系,作者对注册和重混淆协议进行了改进,证明新方案可以保证管理者无法从匿名ID中得到任何真实ID的相关信息。

2.3 信息加密

信息加密技术是最基本的安全防护方法,通过将明文改变成不可读的密文,从而起到保护敏感信息的目的。同样地,信息加密的方法也可以应用到位置隐私保护领域,由于每个位置信息的处理和查询都是基于密文的,这就使得非法攻击者无法解密出用户真实的位置和身份信息。Khoshgozaran等人^[20]提出了一种基于密码学的位置隐私保护方法,与传统的 k -匿名、假名和混淆方案不同的

是,该方案带来的计算和通信开销非常小,而且在查询请求时不需要依赖于可信的中间匿名服务器。

传统的信息加密机制能够保护数据的机密性,但是大多依赖于公钥基础设施,资源提供方只有获取用户的真实公钥证书之后才能加密。属性基加密(ABE)^[21]的提出解决了这一缺陷,它常用于设置灵活的访问控制策略。通过把身份标识看成是一系列的属性,只有当ABE中解密者的身份信息和信息加密者描述的信息一致时,才可以解密加密者加密的信息。ABE应用在位置隐私保护中,可以在位置信息发布时提供加密,只允许有特殊属性的用户可以解密这些信息。Linke等人^[22]设计了基于属性隐私保护的移动传播方案,确保移动用户信息保密,加密解密机制依靠用户权限,提出了一种保护隐私的相互身份验证方案。

2.4 连续查询时的隐私保护技术

上述隐私保护方法多针对单次查询,不能适用于连续查询(如:用户不停地移动,并且重复请求LBS等应用场景)。连续查询是位置服务中一种常见的查询类型,具有位置更新频繁和实时性要求高的特点。如果直接应用传统方法于连续查询,可能会产生隐私泄露、匿名服务器性能开销大等问题,通过匿名化位置查询的辅助工具来混淆位置的有效性在连续地LBS情形下也会受到削弱。因此,学术界也对查询隐私进行了一些研究,并将位置隐私和查询隐私分开进行讨论。

Chow和Mokbel^[23]在2007年首次提出了连续查询隐私保护问题,在服务请求的初始时刻,用户会形成一个匿名集,作者指出将该匿名集作为查询有效期内的最终结果,从而解决将连续查询隐私泄露的问题。但是该方案最初生成的匿名集仅考虑用户初始时刻的邻近性,并没有考虑用户的运动性,因此仍然会造成位置隐私

泄露和服务质量下降。Pingley^[24]等人给出了一种新的查询隐私保护方法,即使用户的身份被显示,也能够保护连续位置服务下的隐私查询。它通过考虑查询情境和用户运动模型来产生虚拟查询,该方案对于服务提供商而言是透明的,多种位置服务的查询会被独立的应答。

2.5 特殊应用场景下的隐私保护技术

除了上述常见的位置隐私保护方法外,针对一些特殊的应用场景,一些研究人员也给出了专门的保护方案。Hashem等人^[25]针对无线自组网提出了一种保护用户身份与位置隐私的算法,其核心采用的是 k -匿名技术。Ma等人^[26]研究了车载通信系统中的长期位置隐私问题,试图评估累积信息对位置隐私的影响,重点关注了对手能否从信息中提取特征。Chow等人^[27]针对无线传感器网络设计了一种以 k -匿名技术为核心的具有位置隐私保护属性的监控系统,在提供高质量服务的同时也保障节点的隐私。Ren-Hung等人^[28]针对社交网络中集中式 k -匿名隐私保护方案的缺陷,提出了一种分布式的结构,使得用户通过在线社交网络关系实现相互信任,从而不再依赖于单一的可信匿名服务器。

容易看出,每类位置隐私保护技术都有不同的特点,针对不同的应用需求,我们将各种位置隐私保护技术的分析结果列在表1中。从表1可以

看出,他们的保护目标、关键技术等不尽相同。

3 存在的问题

上面介绍了近年来智能移动终端上位置隐私保护技术的主要研究成果,这些工作都取得了一定成果,但随着新技术和攻击手段的不断发展,目前仍有几个方面的相关问题有待解决。

3.1 缺乏完整而系统的位置隐私保护理论

虽然近年来关于位置隐私保护的研究越来越多,并提出了许多具体方案,但缺乏一个完整而系统的位置隐私保护理论,尤其是缺乏面向智能移动终端的位置隐私保护理论。首先,一个完整而系统的理论应该从明确的安全需求开始;其次,一个完整而系统的理论要合理假设对手的能力;最后,基于明确的安全需求与合理的对手能力,建立相应的安全模型。若没有上述的理论基础,则容易出现错误的结论。当前针对智能终端的位置隐私研究中,研究人员大多采用相同的位置隐私保护定义,即防止对手获得用户当前或过去的位置。这一定义尚停留在经验式的层面上,既没有划分出不同等级的安全需求,也没有指明不同对手的能力。而且大部分研究偏离了真正的安全需求,如以 k -匿名技术的核心的研究专注于降低对手对其分析结果的确

▼表1 位置隐私保护技术对比分析

保护技术	保护目标	关键技术	代表文献
位置模糊	位置	虚假位置、地标技术、模糊空间	文献[13-15]
身份隐藏	身份	匿名、假名、混合区、盲签名	文献[4]、文献[16-19]
信息加密	位置/身份	加密解密、属性基加密	文献[20]、文献[22]
连续查询时的位置隐私保护	连续查询内容	匿名集	文献[23-24]
特殊应用场景下的位置隐私保护	无线自组网	k -匿名	文献[25]
	车载网络	累积通信	文献[26]
	无线传感器网络	k -匿名	文献[27]
	社交网络	分布式 k -匿名	文献[28]

定性而非分析结果本身准确性,这正是由于缺乏坚实的位置隐私保护理论基础导致的。因此,随着位置隐私保护理论的完善,有必要设计更合适的位置隐私保护方法。另外,上述工作基本都是针对具有局部监控能力的对手,而没有考虑智能终端环境下无处不在的更强对手,因此这些方案在当前技术下基本都是不安全的。

3.2 缺乏隐私保护与服务质量的权衡方法

采用位置隐私保护方法一般都会降低位置服务质量,如准确度、精度、可信度等。例如,以实现 k -匿名为目标的位置信息保护方法,或用可信第三方的位置代替用户的位置,从而降低了用户位置的准确度,或用一片区域代替用户的位置,从而降低了用户位置的精度。在一些情况下,这种位置信息质量的降低不会影响用户获得的服务质量(如天气服务等对位置信息不敏感的应用,只需要精确到城市即可),但在更多情况下,用户的服务质量会因此下降(如兴趣点查询服务、导航服务等对位置精度敏感的应用,需要相对准确的位置信息)。然而,目前大部分位置隐私保护方法并没有考虑服务质量的需求,只是根据预设的隐私保护需求(如 k -匿名中的 k)来处理位置数据,这无疑会影响用户的体验。虽然已有一些研究考虑了服务质量与位置隐私的平衡,但这些研究都只针对单个的服务质量目标,尚缺乏对服务质量的完善评估。

3.3 缺乏对软件泄漏位置隐私的有效度量方法

当前大部分位置隐私保护方法主要针对恶意服务器^[29],即服务器获得用户提交的位置数据之后无法威胁用户的隐私。然而,大部分用户的位置数据都是通过移动终端上的软件发布,而这些软件则是由相应的服务提供商开发,现有位置隐私保护方

法并没有考虑到这种由软件泄漏位置数据的情况。在2014年的CCS会议上,Fawaz和Shin^[30]提出了一种针对移动终端环境的位置隐私保护框架,填补了这方面的空白。但是,作者提出的框架需要大量的用户交互,并且缺乏对导航等关键软件的支持。软件位置隐私程度的度量是一个前沿的研究领域,目前已有的研究方法主要是根据软件收集了什么位置数据、收集了多少位置数据或者收集位置数据是否经过了用户的授权来判断,并简单地将软件分为危害位置隐私和不危害位置隐私两类。然而,这些方法都没有考虑软件自身的功能需求和当前的用户环境,因此并不能准确地判断一个服务软件是否真正危害位置隐私。在位置隐私保护的方法上,如何对用户位置发布的移动终端软件做出合理的判断仍是一个亟待解决的课题。

3.4 大数据时代带来新的挑战

大数据时代用户的各种数据会从不同的角度和途径被收集,其中隐含了人们的行为模式、敏感信息和习惯偏好等隐私数据,为人们带来了严重的安全威胁。在大数据时代,传统的位置隐私保护方法已经不能完全胜任工作,攻击者可以从多种渠道获得用户各种类型的信息,这些信息包括位置数据和非位置数据,而这些数据均可以直接或者间接地泄露用户的位置隐私。例如,用户在服务A中保护起来的位置数据可能在另一个服务B中被泄露,如果攻击者同时获得了服务A和服务B的数据,即使服务A进行了很好的隐私保护,仍然可以重构出用户的隐私数据。目前,大数据、移动互联网和传感设备等位置感知技术的发展已经形成了位置大数据,大数据施展手段的条件也已经成熟。一方面,实时在线、携带方便和情景感知的特点使得智能移动终端上的信息生产呈现爆炸性的增长,这为大数据技术的实践提供了数据

基础。另一方面,成熟的数据挖掘技术可以从大量位置数据中有效地推测出有价值的信息,这为大数据技术提供了方法基础。因此,如何应对位置大数据带来的新挑战,将是未来位置隐私保护技术发展的一个重要研究方向。

4 结束语

智能移动终端的发展势不可挡,存在的安全问题也不能忽视,但是我们不能因噎废食,需要正确应对当前存在的安全威胁,特别是位置隐私泄露问题,寻找切实可行的方案。本文研究了目前智能移动终端上基于位置服务的隐私保护方法,总结了位置隐私保护的理论模型和技术方法,探讨了这些技术存在的问题。在研究新技术时,我们应充分考虑智能移动终端的完整保护周期,从数据源头到数据传输再到数据处理全方位保护终端安全,将使得未来智能移动终端的发展更加健康,在为用户提供个性化服务时可以无后顾之忧。

参考文献

- [1] 中国互联网络信息中心. 2013-2014年中国移动互联网调查研究报告 [EB/OL]. [2015-03-01]. <http://www.cnnic.net.cn/hlwfzj/hlwzxbg/201408/P020140826366265178976.pdf>
- [2] 360 互联网安全实验中心. 中国手机安全状况报告 [EB/OL]. [2015-03-01]. <http://zt.360.cn/report>
- [3] SAMARATI P, SWEENEY L. Generalizing Data to Provide Anonymity when Disclosing Information [C]//Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, New York, NY, USA, 1998
- [4] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking [C]//Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys '03), San Francisco, USA, 2003:163-168
- [5] MACHANAVAJJHALA A, GEHRKE J, KIFER D, VENKITASUBRAMANIAM M. L-diversity: privacy beyond k -anonymity [C]//Proceedings of the 22nd International Conference on Data Engineering, 2006
- [6] LI N, LI T, VENKATASUBRAMANIAN S. l -Closeness: Privacy Beyond k -Anonymity and

- l*-Diversity [C]//Proceedings of the IEEE 23rd International Conference on Data Engineering (ICDE 2007), 2007: 106–115
- [7] DWORK C. Differential Privacy: A Survey of Results [J]. Theory and Applications of Models of Computation, 2008,35(1):1–19
- [8] ANDRÉS M E, BORDENABE N E, CHATZIKOKOLAKIS K, PALAMIDESSI C. Geo-indistinguishability: differential privacy for location-based systems [C]//Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security, New York, NY, USA, 2013:901–914
- [9] MCSHERRY F, TALWAR K. Mechanism Design via Differential Privacy [C]//Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, 2007. FOCS'07, 2007:94–103
- [10] DWORK C, LEI J. Differential privacy and robust statistics [C]//Proceedings of the 41st annual ACM symposium on Theory of computing, New York, NY, USA, 2009:371–380
- [11] FREUDIGER J, MANSHAEI M H, HUBAUX J-P, PARKES D C. On Non-Cooperative Location Privacy: A Game-Theoretic Analysis [C]//Proceedings of the 16th ACM conference on Computer and communications security, 2009:324–337
- [12] REZA S, GEORGE T, CARMELA T. Protecting Location Privacy: Optimal Strategy against Localization Attacks [C]//Proceedings of the 2012 ACM conference on Computer and Communications Security, CCS'12, 2012:617–627
- [13] KIDO H, YANAGISAWA Y, SATOH T. An Anonymous Communication Technique Using Dummies for Location-based Service [C]//Proceedings of the IEEE International Conference on Pervasive Services, 2005: 88297
- [14] HONG J I, LANDY J A. An Architecture for Privacy-Sensitive Ubiquitous Computing [C]//Proceedings of the International Conference on Mobile Systems, Applications, and Services(MobiSys'04), 2004: 1772189
- [15] GRUTESER M, GRUNWALD D. Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking [C]//Proceedings of the International Conference on Mobile Systems, Applications, and Services(MobiSys'03), 2003:1632168
- [16] DUCKHAM M, KULIL L. A formal model of obfuscation and negotiation for location privacy. [C]//Proceedings of the IEEE International Conference on Pervasive Services, 2005: 88193
- [17] BERESFORD A R, STAJANO F. Mix zones: user privacy in location-aware services [C]//Proceedings of the Second IEEE Annual Conference, Pervasive Computing and Communication Workshops, 2004:127–131
- [18] QI H, WU D, KHOSLA P. The quest for personal control over mobile location privacy [J]. IEEE Communication Magazine, 2004,42(1):130–136
- [19] JIAN L, YING Q, PEI H, MENTIAN R. Improved Mechanism for Mobile Location Privacy [C]//Proceedings of the Malaysia International Conference on Communication, 2005:559–563
- [20] KHOSHGOZARAN A, SHAHABI C, SHIRANI-MEHR H. Location privacy: going beyond *k*-anonymity, cloaking and anonymizers [J]. Knowledge and Information Systems, 2011,26(3):435–465
- [21] SAHAI A, WATERS B. Fuzzy identity-based encryption [J]. Advances in Cryptology–Eurocrypt, 2005, 34(9):457–473
- [22] LINKE G, CHI Z, HAO Y, YUGUANG F. A Privacy-preserving Social-assisted Mobile Content Dissemination Scheme in DTNs [C]//Proceedings of the INFOCOM, 2013: 2301–2309
- [23] CHOW C, MOKBEL M F. Enabling privacy continuous queries for revealed user locations [C]//Proceedings of the Int Symposium on Advances in Spatial and Temporal Databases (SSTD). Boston: Springer, 2007
- [24] PINGLEY A, NAN Z, XINWEN F. Protection of Query Privacy for Continuous Location Based Services [C]//Proceedings of the INFOCOM, 2011:1710–1718
- [25] HASHEM T, KULIK L. Safeguarding Location Privacy in Wireless Ad-Hoc Networks [C]//Proceedings of the UbiComp 2007: Ubiquitous Computing, 2007: 372–390
- [26] MA Z, KARGL F, WEBER M. Measuring Long-Term Location Privacy in Vehicular Communication Systems [J]. Computer Communications, 2010, 33(12):1414–1427
- [27] CHOW C-Y, MOKBEL M F, HE T. A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks [J]. Mobile Computing, IEEE Transactions on, 2011,10(1):94–107
- [28] RENHUNG H, FUHUI H. SocialCloaking: a Distributed Architecture for *k*-anonymity Location Privacy [C]//Proceedings of the International Conference on Computing Networking and Communications, 2014: 247–251
- [29] WERNKE M, SKVORTSOV P, DÜRR F, ROTHERMEL K. A classification of location privacy attacks and approaches [J]. Ubiquit Comput, 2014,18(1):163–175
- [30] FAWAZ K, SHIN K G. Location Privacy Protection for Smartphone Users [C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014:239–250

作者简介



杜瑞颖, 武汉大学计算机学院教授、博士生导师; 教育部高等学校信息安全专业教学指导委员会委员; 主要从事信息安全、无线网络安全、计算机网络等方面的教学和科研工作; 已发表学术论文 40 余篇, 获得发明专利 3 项。



王持恒, 武汉大学计算机学院在读博士研究生; 研究领域为网络安全、手机安全。



何琨, 武汉大学计算机学院在读博士研究生; 研究领域为网络安全、移动计算。

综合信息

全球未来网络暨 SDN 技术大会北京开幕 以 SDN 为核心的未来网络并不遥远

2015 年 5 月 18—19 日, “2015 全球未来网络暨 SDN 技术大会”在北京盛大召开。中国工程院院士刘韵洁、ONF 执行总裁 Dan Pitt、全球 5G 联盟主席 Latif Ladid、ICANN 首席技术官 David Conrad、互联网体系结构委员会(IAB)主席 Andrew Sullivan、耶鲁大学教授 Richard Yang 等全球未来网络及 SDN/NFV 行业顶级专家, 围绕

当前网络面临的挑战与对策、未来网络的技术发展趋势及 SDN 开放网络的未来走向等重大议题展开讨论。

刘韵洁院士在大会现场演讲时表示, 网络现在遇到的问题、网络未来的需要等一系列问题已不可忽视, 只有大家齐心协力, 探讨新型技术、架构才能解决当前问题。SDN 的出现, 使得整个网络简单化, 尽管面临很多调整, 但 SDN 未来前景不可代替。

(转载自《中国信息产业网》)

移动数字取证技术

Mobile Forensics Technology

丁丽萍/DING Liping
岳晓萌/YUE Xiaomeng
李彦峰/LI Yanfeng

(中国科学院软件研究所, 北京 100190)
(Institute of Software, Chinese Academy
of Sciences, Beijing 100190, China)

数字取证是指科学地运用提取和证明方法, 对于从电子数据源提取的电子证据进行保护、收集、验证、鉴定、分析、解释、存档和出示, 以有助于进一步的犯罪事件重构或者帮助识别某些与计划操作无关的非授权性活动。无线通信技术的普及和智能终端应用的便捷带来了诸多的安全问题及针对智能终端的犯罪活动。移动支付等涉及个人财产和隐私信息的应用层出不穷, 导致针对移动通信系统的犯罪激增。据统计, 欧洲 80% 的犯罪涉及移动数字取证, 英国 90% 的犯罪涉及移动数字取证, 美国 70% 的犯罪涉及移动数字取证。移动取证正在发展成为数字取证的主要工作。同时, 移动通信安全事件的事前安全防护与事后追责的诉讼相关理论和技术的研究也是信息安全和取证领域的研究热点问题。

数字取证技术的研究有鲜明的国家特点, 即国家的性质、法律和制

收稿日期: 2015-03-01

网络出版时间: 2015-05-08

基金项目: 国家高技术研究发展(“863”)计划(2015AA011709); 国家科技重大专项基金资助项目(2012ZX01039-004); 中国科学院战略性科技先导专项基金资助项目(XDA06010600)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0030-004

摘要: 对应移动数字取证技术的 4 个方面: 移动设备取证、移动系统取证、移动网络取证和移动应用取证, 给出了移动设备取证的步骤和手段, 基于 iOS 和 Android 系统的数字取证技术及其特点, 移动网络下数字取证的基本手段和技术, 移动应用取证的基本特征; 认为随着越来越多的新概念和新技术的发展, 未来智能移动终端数字取证技术将成为数字取证的主流之一。

关键词: 智能移动终端; 数字取证; 移动取证; 网络犯罪

Abstract: In this paper, we suggest that current smart mobile digital forensics technology can be categorized as: mobile device forensics technology, mobile systems forensics technology, mobile network forensics technology, and mobile application forensics technology. In terms of mobile device forensics, we propose the procedure and technology of mobile devices forensics. In terms of mobile systems forensics, we propose the digital forensics technology and features of iOS and Android mobile system. In terms of mobile network forensics, we propose the basic digital forensics method and technology under mobile network. In terms of mobile applications forensics, we propose the basic features of mobile applications forensics. According to the article, with more and more new concepts and new technology development, in the future, the smart mobile terminal digital forensics technology will be one of the mainstream of digital forensics.

Keywords: smart mobile terminal; digital forensics; mobile forensics; cyber crime

度对于数字取证技术的研究均具有一定的影响和制约。照搬照抄国际上的数字取证技术和工具的做法是不可取的, 结合中国国情的数字取证探索值得大力提倡。目前, 中国在操作系统的可取证研究、BIOS 芯片取证方面已经推出了自主创新的研究成果, 但与国际上更为成熟的数字取证技术相比, 差距还比较大。

无线通信技术的复杂性和多样性使得数字取证面临诸多难点问题。从移动互联网的组成看, 移动取证包括:

(1) 移动设备取证, 包括各种不同型号品牌的手机、平板电脑(PAD)、自带设备办公(BYOD)、各种

不同的物联网终端等。

(2) 移动系统取证, 包括各种移动终端操作系统的取证。

(3) 移动网络取证, 包括对于各种协议的分析和网络中传输的数据包的截获与提取分析。

(4) 移动应用取证, 包括对各种不同的应用采用不同的技术方法有针对性地进行证据获取和分析。

移动设备取证、移动系统取证、移动网络取证、移动应用取证是无法完全隔离开来的, 需要综合考虑。

1 移动设备取证

美国国家标准技术研究所(NIST)在 2014 年 5 月份推出了移动

设备取证的指导原则^[1],对移动设备取证的目的和范围、方式和方法做了系统性的分析和介绍,其中包括移动设备的特点、存储结构、标识模型特点、移动网络的特点、取证工具的能力、现场的保护和评估、打包传输和存储证据、现场应急处理、移动设备标识、工具选择和期望、移动设备存储获取、外围设备、对移动设备的云服务等内容。

综合来讲,移动设备取证可以分为4个步骤:保护证据、获取、检查和分析、报告。移动取证的步骤如图1所示。

保护证据的目的有两个,一是要最大限度地获取相关的证据数据,二是要保护证据数据的完整性和原始性以确保其可采性。获取证据是针对原始数据的镜像、提取等。鉴定与分析是要找出能证明特定事件的发生与否的证据。报告是要按照诉讼和调解部门的要求出具鉴定和取证的结论性报告。

根据提取数字证据的不同手段和方式,可以将移动设备取证分为5个层次,自底向上逐个难度增加,其分别是:手工提取、逻辑提取、十六进制转储、芯片拆除和微码读取。移动设备取证的5个层次如图2所示。

1.1 手工提取

所谓人工提取是指手工使用按钮、键盘、触屏等方法浏览并用照相机拍摄显示的数据内容。如果数据量很大,人工提取的难度将会很大。现在有一些自动化的工具可以帮助自动实现人工提取过程。目前,已经有一种设备,把手机固定在一个装有照相机的架子下,相机拍摄下每一个屏幕显示会通过一根线自动传输到电脑中并打上 Hash 固定成证据。

1.2 逻辑提取

逻辑提取就是要用计算机和移动设备建立连接,然后,使用相应的逻辑提取工具进行提取。进行逻辑

提取应该注意的问题是要牢记连接方式和相关的协议,因为错误的连接方式和协议可能会导致数据被篡改和提取到错误的数。

1.3 十六进制转储

十六进制转储主要是用来直接提取闪存上的数据。这类方法的挑战是如何解析和解码捕获到的数据。检测到文件系统的逻辑视图并报告一些文件系统以外的残余数据也是一个挑战。这个层面的工具包括:连接线或者 Wi-Fi 以及取证工作站等等。

1.4 芯片拆除

芯片拆除方法也是用来提取闪存中的数据。但是,这种方法是更直

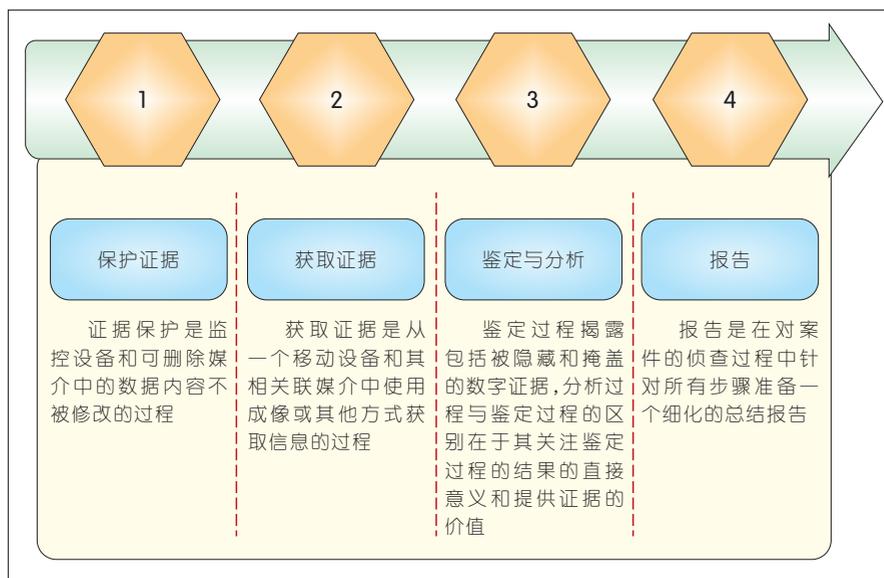
接的,要求对芯片创建一个二进制/十六进制镜像。为了获取二进制/十六进制文件,均衡抹除算法必须被逆向工程。完成后,二进制镜像文件就可以被分析了。这种方法和传统的磁盘镜像密切相关。这种方法的作者需要进行训练。

1.5 微码读取

微码读取是通过电子显微镜对 NAND 和 NOR 两种类型的闪存进行物理提取的方法。需要专家、合适的设备、时间和对相关信息的深度了解。这种方法仅仅用于其他方法不能用并且案件是大案和要案的情况。

1.6 移动设备取证工具

目前国际上有一些移动设备的



▲ 图1 移动取证的步骤

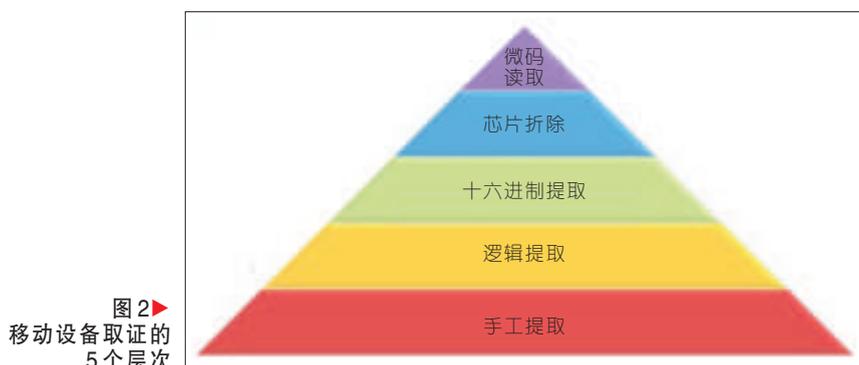


图2 移动设备取证的5个层次

取证工具,例如:

(1) FinalShield

FinalShield是一种用来屏蔽手机信号的取证辅助工具,该工具通过内部USB与Android系统手机进行连接,计算机或特定的手机取证工具利用FinalShield外部USB与该设备进行连接,作为手机取证的辅助工具共同得到有效的电子证据,可以有效的防止取证过程中有电话打入或短信接收,从而造成手机原始数据不必要的破坏或丢失。

(2) XRY

XRY是一款便携式取证箱,用来手机内存转储和采集数据的工具。此设备是由SIM卡读写器、USB通信单元、数据线、记忆卡读卡器、SIM复制卡等组成的。在安全模式下可以读取手机内的Message、telephonenumber、addressbooks、pictures、video等。该工具效果理想,并且容易操作,可以方便快捷的完成手机数据的分析、获取、查看工作,同时,还能通过加密文件的创建,保护数据不被其他未经允许的人员进行查看。该工具完成取证工作后,会得出相应的分析报告,方便调查工作人员查看详细的取证结果。

(3) OxygenForensic

OxygenForensic通过运用高级底层通信方式,获取更多数据,相比其他对智能手机、PDA以及普通手机的逻辑分析软件,显示了更大的优越性,尤其适合于Android系统手机的取证工作。

(4) BitPIM

BitPIM是一种电话管理软件,能够查看手机的Phonebook、calendar、wallpapers、ringtones等数据。该软件可以在Linux等操作系统上运行,前提是需要我们安装正确的驱动程序。

(5) CELLDEK

CELLDEK是一款便携式手机取证箱,可以提取Android系统手机的原始数据。设备中嵌入一台笔记本,数据的提取和分析就是通过笔记本

内的特定软件来实现的。

2 移动系统取证

一般而言,移动设备的常用操作系统有iOS、Android、Windows Phone、BlackBerry等,目前比较主流的是iOS和Android,主要的移动系统取证研究也是围绕着这两个操作系统^[2]。

分析移动操作系统的取证方法,首先,要了解其文件系统及存储管理系统:用于存储的硬件是闪存控制器、NAND闪存、多媒体存储卡。内核负责存储的模块包括:存储设备的驱动、用于访问内存设备的子系统、块设备子系统、虚拟文件系统(VFS)、能够很好地支持大容量NAND的文件系统等等。Android操作系统为了实现应用的隔离,使用了沙箱的安全架构,这也是移动系统取证需要考虑的^[3]。

2.1 Android系统取证

(1) 逻辑技术取证

在有ROOT权限的情况下,可以用adb pull命令把文件系统的不同部分复制到Ubuntu工作站中进一步分析。备份分析使用的RerWare、AFLogical等也是不错的取证工具。

(2) 物理取证

包括硬件与终端实现连接的方法或者是物理上获取终端设备的方法,也包括将终端设备中的软件在具有ROOT访问权限条件下运行以获取分区完整镜像的技术,JTAG以及ROOT权限下的各种技术方法等。

通过各种取证手段获取时间的时序、系统的文件类型、对文件分区的镜像和分析等等。

2.2 iOS系统取证

iOS系统越狱和取证的关系问题:越狱使得取证容易了,数据却不安全了。越狱的好处——提权并安装未经Apple验证的程序;越狱后的风险——系统安全性大幅降低、可随意安装未经验证的应用(App)。iOS

的文件系统是HFS+,SQLite数据库包括地址簿、短信和呼叫记录等^[4]。

iOS设备和Android设备的最大区别就是其安全性。iOS设备可以设置一个PIN码(一般4位)来阻止非法访问,可以设置连续10次错误码将抹掉手机上的所有数据,还有一个会员机制——MobileMe,允许用户在设备丢失的情况下远程设置密码^[5]。

iOS系统取证的内容:由于iOS的加密机制,仅仅获取磁盘镜像还不行,应该先破译或者绕过密钥;内容保护密钥必须在获取阶段从设备中提取;需要解密存储的内容;密码需要用来完成一个主密钥集合;实际操作中,应该先线下提取源数据和计算机保护密钥^[6]。

iOS系统取证方法^[7]:

(1) 直接从iPhone获取数据。这种方式是指从连接在电脑上的手机中直接获取数据。

(2) 利用苹果的协议获取iPhone文件系统一个备份或者逻辑拷贝^[8]。这种方式仅仅能从一个镜像文件中获取证据(利用同步协议),最大的问题也是密钥的破解。

(3) 物理逐字节复制。这种方式即以传统的物理克隆的方法产生一个镜像文件。此方法的困难在于数据太大并且分析过程复杂,有时需要修改分区。iOS系统移动取证的最大难点在于突破加密机制^[9]。

2.3 Android与iOS系统取证对比

iOS系统和Android系统各有优势,iOS系统是完全封闭的系统,不开源,但是这个系统经过苹果的严格管理,在大部分情况下,第三方应用是无法拿到所有应用编程接口(API)的,是高安全性的一个优秀的系统,但是很多软件收费,必须通过越狱来达到免费得目的。从移动取证的难度上来说,iOS系统的取证难度较大,尤其是在不越狱的情况下尤为困难。

Android是一个开源并且免费的系统软件,在设计上Android就允许

自由替换系统组件,但是,这个系统本身安全性不高,并且平台系统散乱,形成了一个系统多个硬件的情况,但是由于系统开源,造成了软件免费,盗版猖獗的情况^[10]。从移动取证的难度上来说,Android系统的取证较iOS系统来说难度相对小些。

3 移动网络取证

移动网络取证的目的是分析网络传输的信号,包括截取数据包,分析数据和确定一些关键信息,如嫌疑人手机的位置等等。

在移动网络中,每一个移动基站有其自己的覆盖区域。蜂窝网络或者其标识(ID)也可用于识别无线电信号在该区域中的位置。基站会根据ID来识别属于它的用户及其具体位置。

取证人员首先需要获取网络的一个真实的拓扑图。然后,要了解移动网络的覆盖区域,或者是,我们要取证的区域内的基站数量、基站的拥有者等等。获取的网络数据对于蜂窝的覆盖可以用来判断嫌疑人可能或者不可能在案发现场。

4 移动应用取证

移动终端应用程序数量非常庞大,特别是对于苹果和安卓手机的应用,而且第三方应用程序包含的数据非常丰富。这些第三方应用由世界各地的开发人员完成,应用的数据也会有各种不同的格式:文本格式、SQLite数据库格式等等。文件备份的位置也很重要,很多智能手机应用的数据存在SQLite数据库中。App的数据恢复就是对于SQLite数据的恢复,如果数据没有被覆盖过,数据很容易恢复,使用的工具也很多,常用的取证工具都能做到。总之,App的取证应该具体问题具体分析,目前没有统一的解决方案^[11]。

5 结束语

移动数字取证的趋势应该集中

在移动设备取证、移动系统取证、移动网络取证和移动应用取证这4个方面。取证的效率一直是数字取证的重点和难点问题,移动取证也是如此。取证过程的处理速度主要表现在数据获取的速度、密码破解的速度等等。数据存储的特征主要表现在容量、结构、速度等^[12]。随着云计算和大数据技术的发展,云计算技术和大数据技术对移动取证的影响也开始凸显。云计算给数字取证带来的是便利和挑战,基于基础设施即服务(IaaS)提供的条件,建立专门的取证服务器,通过克隆技术,我们无需临时寻找存储设备,并花时间等待其启动并进入使用状态,从而大大降低成本和缩短时间;同时,云计算也给从云环境中提取证据成为一个新的研究课题^[13]。除此之外,如何利用大数据技术取证和如何对大数据中的电子证据进行提取两个方面的研究也在同步进行^[14]。结合越来越多的新概念和新技术的发展,未来智能移动终端数字取证技术将成为数字取证的主流之一。

参考文献

- [1] AYERS R, BROTHERS S, JANSEN W. Guidelines on mobile device forensics [J]. NIST Special Publication, 2013, 80(1):101-104
- [2] Bill Teel. Mobile Device Forensics Overview [EB/OL]. [2015-03-01]. <http://www.mobileforensicscentral.com/mfc/documents/MobileDeviceForensicsOverview-March2011.ppt>
- [3] ANDROULIDAKIS I I. Mobile Phone Security and Forensics: A Practical Approach [M]. Springer Science & Business Media, 2012
- [4] HOOG A, STRZEMPKA K. iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices [M]. Elsevier, 2011
- [5] ZDZIARSKI J. Hacking and securing iOS applications: stealing data, hijacking software, and how to prevent it [M]. O'Reilly Media, Inc., 2012
- [6] AHMED R, DHARASKAR R V. Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective [C]//Proceedings of the 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government. 2008: 312-23
- [7] ANDREW H. iPhone Forensics [EB/OL]. [2015-03-01]. <http://www.mandarin70.it/>

- Documents/iPhone-Forensics-2009.pdf
- [9] BELENKO A, SKLYAROV D. Evolution of iOS Data Protection and iPhone Forensics: from iPhone OS to iOS 5 [C]//Proceedings of the Blackhat Abu Dhabi Conference. 2011
- [9] JONATHAN Z. iOS Forensic Investigative Methods [EB/OL]. [2015-03-01]. <http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf>
- [10] QUICK D, ALZAABI M. Forensic analysis of the android file system yaffs2 [J]. NIST Special Publication, 2011, 78(1):81-87
- [11] LESSARD J, KESSLER G. Android Forensics: Simplifying Cell Phone Examinations [J]. NIST Special Publication, 2010, 77(1):55-83
- [12] BARMPATSALOU K, DAMOPOULOS D, KAMBOURAKIS G, et al. A critical review of 7 years of Mobile Device Forensics [J]. Digital Investigation, 2013, 10(4): 323-349
- [13] SIMOU S, KALLONIATIS C, KAVAKLI E, et al. Cloud Forensics: Identifying the Major Issues and Challenges [C]//Proceedings of the Advanced Information Systems Engineering. Springer International Publishing, 2014: 271-284
- [14] GUARINO A. Digital Forensics as a Big Data Challenge [M]. ISSE 2013 Securing Electronic Business Processes. Springer Fachmedien Wiesbaden, 2013

作者简介



丁丽萍,中国科学院软件研究所研究员,中国科学院基础软件国家工程研究中心电子取证与系统安全研究室负责人,中国电子学会计算机取证专家委员会主任;主要从事系统安全、可信计算、计算机取证等方面的教学、科研和工程开发工作;已发表学术论文40余篇,出版专著1部,获得发明专利3项。



岳晓萌,中国科学院软件研究所助理工程师,中国科学院在读博士研究生;主要从事系统安全、可信计算、虚拟化技术等方面的科研和工程开发工作。



李彦峰,中国科学院软件研究所工程师,中国科学院在读博士研究生;主要从事系统安全、Android应用安全等方面的科研和工程开发工作。

基于 Android 移动客户端的互联网 数据安全实证研究

Internet Data Security Based on Android Mobile Clients

何昱晨/HE Yuchen
石文昌/SHI Wenchang

(中国人民大学信息学院, 北京 100872)
(School of Information, Renmin University
of China, Beijing 100872, China)

随着通信技术的不断发展和移动通信设备的不断革新,以智能手机为代表的移动设备已逐渐成为人们日常生活中不可或缺的重要组成部分。文献[1]对2014年手机互联网使用情况进行的总结,使用手机上网人群的比重已达到85.8%,手机超过PC成为收看网络视频的第一终端。移动互联网的应用与日俱增,在人们日常生活中扮演着重要作用,由此应运而生的便是人们对移动互联网数据安全的担忧。相关研究表明,移动设备面临的最大的威胁来自以软件为中心实施的攻击,而其中很大一部分都是利用了浏览器漏洞^[2-4]。使用智能手机等移动客户端访问互联网将会对互联网数据安全产生怎样的影响已成为一个亟待回答的问题。

1 问题及其研究方法

1.1 问题描述

云存储是得到广泛运用的互联

收稿日期: 2015-03-11

网络出版时间: 2015-04-30

基金项目: 国家自然科学基金
(61472429); 北京市自然科学基金
(4122041)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0034-004

摘要: 基于 Android 移动客户端为研究平台,选取一种云为研究对象,对用户通过云 Android 客户端访问云端数据时在客户端留下的痕迹进行了研究;研究表明,在手机上存在访问云端数据的痕迹,从这些痕迹中能够提取与用户以及云相关的元信息,并且能从中推断部分用户行为。

关键词: 云数据安全; 移动客户端; 安卓; 访问行为; 痕迹

Abstract: With an Android mobile client as a research platform and a cloud as the research object, we explore the traces of access behavior left on the client side when a user accesses data stored on the cloud through an Android mobile client. The result of our research shows that traces of cloud data exist on the smart phone. We can extract the metadata of the user and a cloud and infer user behaviors from those traces.

Keywords: cloud data security; mobile client; Android; access behavior; trace

网应用之一,它将数据存储能力作为一种服务提供给使用者,是一种重要的云计算服务,用户可以通过智能手机等移动客户端方便地使用该服务。而云存储的安全性^[5-6]在一定程度上制约着云存储的发展,因此众多研究者将目光聚焦到云存储安全上。人们在享受互联网数据存储便利的同时也担忧互联网数据的安全性,那么,智能手机等移动客户端本身是否也会给互联网数据安全带来影响呢?这是本文关心的问题。

在常见的智能手机中,Android 操作系统占有较大的市场份额。据 IDC 发布的 2014 年智能手机出货量数据,采用 Android 和 iOS 为操作系统的智能手机占 96.3%,其中 Android 手机为 81.5%^[7]。因此,本文以 Android 移动客户端作为研究平台,选取中国实

用的一种云为研究对象,研究 Android 移动客户端的访问行为对云端数据安全可能造成的影响。

本文采用 Android 移动客户端去访问存储在云端的数据,分析、判断客户端是否会留存与云端数据相关的信息,目的是回答以下问题,第一,客户端是否会留存反映云端状况的相关信息,如果有,在哪些位置能够找到这些信息;第二,使用者对云端数据不同的操作是否会对留下的信息产生影响;第三,不同的文件类型是否会留下不同的信息;第四,在使用 Android 客户端访问云端数据之后,客户端的状态是否会对信息产生影响;第五,这些信息中是否包含元信息,如果有,能了解云相关的哪些元信息,是否可能包含敏感信息;第六,从留下的信息中能否反向推断出

使用者的行为。

1.2 Android 系统存储结构

本文针对 Android 智能手机开展研究。Android 手机往往拥有以下 3 种存储介质,容量很小的易失性存储器(RAM)、内部存储器(NAND-flash)和外部可插拔的 SD 卡^[9],还有部分 Android 手机有一个模拟的 SD 卡,物理上是内部存储器,逻辑上是外部存储器,即 SD 卡。内部存储器上储存着所有重要的系统数据以及用户安装的应用程序的系统数据。

用户在安装应用程序的时候可以选将应用程序安装到本地或者 SD 卡上,而与用户应用程序相关的数据通常会存储在内部存储器和外部 SD 卡上。在内部存储器上,应用程序相关的数据会被存储到/data/data/<应用程序包名>的文件夹下^[9],并且在该文件夹下也有一些通用的子文件夹:lib 存储库文件,databases 存储 SQLite 数据库文件及数据库日志,shared_prefs 存储配置信息,cache 存储缓存数据,而 files 存储应用程序私有文件。在外部存储器上,应用程序数据存储位置并未统一,但是常见是以应用程序包名为名称的文件夹。

1.3 提取信息的方法

本文选取中国实用的一种云为研究对象,用云的 Android 手机客户端访问云盘数据,通过分析手机内外部存储器的信息来判断用户数据和用户使用轨迹的安全性。因此在研究中就会涉及如何获得手机内部存储器和外部存储器的数据。

获得外部存储器的方法较为简单,以手机 HTC Sensation X315e 为例,只需将手机通过数据线连接到电脑上,在手机上选择打开 USB 存储,手机的 SD 卡就会被当作电脑的移动设备,可容易获得 SD 卡中的数据。还有部分手机的外部存储器是模拟的 SD 卡,当用数据线连接在电脑上时,这个模拟的外部设备会直接被当作

媒体设备,无需在手机上执行任何操作便可以在电脑上访问手机的外部存储器,如 Samsung SM-N900。

获得内部存储器中的数据可以通过 adb pull 命令将文件从手机内部存储器导出到电脑上,或者用 dd 命令得到镜像,再对镜像进行分析得到内部存储器中的数据。

1.3.1 用 adb pull 命令导出文件

在 Android 中,可以使用 adb pull 命令能将内部存储器中的文件导出到电脑。要获取 Android 应用程序相关的文件,就需要访问/data/data 文件夹下的内容,而只有 root 用户才能访问该文件夹下的内容,因此在实验中需要获得 root 权限,当非 root 用户试图访问/data/data 文件夹下的内容时会提示权限不足。

1.3.2 用 dd 命令制作镜像

镜像可分为单一分区镜像和整个内部存储器镜像,分别为分区和整个内部存储器的逐位拷贝。单一分区镜像能够获得分区中所有文件的内容、元数据以及被删除文件的信息,而整个内部存储器镜像还能获得分区之间和分区之外的数据^[10]。

使用 dd 命令可以获得镜像,例如:dd if = /dev/block/mmcblk0p29 of = /sdcard/ddimg,if 后是待拷贝分区,of 后是输出路径。上述命令的意义是将/dev/block/mmcblk0p29 设备文件复制到 SD 卡上,文件名称为 ddimg。而分区被挂载的位置可以通过 mount 命令查看。

2 实验方法设计

本文在设计实验时借鉴了 Grispos 等人在云存储数据取证方面的实验思路^[11],使用手机客户端对云端数据进行不同操作,判断云端数据是否会在手机上留下痕迹,如果有,进而分析不同的操作类型、手机及云存储服务手机客户端不同的状态是否会对痕迹产生影响。

实验的基本思想是:使用电脑将不同类型的文件上传至云盘,通过 Android 客户端对云盘中的文件进行不同操作。重复多次上述对文件的操作,每次对应着手机或云不同的状态。针对每次实验,分析内外部存储器上的文件,判断是否有云端痕迹残留在手机上。下面将分别从选取哪些类型的文件、对文件执行怎样的操作以及如何获得手机存储器的信息等方面对实验进行阐述。

2.1 文件类型的选取

云存储相当于一个远程的存储设备,因此用户往往在云盘上存储着常用的文档文件和较占本地空间的多媒体文件。故而,在本文选取常见的文档格式 docx、pdf、txt,常见的图片格式 png、gif、jpg、bmp、psd (PhotoShop 专用格式),常见的音乐格式 mp3、wma,常见的视频格式 mp4、mov、flv、rmvb 作为实验文件格式。其中 flv 是常见的在线视频文件格式,云存储不仅是一个远程存储设备还是一个在线存储设备,用户也可以使用它在线浏览视频。

2.2 对数据操作的分类

Grispos 等人在使用云存储手机客户端访问云端数据时,将对数据的操作分为 4 种:在线浏览、在线浏览并下载、不执行任何操作、在线浏览并删除云端文件^[11]。本文同样需要对同一类型的文件执行不同的操作,因此借鉴 Grispos 的思路将同一类型的文件上传 4 个,在云存储手机客户端上对同一类型的 4 个文件分别执行上述的 4 种操作。

手机本身包括两种状态,一种是开机状态,一种是关机状态,与本研究相关的还有两种与云存储服务相关的状态是注销用户和清除应用缓存。大多数需要登录的应用程序只有在用户主动注销用户的时候才会执行注销用户的操作,该操作可能会影响账户相关信息。而清除应用缓

存则类似将应用恢复至刚安装时的状态,对应用程序的信息也会产生一定影响。因此本文将分析在实验结束之后保持手机开机、将手机关机之后再开机、云盘注销用户(退出登录)、云盘清除应用缓存这4种状态。

2.3 获得手机存储器数据的方式

在分析内部存储器时,选择分析镜像的方法。通过 adb pull 导出的文件只包含文件的内容,不包括文件的元信息,同时也不包含被删除的文件的信息。然而文件的元信息和被删除文件的信息都是研究中期望获得的。本文只关注与云存储手机客户端相关的数据,因此只需要制作/data 所在磁盘分区的镜像即可。在分析 SD 卡的数据的时候,将手机通过数据线连接到电脑上,并选择打开 USB 存储,直接在电脑上分析文件。

分析过程如下:首先使用 dd 命令制作/data 分区的镜像,再将镜像导出至电脑上,使用取证大师对获得的镜像进行分析,分析/data/data/<XX cloud package name>文件夹下的子文件,再将它们导出到电脑上,使用 SQLite Development 对其中的 SQLite 数据库文件进行分析,用 Notepad++ 对文本文件进行分析,用 UltraEdit 对二进制文件进行分析。

3 实验及结果分析

3.1 详细实验流程

大致的实验流程如图1所示。第一,在电脑上将文件上传到某云盘;第二,为手机获得 root 权限,将其恢复到出厂设置,打开“允许安装未知来源的应用程序”和“USB 调试”选项;并在手机上安装云 apk;第三,登录某云盘手机客户端,对文件相应操作,如表1所示;第四,保持手机和云盘在以下状态之一:保持手机开机、手机关机再开机、保持手机开机且云盘退出登录、保持手机开机且云盘清除数据、手机关机再开机且云盘清除



▲图1 简要实验流程

数据;第五,制作手机 data 分区镜像,对 SD 卡上的文件和镜像进行分析。

3.2 实验环境

实验电脑为 Dell,采用 Win7 专业版 32 位,CPU 为 Intel i5,其他辅助工具及版本如下:adb v1.0.31、取证大师 v3.3、SQLite Development v4.0、Notepad++ v6.5、UltraEdit v21.20。

3.3 外部存储器结果

3.3.1 HTC 手机实验结果

通过分析 SD 卡上以云应用程序包名命名的文件夹,能够得到如下结论:第一,所有文件类型都能够在 SD 卡上被发现;第二,文件类型会对能否在 SD 卡上发现文件产生影响。文档和音乐文件都是只要在线浏览便能在 SD 卡上找到文件;对于图片文件,psd 类型的文件只要在线浏览便能在 SD 卡上找到,而 bmp、gif、jpg、png 类型的只有在线浏览并下载才能在 SD 卡上发现;只有在线浏览并下载的视频文件才能在 SD 卡上找到;第三,对文件执行的不同操作会对能否在 SD 卡上发现文件产生影响。所有执行在线浏览并下载的文件均能在 SD 卡找到;所有不执行任何操作的文件均不会出现在 SD 卡上;第四,手机或者 XX 云的状态不会对 SD 卡上存储的文件造成影响。由于篇幅所限,在这里只列出视频文件在 SD 上的结果,如表1所示。

3.3.2 Samsung 手机实验结果

在 Samsung 手机上进行实验的结果大多数都与 HTC 手机上的相同,下面只列出不同的结果:第一,MOV 类型的文件不会出现在 SD 卡上,即使该类型的文件被执行了下载的操作;第二,与 HTC 手机不同,在线浏览的 psd 类型文件不会出现在 SD 卡上。

3.4 内部存储器结果

3.4.1 HTC Sensation X315e 实验结果

当手机在实验中保持开机时发现:cache 文件夹下的 uil-images 文件夹中存储着缓存图片和视频的缩略图;files 中的 imei.dat 文件中存储着手机的 imei 号。通过分析 databases 文件夹的数据库文件能够得到如下数据:<uid>filelist.db 能够得到云盘缓存文件的详细信息;account.db 能够得到用户详细信息;yidisk.db 能够得到下载任务的详细情况。shared_prefs 文件夹下的配置文件中包含云相关数据:当前是否在 Wi-fi 环境下上传和下载,是否自动备份照片和视频,云盘中是否存储图片,当前 ip 地址,最后登录的用户名及用户名类型。

而当手机和云盘保持不同状态时,本文发现,手机关机对 cache、databases、shared_prefs 文件夹中数据无影响;注销用户会导致 cache 文件夹内容被删除且不可恢复,对 databases 和 shared_prefs 文件夹无影响;而清除缓存则会删除这3个文件夹内容且不可恢复。

3.4.2 Samsung SM-N900 实验结果

当手机在实验中保持开机时,从 databases 文件夹中能够得到更多信息:<uid>cloudp2p.db 能够得到用户黑名单,好友信息,用户所参与的对话和群组的相关信息;account.db 依旧能够得到用户信息;<uid>filelist.db 能够得到云盘缓存文件详情,下载文件详情,用户分享动态相关信息,以及按浏览顺序存储的在线播放视频文

▼表 1 视频文件在 SD 卡上的实验结果

名称	执行操作	手机或应用的状态			
		手机开机	手机关机	注销用户	清除缓存
01.flv	在线浏览	无	无	无	无
02.flv	在线浏览并下载	有	有	有	有
03.flv	不执行任何操作	无	无	无	无
04.flv	在线浏览并删除	无	无	无	无
05.mov	在线浏览	无	无	无	无
06.mov	在线浏览并下载	有	有	有	有
07.mov	不执行任何操作	无	无	无	无
08.mov	在线浏览并删除	无	无	无	无
09.mp4	在线浏览	无	无	无	无
10.mp4	在线浏览并下载	有	有	有	有
11.mp4	不执行任何操作	无	无	无	无
12.mp4	在线浏览并删除	无	无	无	无
13.rmvb	在线浏览	无	无	无	无
14.rmvb	在线浏览并下载	有	有	有	有
15.rmvb	不执行任何操作	无	无	无	无
16.rmvb	在线浏览并删除	无	无	无	无

件的详情。

而当手机和云盘保持不同状态时,本文发现手机关机机会使 databases 和 files 文件夹增加与设备相关的文件,而对 shared_prefs 无影响;而注销用户对这 3 个文件夹数据几乎没有影响;清除缓存不会删除全部数据。databases 中还有 account.db, advertise.db 等 4 个数据库文件;files 中还保存着云登录时的 html 文件;shared_prefs 中还发现用户 ip 地址。

3.4.3 Samsung SM-G9008V 实验结果

Samsung SM-G9008V 实验结果与 SM_N900 几乎没有差别,见 3.4.2,只是在云盘清除缓存的情况下除了 lib 的所有文件都被删除了。

4 结束语

本文从客户端和服务器相结合的角度探究互联网数据安全问题,国际上也有类似的研究。Grispos G 等人研究智能手机是否能够成为云存储取证的代理^[1],本文更关注数据访问痕迹的检测与分析。GAI

Mutawa N 等人以社交软件为研究对象,在手机上执行预定义的活动集合,借手机手机的备份,通过人工分析探讨是否能从中发现与预定义活动集相关的信息^[12],而本文借助于镜像,通过分析元数据和删除文件信息来研究 Android 移动客户端上的用户行为对互联网数据安全可能带来的影响。

本文以 Android 手机客户端访问云盘中的数据为场景,检测从手机上能否发现涉及云端数据安全的行为轨迹。实验研究表明,手机上留存有云端数据的访问痕迹,从这些痕迹中能够提取云端及用户相关的元信息,同时,借助残留信息能在一定程度上反向推测用户的行为,这对云端数据的安全性具有一定的负面影响,是互联网数据安全的一种隐患。可见,移动客户端给移动互联网的数据安全带来了新的挑战,值得业界重视,并采取有效措施应对相应的挑战。

参考文献

- [1] 第 35 次中国互联网络发展状况统计报告 [EB/OL]. [2015-03-08]. <http://www.cnnic.net.cn/>

hlwzfzj/hlwzxbg/hlwztjbg/201502/t20150203_51634.htm

- [2] BECHER M, FREILING F C, HOFFMANN J, et al. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices [C]//Proceedings of the Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011: 96-111
- [3] DWIVEDI H. Mobile application security [M]. Tata McGraw-Hill Education, 2010
- [4] CHAOUCHI H, LAURENT-MAKNAVICIUS M. Wireless and Mobile Networks Security [M]. Wiley-ISTE, October, 2009
- [5] WANG C, WANG Q, REN K, et al. Privacy-preserving public auditing for data storage security in cloud computing [C]//Proceedings of the INFOCOM, 2010:1-9
- [6] WEI L, ZHU H, CAO Z, et al. Security and privacy for storage and computation in cloud computing [J]. Information Sciences, 2014, 258(4): 371-386
- [7] IDC: 2014 年 Android 市场份额 81.5% iOS 份额下降 [EB/OL]. [2015-03-08]. <http://tech.163.com/15/0225/07/AJ9HL4H7000915BD.html>
- [8] KIM H, AGRAWAL N, UNGUREANU C. Revisiting storage for smartphones [J]. ACM Transactions on Storage (TOS), 2012, 8(4): 14-18
- [9] HOOG A. Android forensics: investigation, analysis and mobile security for Google Android [M]. Elsevier, 2011
- [10] FARMER D, VENEMA W. Forensic discovery [M]. Upper Saddle River: Addison-Wesley, 2005
- [11] GRISPOS G, GLISSON W B, STORER T. Using smartphones as a proxy for forensic evidence contained in cloud storage services [C]//Proceedings of the System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, 2013: 4910-4919
- [12] MUTAWA N, BAGGILI I, MARRINGTON A. Forensic analysis of social networking applications on mobile devices [J]. Digital Investigation, 2012, 9(S):24-33

作者简介



何昱晨,中国人民大学信息学院在读硕士研究生;主要研究方向为云安全、云取证;正参与 1 项国家自然科学基金和 1 项北京市自然科学基金等科研项目的工作。



石文昌,中国人民大学信息学院教授、博士生导师,中国人民大学信息安全研究所负责人,教育部信息安全专业教学指导委员会委员;主要研究方向为可信计算与系统安全;曾完成 UNIX 操作系统在中国的移植,开发出符合国际/国家标准的安全操作系统;已发表学术论文 100 余篇,出版著作、教材 3 部。

移动互联网安全测评关键技术研究

Key Technologies of Security Test for Mobile Internet

范红/FAN Hong
杜大海/DU Dahai
王冠/WANG Guan

(公安部第一研究所检测中心, 北京 100048)

(Testing Center, the First Research Institute of Ministry of Public Security, Beijing 100048, China)

移动互联网(MI)^[1]是一种通过智能移动终端,采用移动无线通信方式获取业务和服务的新兴业务,包含终端、运行环境和应用3个层面。终端层包括智能手机、平板电脑、电子书、MID等;软件包括操作系统、中间件、数据库和安全软件等。

移动互联网结合了传统互联网和移动通信技术的技术,同时创造出了很多新的产业链。手机转账、手机购物、移动互联网金融、移动定位技术、近场通信技术、基于移动定位技术的周边交友、移动搜索、微博、朋友圈等社交网络、手机地图等都是新的应用。移动智能终端正逐渐完善功能,融合了传统的PC技术,在智能终端上可以实现应用程序的安装和卸载。智能终端也拥有多种操作系统,包括Apple公司的iOS、Google公司的Android、Nokia公司的Symbian、Microsoft公司的Windows Phone等,还有一些基于Android系统开发的手机操作系统,使得移动智能

收稿日期: 2015-03-06

网络出版时间: 2015-04-28

基金项目: 国家高技术研究发展(“863”)计划(2009AA01Z437、2009AA01Z439); 国家发改委2012年信息安全专项(发改办高技[2012]2091号)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0038-003

摘要: 探讨了移动互联网安全测评的5个重要方面: 物理安全、移动智能终端安全、网络安全、应用安全和网络安全管理; 给出了具体的测评指导内容; 认为窃听、恶意吸费、信息窃取、位置信息泄露、金融窃取等安全事件频发, 移动互联网的安全问题严重威胁到国家安全、金融安全、社会稳定和人民的根本利益, 采取相应措施来保障移动互联网的安全必须得到高度重视。

关键词: 移动互联网; 信息安全; 风险评估; 安全测评

Abstract: In this paper, we discuss five key areas of mobile internet security testing: physical security, mobile terminals' security, network security, application security and network security management. Detailed test guidance is given in this paper. The security problem of mobile internet has attracted much attention. Sniffing, malicious charge, information theft, position leakage, financial stealing and other security incidents occur frequently. Security of the mobile Internet affects national security, financial security, social stabilization and people's interest. Therefore, some measures need to be carried out for the security of Mobile Internet.

Key words: mobile Internet; information security; risk assessment; security test

终端的技术呈现多样化, 由此而产生的安全问题也趋于复杂。

在移动智能终端的操作系统中, 很多应用软件是在市场开放应用的情况下被用户任意下载。一些黑客程序被用户无意识的下载到移动智能终端并被安装, 从而在移动终端装上了“后门”程序, 不法分子便可以借此窃取用户信息。据工信部2014年1月发布的统计数量, 中国移动互联网用户数量已经突破8亿。由于存在全球最大的用户, 中国移动互联网用户的信息安全面临更大的威胁。据2014上半年网秦手机安全报告: 中国居全球手机病毒感染榜首。中国大陆地区以18.20%感染比例高居全球智能手机病毒重点感染区域第一; 印度、沙特、印度尼西亚分别以

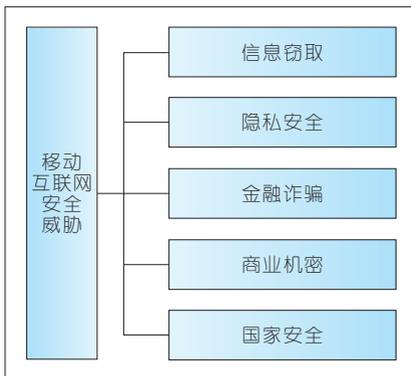
14.20%、9.60、8.20%紧随其后; 美国以7.70%感染比例居全球第5^[2]。移动互联网安全已经成为中国网络安全问题的一个严重威胁。移动互联网面临着信息窃取、隐私信息泄露、金融诈骗、商业机密和国家安全等多个方面的威胁。

1 移动互联网安全威胁

移动互联网融合了传统互联网的技术, 移动智能终端操作系统多样化, 应用软件市场开放等特点, 使其安全问题较为复杂。移动互联网安全威胁如图1所示。各部分具体说明如下:

(1) 操作系统安全漏洞

操作系统漏洞^[3]是指移动智能终端操作系统(如Android、iOS等)本身所存在的问题或技术缺陷, 给黑客留



▲图1 移动互联网安全威胁

下了攻击的机会。比如iPhone的Mail远程信息泄露漏洞，iPhone内嵌的Mail邮件客户端在处理安全套接层(SSL)连接时存在漏洞，远程攻击者可能利用此漏洞获取用户的敏感信息。如果将iPhone内嵌的Mail邮件客户端配置为对入站和出站连接使用SSL的话，即使邮件服务器的身份已经改变或不可信任，Mail也不会警告用户。能够拦截连接的攻击者可以扮演称为用户的邮件服务器，获得用户的邮件凭据或其他敏感信息。移动智能终端操作系统通常每隔一段时间会更新一个新的版本，提示用户对终端操作系统进行升级，修补之前系统存在的漏洞。

(2) 恶意吸费

在移动智能终端出厂之前或者刷机的时候，尤其是一些山寨手机，会被植入很多用户并不知情的软件。这些软件当中，很多就是后门软件，在用户不知情的情况下，这些后门软件会自动启动。后门软件通过转发短信、盗打电话等方式扣费。

(3) 信息窃取

通过植入木马软件，读取存储在移动智能终端的数据信息，比如通讯录、短信、通话内容、记事本、时间提醒、银行账号、个人隐私信息等数据，然后通过网络传输到指定地方。

(4) 垃圾信息

垃圾信息是指未经用户同意向用户发送的用户不愿意收到的短信息，或用户不能根据自己的意愿拒绝

接收的短信息。不法分子通过伪造移动式基站，在不同地区获取周边移动智能终端的用户信息，然后通过群发功能给用户推送一些广告等垃圾信息。垃圾信息泛滥，已经严重影响到人们正常生活、运营商形象乃至社会稳定。

(5) 钓鱼欺诈

不法分子通过搭建购物网站、或者假冒网站，使用户在不明实情的情况下输入网银账号及密码等机密信息，不法分子在获取个人账号密码之后，将用户的存款转走。钓鱼网站已经成为目前移动互联网金融诈骗的重要手段，给国家和公民带来了巨大的损失，严重影响着国家和社会的安全和稳定。

(6) 位置信息窃取

移动智能终端中通常包含有全球定位系统(GPS)定位信息，或者通过周边网络接入点信息来获取移动智能终端的精确位置信息，这些包含移动智能终端经/纬度信息的数据被存储在终端中，在移动智能终端接入网络之后，用户的个人位置信息及行走轨迹就会被上传至远端服务器。

(7) 通话窃听

通过安装木马程序在移动智能终端，在移动智能终端开机之后，它可以备份这个手机的所有通话记录，并通过移动智能终端的移动网络或者Wi-Fi来上传到一个固定的位置，从而窃听到他人通话内容。

(8) 后台拍摄

通过安装木马程序在移动智能终端，后台默默启动摄像模式，进行拍照，对照片进行压缩，上传至网络。

(9) 其他

由于移动智能终端的操作系统功能复杂化、多样化、开发性的特点，使得不法分子有更多的入侵机会。通过攻击操作系统漏洞、植入木马等多种手段，使得移动互联网安全遭受到更多的攻击，从而个人、社会和国家等不同层面的信息安全面临着较大的威胁，严重影响了国家和社会的

和谐稳定。

2 移动互联网安全测评关键技术

移动互联网安全问题涉及到多个方面，要想保障移动互联网的安全运营，需要从以下5个方面考虑：物理安全、移动智能终端安全、网络安全、应用安全和网络安全管理。

2.1 物理安全测评

要保证移动互联网的安全，首先必须保证整个网络系统的物理安全。物理安全包括计算机、机房环境、通信设备、设施、线路、电源、中继站、机房、终端等。

(1) 计算机系统环境条件测评。整个计算机系统的运行的环境，包括温度、湿度、空气清洁度、抗静电、供电、电磁干扰、关键设备热备等措施是否合格。

(2) 机房环境测评。计算机系统需要在一个较好的空间中运行，需要注意机房的温度、湿度、防火措施、地面抗静电、避开强震动源、防盗等。

2.2 移动智能终端安全测评

移动智能终端是移动互联网的核心部分，它在移动互联网安全中扮演着两个重要的角色。首先，移动互联网的入侵是从移动终端实施的，病毒、攻击等都可以通过移动智能终端进入到移动互联网；其次，移动互联网中的病毒和攻击又通过移动智能终端得以实现。移动智能终端的安全测评包括5个部分：硬件安全能力、操作系统安全能力、应用层安全要求、外围接口安全能力和用户数据保护能力^[4-5]。

(1) 硬件安全能力。移动智能终端硬件应在芯片级保证移动通信终端内部闪存和基带的安全，确保芯片内系统程序、终端参数、安全数据、用户数据不被篡改或非法获取。

(2) 操作系统安全能力。操作系统是移动智能终端的核心软件，操作

系统的安全型制约着终端的整体安全性。对操作系统的安全能力要求包括通信类功能控制;包括拨打电话、发送短信、发送彩信、发送邮件、移动通信网络数据连接、Wi-Fi连接;本机敏感功能受控机制:包括定位功能、通话录音功能、本地录音功能、拍照/摄像功能、对用户数据的操作;操作系统更新。

(3)应用层安全要求。应用层安全主要是安装在移动智能终端操作系统之上的应用软件的安全要求,包括:应用软件安全配置能力、应用软件安全认证机制、开机自启动程序监控、预置应用软件安全要求。

(4)外围接口安全能力。外围接口安全是确保用户对外围接口的连接及数据传输的可知和可控,外为接口包括无线外围接口和有线外围两种接口。

(5)用户数据保护能力。用户数据保护能力是为了防止用户数据不被非法访问、非法获取、篡改,同时能够通过备份保证数据的可恢复性。用户数据保护能力要求包括:用户数据的授权访问、数据加密存储、用户的数据远程保护、用户数据的彻底删除、用户数据的可恢复性。

2.3 网络安全测评

移动互联网网络包括两个部分:接入网和IP承载网/互联网。接入网采用移动通信网时包含基站、基站控制器、无线路由控制器、交换中心、网关、无线业务支持节点等相关设备;采用Wi-Fi接入时涉及到接入设备。IP承载网/互联网主要涉及路由器、交换机和接入服务器等设备及通信链路^[6-9]。

移动互联网网络安全和互联网类似,主要存在非法访问、网络攻击、网络入侵、病毒传播、洪水攻击、猜测攻击等一些攻击手段^[10-13]。因此,需要对上述安全问题做出相应的检测。主要包括以下检测内容:

(1)身份认证。所有接入设备和

终端在进入移动互联网时,需要对其进行认证,防止非法设备进入移动互联网实施攻击行为。

(2)监控审计。网络中安装有带日志审计功能的安全设备,以便对实施网络攻击的设备进行倒查,查找攻击点的位置及行为。

(3)数据加密。在移动互联网中传输的一些机密数据需要先进行加密处理后再进行传输,防止被窃听者截获。

(4)异常监控。实时监控移动互联网中的设备和流量信息,对于出现异常的设备或者异常的流量,应能够立即产生报警。

(5)漏洞扫描。对移动互联网承载网络内的关键设备进行漏洞扫描,防止攻击陷阱的存在,防患于未然。

(6)渗透测试。在移动互联网内部进行模拟攻击行为、发送病毒、木马等程序,查看网络是否能够对攻击行为采取有效的安全防护。

(7)安全补丁。对移动互联网承载网络内的关键设备进行检查,查看系统是否进行了补丁升级,修补已发现的安全漏洞。

(8)数据备份。对网络内部的关键设备进行定期数据备份,以备出现灾难时候能够应急恢复。

2.4 应用安全测评

移动互联网的应用来自多个不同的方面,可以是移动智能终端的业务,也可以是从互联网传输的数据,还包括这两个结合的一些新业务。这些应用包括即时通讯、网络浏览、文件传输、地图应用、位置定位及网络银行等业务^[14-15]。对移动互联网的应用安全测评包括以下几个方面:

(1)恶意代码查杀。对移动互联网中的应用在提交到应用商店时对其进行恶意代码检测,只有经过检测合格的应用才能上线,防止有恶意代码的应用在移动互联网上蔓延。

(2)访问控制。移动互联网的应用资源比较丰富,为了防止非法用户

对网络中的资源进行访问或者控制,需要对用户进行权限分配,访问资源时进行身份认证,防止移动互联网资源的被非法利用。

(3)内容过滤。对于在移动互联网中传输的数据,需要对其内容进行过滤,过滤内容包括一些垃圾信息、病毒附件。

2.5 网络安全管理测评

除了在技术上需要对移动互联网进行安全管理,从行政及实体上也需要建立相应的安全管理制度,以完善移动互联网的安全运营。网络安全管理主要包括以下几个方面:

(1)建立网络运营规范和标准。对于移动互联网的承载网络的运营情况需要有一套有效、安全的规范制度和标准,防止在实际运行过程中无据可依,违规操作出现安全故障的事故发生。

(2)定期巡检机制。移动互联网的关键设备和设施需要定期对其进行安全检查、抽查,查看其是否出现安全隐患,对于出现问题的地方需要立即采取补救措施。

(3)安全监管。建立第三方检测机构,对移动互联网网络定期进行安全测评,对提供移动互联网应用的商店进行安全检测,实时发布安全检测报告,并对外公布。

(4)应急响应制度。应建立完善的应急响应制度,对于移动互联网运行过程中突发的安全事故,建立相应的安全等级标准,并制订完善的应急响应方案,保障在事故之后能够迅速恢复网络运营。

3 结束语

移动互联网在未来10年必将成为人们日常生活的重要组成部分,从通信到购物、旅行、掌上银行等应用,与个人的衣食住行息息相关,因此必定会带来一系列的安全隐患。解决移动互联网在应用过程中的安全隐患

►下转第54页

DOI: 10.3969/j.issn.1009-6868.2015.03.010

网络出版地址: http://www.cnki.net/kcms/detail/34.1228.TN.20150420.1020.001.html

高移动无线通信干扰的物理层应对思考

Physical Layer Consideration for the Interference in High Mobility Wireless Communications

中图分类号: TN929.1 文献标志码: A 文章编号: 1009-6868 (2015) 03-0041-004

摘要: 从干扰避让、干扰抑制、干扰协调3个层次,针对高移动通信不同的干扰场景、干扰形态和干扰特征,提出混叠信号分离的机理、指导原则、分离方法和评估方法的物理层思考。认为必须在不同场景、网络结构和用户行为模式下,建立有效的干扰模型来分析和研究宽带无线通信网络的信息容量,探讨网络自由度对系统性能的影响,发展新的理论和方法应对干扰。

关键词: 高移动通信; 动态干扰容量; 干扰避让; 干扰抑制; 干扰协调

Abstract: This article proposes the mechanism, principle, methodology and evaluation method of signal separation for different interference scenarios, different interference form and different interference characteristics in high mobility communications, from the three folds of interference avoidance, interference suppression and interference coordination. It is necessary to formulate effective interference model and study the capacity of wideband wireless communication networks in different communication scenarios, different network structures, and for different user behaviors, investigate the effect of network degree of freedom to system performance, and develop new theory and methodology to handle interference.

Key words: high mobility communications; dynamic interference capacity; interference avoiding; interference suppression; interference coordination

陈文/CHEN Wen

(上海交通大学电子信息与电气工程学院, 上海 200240)
(School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

- 高移动通信面临物理层信道、传输层链路,以及网络层拓扑的快变引起的多变复杂干扰
- 需从分析动态干扰容量的基础上,从干扰避让、干扰抑制和干扰协调多层次应对高移动通信的干扰
- 信号处理和无线通信的新技术为高移动通信干扰应对提供了新的方法
- 物理层干扰应对为高移动通信干扰处理的主要手段

1 高移动无线通信的背景

无线通信从最初的点对点、固定、窄带逐步发展到目前的移动、宽带与规模网络化。作为带动信息产业高速增长的重要引擎,无线通信的平稳快速发展,对于促进社会经济发展,改善提高人民生活质量,提升中国在航空、航天、交通运输以及国防

等领域的科技实力起着非常重要的作用。

然而,目前无线通信正面临前所未有的挑战。首先多媒体宽带业务爆炸式发展,频谱资源稀缺日益严重;用户数与业务类型激增,网内、网间干扰成为制约性能和容量的瓶颈;网络拓扑趋于复杂、规模日益增大,系统的优化设计难以实施;信号处理与协作技术的日益复杂更带来设备复杂度、能耗与时延的大幅增加。此外,与民用及国防科技的迅猛发展相呼应,各种新的、更为复杂的无线通

信场景也应运而生,其中超高速移动场景下稳定、可靠、高效的宽带无线通信网络是未来无线通信发展的重要趋势之一。

目前超高移动场景包括轮轨列车(最高测试速度 574.8 km/h,最高运营速度 380 km/h),磁悬浮列车(最高测试速度 581 km/h,运营速度 431 km/h),飞机(运营速度 400 ~ 1 000 km/h),导弹(980 ~ 20 000 km/h)以及航天飞机(第一宇宙速度 28 440 km/h 环绕地球飞行,第二宇宙速度 40 320 km/h 脱离地球引力)等。中国目前已成为世界

收稿日期: 2015-03-18

网络出版时间: 2015-04-20

基金项目: 国家重点基础研究发展(“973”)计划(2012CB316106)

上高速铁路系统技术最全、运营里程最长、运行速度最高、在建规模最大的国家。国家中长期铁路网规划已确定:到2020年中国铁路运营里程将达到12万公里,其中高速铁路1.8万公里。

目前,中国高铁总长已位居世界第一。除了高铁之外,还有高速公路、磁悬浮列车等高速运输工具。这些高速交通工具的发展,对无线通信提出了更高的要求。一方面,旅客希望在高速移动的交通工具上,获得语音、视频、网络等服务;另一方面,也需要可靠传输海量视频监控数据和传感器信息,以满足公众安全的需求。人们感到在乘坐高铁或动车组时,因网络不可靠,电话很难接通,即使接通了也会频繁掉话,视频上网几乎更不可能。事实上,日本新干线、法国TGV、中国台湾高铁和京沪高铁,目前最高只能提供2 Mbit/s以下数据传输速率,大部分只能提供几十 kbit/s 传输速率,打开简单的网页都比较困难。同时,在高移动环境下,手机电池用得特别快,甚至会感觉到手机发烫。这些现象表明,现有技术还无法适应高移动环境下的宽带业务需求。

出现这些现象主要是因为终端高速移动时,物理层信道出现快变,传输层链路发生快变,并且网络层拓扑发生快变。此时,信道和网络状态难以获取,多重干扰难以消除,导致通信系统性能急剧下降。具体表现为:随着终端移动速度增大,通信的差错概率上升,频谱效率和能量效率下降。

为此,我们面临的技术挑战主要为:在快速移动环境下,如何保证良好的传输质量?如何传送更多的数据信息?如何能够节省更多的电池能量?

2 高移动无线通信面临的挑战

由于现有无线通信系统的应用

主要是面向中低速场景,如何针对上述超高速移动场景进行优化设计,实现信息的高效、可靠传输也是无线通信发展面临的新挑战。如果说无线通信的发展是依赖于信息论的发展,那么如今无线通信所面临的新挑战也就是信息论所面临的挑战。功率、能耗、时延、复杂度、移动性等多约束条件,高谱效、高能效、高可靠性等多元优化目标,空、时、频、码多处理域,以及不同系统架构、信道条件和承载业务所带来的复杂场景,这些多因素交织在一起使得无线通信网络的优化设计变得错综复杂。这就使得我们比任何时候都更需要新的信息理论来为我们提供强有力的理论支撑,让我们知道到底网络容量的极限在哪里?复杂网络的优化应该遵循怎样的准则?如果能够从更深、更广的角度来研究和发展信息理论,并以此为基础建立起涵盖高速移动、复杂干扰等场景的宽带无线通信网络重点理论体系,就能够应对上述挑战,解决无线通信网络中的一些基础性和关键性问题并为无线通信未来发展指明方向。

为了应对这些技术挑战,需要研究无线通信网络资源制约性能的规律、高效的网络传输机理和混叠信号可分离机理。这些问题相互衔接、密切相关,其中性能规律主要揭示高移动性条件下通信的性能极限和理论界,而传输机理和信号分离机理则从不同角度揭示了系统优化设计的基本原理与方法,以逼近理论界。由于移动通信系统中的干扰日趋丰富复杂、动态多变,现有将干扰视为噪声的方法没有充分利用干扰的结构化特征,所以需解决如何建立移动环境下的动态干扰模型和如何能够有效地利用干扰特性以实现性能提升的问题。

3 高移动无线通信的干扰特征

计算多用户高斯干扰信道的容

量区域是网络信息论的公开问题之一,目前仅解决了强干扰与弱干扰两种情况下的容量问题。但是无线宽带通信网络快速多变与复杂干扰环境使得无线电干扰形态呈现多样化,多用户、多小区和多网络之间都可能存在干扰;信号中继和邻近节点协作等会引入新的干扰;用户行为越来越复杂,对无线频谱的使用呈现很大的不确定性,使得网络干扰呈现动态性;高速移动场景下快变的无线宽带信道也使干扰形态更为复杂。如高移动宽带通信中多普勒频移产生的载波间干扰,频繁切换引起的小区间干扰,以及相对运动用户间的不对称干扰等。

因而我们必须在不同场景、网络结构和用户行为模式下,建立有效的干扰模型来分析和研究宽带无线通信网络的信息容量,探讨网络自由度对系统性能的影响,发展新的理论和方法应对干扰。

4 干扰抑制和协调

4.1 干扰抑制和协调中的问题

多输入多输出(MIMO)技术^[1]、空时编码技术^[2]、机会调度、Turbo码^[3]、混合自动重传请求(HARQ)、协作中继^[4]等技术的出现,使得信道衰落和加性噪声对通信系统造成的影响成为次要因素,而小区内、小区间和网络间的干扰上升为制约通信系统性能与容量提升的瓶颈。过去三十年里,不断涌现出了一些新颖的、应对通信干扰的关键技术和理论方法。采用码分多址(CDMA)/时分多址(TDMA)/正交频分复用(OFDMA)等多址技术可有效抑制多用户间的接入干扰^[5-9];广义自由度的概念可以帮助我们较为直观明了地分析干扰信道性能限;干扰对齐试图把所有干扰信号都“排列”在同一个子空间中来使有用信号拥有更多的自由度^[10];网络编码和协作通信可以通过多用户间的信号联合设计^[11],将用户间干扰

转化为有用信息的传输策略;博弈论以及机会式调度也是处理资源竞争条件下干扰问题的有效方法^[9]。然而,目前还存在很多问题需要探讨,主要包括:混叠信号可分离机理、现有抗干扰技术的有效性评估方法、干扰协调策略的设计指导准则、高速移动场景下新型抗干扰方法。

(1)混叠信号可分离机理

在复杂干扰场景下,任何通信节点接收到的信号都可能是多个无线电信号的叠加。为了从混叠信号中恢复出有用信号,必须深入研究混叠信号的可分离机理——混叠信号的可分离性原理与分离实现方法。更重要的是,混叠信号的可分离性原理也可以用适于指导无线通信信号的设计。

(2)现有抗干扰技术的有效性评估方法

在无线通信系统中,干扰的构成源于系统架构、频谱管理和分配策略、多址接入方式等因素。对于蜂窝移动通信系统而言,干扰主要来自于小区间;对于 Ad Hoc 网络而言,干扰主要是由多节点同时传输造成的信号重叠;对于无线局域网而言,子网间干扰是它的主要干扰形式。目前,尽管可以利用有效的多址方式、复杂的检测算法和用户协作等方法来对抗这些干扰,但如何从信息资源有效利用的角度在信息论层面评估它们的有效性目前尚缺乏必要的理论做支撑。

(3)干扰协调策略的设计指导的准则

现有的各种干扰协调方法均是以牺牲某种资源为代价来实现的,因此各有利弊。正交多址方式用容量换取了接收机复杂度降低;干扰对齐用反馈信道状态信息(CSI)的开销换取了自由度的提升;多用户多输入多输出用户协作和交换信道状态信息等开销换取了容量的提升;而在认知无线电中,则通过频谱感知与频谱动态接入的开销换取了频谱利用率的

提升。

因此,需要基于信息理论和混叠信号可分离机理,给出一定资源优化目标下的干扰协调策略设计准则,并以此为基础进一步研究应对复杂干扰的新理论与新方法。

(4)高速移动场景下新型抗干扰方法

高速运动的设备会在较短时间内历经多个复杂变化的电磁环境,由此引入的干扰具有快速时变特性,一方面会使得对干扰的估计和跟踪变得更为困难,另一方面由于信号时域相关性的降低,也为系统设计提供了额外的自由度。因此需展开适合高速运动场景的抗干扰技术研究,发现其内在的信息传输规律。

4.2 干扰抑制和协调的基本方法

总体来看,无线通信系统处理干扰的基本方法可以分为3类:第1种方法是利用正交化的方法避免干扰,如频分多址(FDMA)、时分多址(TDMA)、正交码分多址(CDMA)、正交频分复用(OFDM)以及机会式频谱接入等;第2种方法允许用户共享系统的所有自由度并把干扰完全当成噪声,如IDMA等;第3种方法是在允许用户共享系统的所有自由度的同时,利用干扰结构,在发送端、接收端(或同时)对信号与干扰进行一系列的联合处理^[10]。

在点对点的单用户传输中,通过多信道复用,单个用户可以使用多个并行信道提高传输速率。这种方式由于发射机和接收机的天线均为集中放置,因此可以通过发送与接收端信号的联合处理来提高容量,例如基于奇异值分解(SVD)的多输入多输出复用技术^[11]。

多用户广播信道,往往采用发送信号联合处理技术。预编码技术在发送端实现与信道匹配的预处理,可有效抑制多用户间干扰,通用的技术包括线性预编码技术(如迫零算法(ZF)、块对角化和最小均方误差

(MMSE)等)^[12]和非线性预编码技术(如 Tomlinson-Harashima 预编码(THP)、迫零脏纸编码(ZF-DPC)等)。污纸预编码(DPC)技术是另外一种重叠编码技术,适合于发送端已知干扰的信道信息,可用于逼近诸如多用户多输入多输出广播信道等容量限^[13-15]。

多用户多址接入信道,往往采用接收端联合信号检测技术。Verdu的工作加速了多用户检测理论的发展。蜂窝系统中的多基站协作可以看作是广播信道,此时发射及与接收均为分布式的,需要进行信息的交换以及预编码设计;而基于中继的传输则可以看成是点到点信道、广播信道和多址接入信道的组合,其复杂的网络结构使得发送、中继、接收端的处理技术以及资源优化分配策略变得更为复杂。

干扰对齐是一种新型的预编码方法,它把所有干扰信号都“排列”在同一个子空间中,使每个用户(在特定信道限制下)能获得接近1/2的自由度^[16]。干扰对齐的思想可以应用到上述各种干扰信道中,但有许多细节问题需要解决。例如,哪些数量的天线配置和自由度要求能够通过干扰对齐来实现,如何求解出需要的预编码和解码矩阵等。另外,对于3个用户以上的一般情况,目前只有次优的迭代求解方法。干扰对齐要求发送端确知信道信息,对于已知部分信道信息或有限反馈情况下的干扰对齐技术,目前我们还需要做进一步的研究。

4.3 干扰抑制和协调的研究内容

未来移动通信的发展要求增加网络的覆盖,提高传输速率,支持高移动性,同时要求容纳更多的用户,而用户密度的提高导致小区内、小区间和网络间的干扰日趋复杂,成为严重制约通信系统性能与用户容量提升的瓶颈。

目前,应对干扰的方法可以从干

扰信号分离、干扰避让、干扰博弈、干扰协调和干扰利用等多个角度展开,包括有效的多址接入方式、基于确定与统计特性的干扰分离方法,基于多用户分集的机会式调度算法,以及基于干扰对齐、预编码、协作通信等的干扰协调和基于网络编码的干扰利用技术。随着无线通信系统的发展,现有抗干扰理论面临着高频谱效率与多用户容量巨大需求、各种无线应用需求的多样化以及快速多变的复杂环境等多方面的挑战,需要发展新的抗干扰理论,包括:如何利用信号的不同特征区分不同用户,探索混叠信号的可分离机理与分离方法;如何设计高频谱效率、高用户容量以及低复杂度的新型多址接入方法;如何根据不同干扰环境的本质特征,以更合理地提炼干扰网络模型,并发展相应的“干扰避让”、“干扰协调”和“干扰利用”等一系列抗干扰理论和方法,以更好地适应复杂多变的无线干扰环境。

面向高速移动等快变复杂场景,需研究混叠信号的可分离机理与分离方法、新型多址接入理论、从干扰分离、干扰避让、干扰协调与干扰利用展开抗干扰理论与策略研究。主要内容如下:

- (1) 干扰分离机理与干扰避让方法
 - 混叠信号可分离机理
 - 基于正交多址的干扰避让理论与方法
 - 基于混叠多址的干扰分离理论与方法
 - 基于认知的网间干扰避让理论与方法
- (2) 新型抗干扰理论与方法
 - 基于干扰信道容量的抗干扰度量理论
 - 基于频谱共享的干扰博弈理论与方法
 - 基于网络的多输入多输出以及干扰对齐的相关干扰协调理论与方法
 - 基于物理层网络编码的用户

间干扰利用理论与方法

5 结束语

文章针对高移动无线通信场景干扰的多变性和复杂特性,讨论了高移动通信干扰应对物理层理论和方法,特别是从干扰避让、干扰抑制和干扰协调等层面,探讨了高移动通信干扰分离的机理和方法,并提出了需要研究的问题,为相关领域的研究人员提供参考。以上论述表明,物理层干扰应对方案是高移动通信干扰处理的主要方法,较之系统构架的优化更为基本,并可以给人们带来更大的系统增益。

参考文献

- [1] WANG Z, and CHEN W. Relay Beamforming Design with SIC Detection for MIMO Multi-Relay Networks with Imperfect CSI [J]. IEEE Transactions on Vehicular Technology, 2013, 62(8): 3774-3785
- [2] ZHU H, and CHEN W. Comments on a New ML Based Interference Cancellation Technique for Layered Space-Time Codes [J]. IEEE Transactions on Communications, 2010, 58(11): 3054-3055. doi: 10.1109/TCOMM.2010.083110.100001
- [3] WEI Y, JIANG M, XIA B, CHEN W, and YANG Y. A CRC-aided Hybrid Decoding Algorithm for Turbo Codes [J]. IEEE Wireless Communications Letters, 2013, 2(5): 471-474
- [4] TANG H, CHEN W, LI J, and WAN H. Achieving Global Optimality for Joint Source and Relay Beamforming Design in Two-Hop Relay Channels [J]. IEEE Transactions on Vehicular Technology, 2014, 63(9): 4422-4435. doi: 10.1109/TVT.2014.2311472
- [5] WEI L, and CHEN W. Optimal Upward Scaling of Minimum-TSC Binary Signature Sets [J]. IEEE Communications Letters, 2012, 16(2): 168-171. doi: 10.1109/LCOMM.2011.120211.111534
- [6] WU Q, CHEN W, TAO M, LI J, TANG H, and WU J. Resource Allocation for Joint Transmitter and Receiver Energy Efficiency Maximization in Downlink OFDMA Systems [J]. IEEE Transactions on Communications, 2015, 63(2): 416-430. doi: 10.1109/TCOMM.2014.2385705
- [7] ZHU H, LI B, and CHEN W. A practical and efficient algorithm for distributed interference alignment based on cognitive radio [C]//IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), Chengdu, China, 2010: 1-4. doi: 10.1109/WICOM.2010.5600120
- [8] WEI S, LI J, CHEN W, ZHENG L, and SHU H. Design of Generalized Analog Network Coding for a Multiple-Access Relay Channel

[J]. IEEE Transactions on Communications, 2015, 62(1): 170-185. doi: 10.1109/TCOMM.2014.2376954

- [9] SIDHU G, and GAO F, WANG W, and CHEN W. Resource Allocation in Relay-Aided OFDM Cognitive Radio Networks [J]. IEEE Transactions on Vehicular Technology, 2013, 62(8): 3700-3710. doi: 10.1109/TVT.2013.2259511
- [10] ZHANG M, YI H., YU H, LUO H and CHEN W. Joint Optimization in Bidirectional Multi-User Multi-Relay MIMO Systems: Non-Robust and Robust Cases [J]. IEEE Transactions on Vehicular Technology, 2013, 62(7): 3228-3244. doi: 10.1109/TVT.2013.2255898
- [11] ZHU H, CHEN W, LI B, and GAO F. An Improved Square-Root Algorithm for V-BLAST Based on Efficient Inverse Cholesky Factorization [J]. IEEE Transactions on Wireless Communications, 2011, 10(1): 43-48. doi: 10.1109/TWC.2010.110510.100555
- [12] WANG Z, and CHEN W. Regularized Zero-Forcing for Multiantenna Broadcast Channels with User Selection [J]. IEEE Wireless Communications Letters, 2012, 1(2): 129-132
- [13] COSTA M. Writing on dirty paper [J]. IEEE Trans. Inform. Theory, 1983, 29(3): 439-441
- [14] CARIE G and SHAMAI S. On the achievable throughput of a multi-antenna Gaussian broadcast channel [J]. IEEE Trans. Inform. Theory, 2003, 49(7): 1691-1706. doi: 10.1109/WCL.2012.022012.110206
- [15] WEINGARTEN H, STEINBERG Y, and SHAMAI S. The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channels [J]. IEEE Trans. Inform. Theory, 2006, 52(9): 3936-3964. doi: 10.1109/TIT.2006.880064
- [16] CADAMBE V R and JAFAR S A. Interference Alignment and degrees of Freedom of the K-User Interference Channel [J]. IEEE Trans. Inform. Theory, 2008, 54(8): 3425-3441. doi: 10.1109/TIT.2008.926344

作者简介



陈文,上海交通大学电子信息与电气工程学院责任教授、博导,信号处理与系统研究所所长,IEEE高级会员,上海市电子学会理事,中国电子学会信息论分会委员,IEEE通信学会通信理论委员,IEICE上海分会主席;主要研究网络编码、中继通信、MIMO-OFDM

系统和绿色通信;先后主持“973”课题、子课题、国家自然科学基金等20余项;在IEEE期刊发表论文60余篇,在IEEE国际会议发表论文100余篇,授权/申请专利20余项。

DOI: 10.3969/j.issn.1009-6868.2015.03.011

网络出版地址: http://www.cnki.net/kcms/detail/34.1228.TN.20150422.1640.001.html

对高铁宽带移动通信系统架构演进的思考

Evolution of Broadband Mobile Communication System Structures for High-Speed Railway

中图分类号: TN929.1 文献标志码: A 文章编号: 1009-6868 (2015) 03-0045-05

摘要: 探讨控制面与用户面分离的高铁移动通信系统网络架构设计, 以及相关的频谱融合和干扰协调问题。认为有别于公众移动通信系统, 高铁移动通信技术包括两个重要的技术指标: 传输性能和可靠性能, 目前正是开展高铁高可靠和大容量移动通信系统研究的最佳时期。相关研究表明, 对于未来高铁移动通信系统的高性能传输需求, 需要更多地在物理层之上设计有效的解决方案。

关键词: 高铁; 宽带移动通信; 5G; 架构; 频谱融合; 干扰协调

Abstract: This paper discusses decoupling of control plane from user plane, technologies for spectrum convergence, and interference coordination for high-speed railway (HSR) mobile communication systems. Unlike public mobile communication systems, HSR mobile communication systems have two important technical indexes: transmission performance and reliability performance. The author suggests furthering research highly reliable, high-capacity HSR mobile communication systems. Existing research shows that, to create high performance in future HSR, we should pay much more attention to efficient solutions in the physical layer.

Keywords: high-speed railway; broadband mobile communications; 5G; structure; spectrum convergence; interference coordination

方旭明/FANG Xuming

(西南交通大学信息科学与技术学院, 四川成都 610031)
(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

- 向具有 5G 特征的未来高铁移动通信系统演进需要提前布局
- 现有较低频率的优良频段已分配殆尽, 向未来高频扩展不可避免
- 如何从体系架构上适应高频段的扩展, 并保证高可靠和大容量需求, 是我们今后要大力开展的研究方向

随着中国装备制造业的快速崛起, 近年来高铁发展水平开始举世瞩目。尤其从“十一五”开始, 中国已成为世界上一次建成里程最长、运营速度最快的高铁国家。按照《综合交通网中长期发展规划》, 到 2020 年, 中国高铁总规模将达到 1.8 万公里, 将占世界高铁总里程的一半以上。高铁技术正逐渐成为中国走向

收稿日期: 2015-03-20

网络出版时间: 2015-04-22

基金项目: 国家重点基础研究发展 (“973”) 规划 (2012CB316100); 国家自然科学基金 (61471303); 铁路总公司科技研究开发计划重点课题 (61471303)

世界的一个国家品牌。与此同时, 另一个引以为傲的国家品牌是移动通信技术。如何保证并持续提升中国高铁的整体技术实力, 并借着移动通信技术向第 5 代移动通信 (5G) 演进的契机, 使中国高铁移动通信技术也跃上一个新的台阶, 这是我们从国家战略上必须思考和提前布局的问题。

客观地说, 目前世界范围内的高铁移动通信水平与公网移动通信水平相比还有较大的差距, 特别是旅客在高铁上移动互联网的服务体验是影响高铁形象的一个严重问题。主要性能指标如带宽、接通率、掉话率、

切换失败率等在高速移动场景下大大恶化, 其主要原因在于高移动性对移动通信带来了以下问题:

- 大多普勒频移扩展、大时延扩展和角度扩展
 - 信道快速时变、信道估计和信道预测困难
 - 隧道、山区、U 型槽等环境非常复杂
 - 高速切换、频繁切换和群切换等
- 值得庆幸的是, 以提升移动通信服务质量 (QoS) 为目标的 5G 关键技术的研究已经展开, 一些新的技术, 如基于云的无线接入网络和新型协

作网络架构,控制面/用户面(C/U面)分离的网络架构,通过毫米波、载波聚合或动态频谱分配的频谱融合技术均可能成为潜在的解决上述问题的手段。

此外,对于未来移动通信系统,无论是公用系统还是专用系统,带宽资源需求与频谱资源供给之间的矛盾日益扩大,如何在许可证频谱之外寻求更广阔的频谱资源?一个自然而然的思路就是利用认知无线电技术,在现有的非许可证频谱中寻求支持,合理地利用微波和毫米波频段的非许可证频段。

因此,考虑下一代移动通信技术的普适性,同时考虑未来高铁移动通信的需求和特点,需要开展基于5G关键技术的高铁移动通信系统关键技术研究。我们相信,开展上述问题研究符合国家的科技发展战略和重大需求,也符合通信产业发展的需要,有利于下一代移动通信网络和高铁相关的关键技术的突破。

1 高铁宽带移动通信现状及发展动态

1.1 与非许可证频段融合的移动通信研究现状

目前,传播特性良好的低频段已十分拥挤,为了满足未来移动通信系统中用户的海量带宽需求,运营商需要向拥有较宽连续频谱的高频频段甚至毫米波频段扩展。本研究提出聚合利用许可证频段与非许可证频段、毫米波频段的频谱融合技术。有别于传统的频谱聚合技术,这里聚合的成员频谱数量多、跨度大。因此,我们将其定义为频谱融合。

近年来,频谱聚合得到了学术界的高度关注与重视,并取得了一些研究成果。文献[1]概述了频谱聚合的发展现状、关键技术、技术挑战及发展趋势。文献[2]从认知理论出发,研究了一种基于用户带宽需求的频谱聚合策略,可以有效避免频谱碎片的

产生,同时减小终端复杂度,但文章中只研究了许可证频段的频谱聚合。文献[3]指出频谱聚合时需要考虑成员载波的带宽限制,但其仅分析了相近带宽聚合,没有分析载波之间的频谱距离。从现有研究现状看,现有研究成果主要还停留在许可证频段的频谱聚合,并且聚合的成员频谱跨度小,频谱特性差异较小,成员频谱数量和成员频谱带宽种类有限。对于聚合分布在许可证频段和非许可证频段的跨度更大、数量更多的成员频谱,会存在比传统频谱聚合技术中的衰耗差异更大、覆盖更不均匀、上下业务更不对称及切换频繁等一系列问题。

1.2 C/U分离的移动通信系统架构研究现状

随着安全列车视频实时监控、旅客移动互联网等业务需求的出现,未来高铁移动通信系统需要支持更大容量的传输。在移动网络的发展初期,高铁移动通信系统的主要业务形式是数据量较小的语音业务,通过同构网小区分裂技术便可以满足网络的容量需求,因此耦合的控制面与用户面架构并没有引起太多关注^[4]。然而随着移动用户的不断增加及数据业务的兴起,小区分裂导致的严重小区间干扰及较高的建网成本限制了同构网的发展。在异构网中,覆盖范围较小的低功率节点分布在宏基站的覆盖范围内,采用小区间干扰协调技术后,这种网络结构可以带来更大的传输容量^[5]。然而,用户在异构网中移动时会导致频繁的切换甚至重新接入,这不但影响了用户体验,也增加了网络的信令开销,这就是耦合的控制面与用户面架构在异构网中暴露的缺陷。根据文献[6],尽管现有的LTE/SAE系统架构已经在核心网中分离了控制面与用户面,然而在物理传输过程中这两个平面仍然是耦合的。文献[7-9]初步研究了高铁移动通信网络中控制面与用户面分离

的基本架构和切换问题。

1.3 基于频谱融合的移动通信系统架构研究现状

目前关于下一代云无线接入架构的研究都是针对公众移动通信场景,缺乏基于高铁移动通信场景的。然而上述问题也同样存在于高铁专用移动通信系统中,为了保障行车安全,列车之间存在发车时间间隔,即在某一时刻某一线路上的列车数目很少,这导致高铁专网基站的利用率很低。此外,对于基站间相互独立的网络架构,高速移动意味着频繁的越区切换,降低了无线传输的可靠性,严重威胁行车安全。因此,需要充分利用高铁移动通信系统的特殊性,研究基于该场景的云无线接入架构,并将铁路沿线的基带处理单元集中在一起,实现全局控制,这不但可以提高基站利用率、增强频谱融合灵活性,还可以通过灵活的资源配置实现群小区构造,降低切换流程复杂度,提高列控、列调信息的传输可靠性。目前,在这一领域还没有看到有显示度的成果。

1.4 高铁不同频段融合系统的干扰协调技术研究现状

最近,如何有效利用非许可证频段提高移动系统容量成为业界特别关注的一个问题。在非许可证频段的使用问题中,最重要的就是要解决占用非许可证频段的系统与其他使用非许可证频段系统之间干扰影响的问题。由于非许可证频段上干扰的发生在空域和频域上具有随机性,文献[10]提出了一种新的空间-频段上的干扰分析模型,文中假设在任何区域内以及任何频段上单位面积和单位频段上的干扰强度 $\lambda/\text{Hz}/\text{m}^2$ 服从泊松过程,为非许可证频段上的干扰分析提供了合理的数学模型。但是文中只涉及到干扰强度的检测,并没有分析干扰强度和许可证频段接入与退出的关系。文献[11]使用认知

无线电技术对可用非许可证频段进行感知与检测,并对系统接收端与发送端的作用进行了分析与研究,但是文献中提出的非许可证频段资源感知方法和流程在现有的通信系统中并不适用,需要进一步改进。因为非许可证频段为非授权特性,当通信系统使用该频段时,随时有可能由于被干扰而造成通信中断。文献[12-13]通过马尔科夫链定量分析了两个系统共用一个非许可证频段时因为相互干扰而造成的通信中断的概率,但是文中并没有针对干扰协调提出具体有效的解决方案。文献[14-15]采用一种新的帧结构,通过周期性地每一个无线帧内的前几个子帧进行频谱感应,随后在后面的子帧上根据频谱感应结果进行非许可证频段上的数据传输,避免非许可证频段上干扰的发生。但是文中的方案只适用于次用户占用其他系统许可证频段的场景。

2 高铁宽带移动通信研究方向和思路

2.1 非许可证频段与许可证频段的融合

未来移动通信系统将面临用户的海量带宽需求,带宽是个永恒的问题。高铁运行线路有一定的特殊性,即很多地段非许可证频段均空闲,但与传统认知无线电不同的是,这里合理使用非许可证频段不存在主从用户,所以不存在频谱的避让问题。因此,从扩大系统频谱和降低频谱使用成本考虑,在使用许可证频段的高铁公网或高铁专网移动通信系统中融合非许可证频段是非常有意义的。但是具有较大频谱间隔并包含毫米波段的多段频谱融合利用在理论和技术上还存在许多挑战。建议相关人员可以分析高频非许可证频段在高速移动场景下的信道特性和适用条件,研究解决高频偏、高衰耗、高频切换、车体穿透损耗等关键技术问

题,使融合非许可证频段与许可证频段的频谱能适应高铁场景,解决未来高铁无线通信系统中用户的海量带宽需求。

对于高铁场景下非许可证频段与许可证频段的融合,其主要问题是非许可证频段与许可证频段不连续,及各段频谱存在信道特性不一、传播损耗差异大、容量不等、多普勒频移相差很大等问题,要在这些谱段上传输一个完整的信息流,需要解决如何将信息流在有一定频率间隔的频段上进行高效的调度分发以及如何将从各个频段上接收到的信息流进行可靠汇聚,从而达到连续谱传输的效果。由于融合频段的总频谱宽度和跨度较大,建议相关人员可以对各谱段在物理层进行独立的编码调制,并在链路层进行信息流的高效调度和可靠汇聚。具体建议包括:

(1)针对高铁场景非许可证频段与许可证频段融合信道的估计进行研究,即根据高铁场景下位置和速度可先验获取等特点,估计不同频段在给定位置的信道特征、多普勒频偏、本地频谱政策、频谱利用状态等。

(2)针对非许可证频段与许可证频段信道特性的差异,设计速率适配机制。对于非许可证频段与许可证频段的跨频段融合,如果各成员频谱分配相同的功率,由于高频成员频谱的信道衰减大于低频成员频谱,高频成员频谱的覆盖范围则会小于低频的,以至于小区不同位置的用户可以调度的成员频谱数目不同。因此,需要在融合环境下,研究适当的功率适配机制,使得融合后的各成员频谱具有近似的覆盖范围。

(3)针对需融合的频段宽度和跨度较大的情况,设计高效可靠的调度和汇聚策略,即研究如何将信息流在有一定频率间隔的频段上进行高效的调度分发以及如何将从各个频段上接收到的信息流进行可靠的汇聚,从而达到连续谱传输的效果。

(4)研究高铁场景非许可证频段

与许可证频段融合的自适应控制机制。即针对非许可证频段与许可证频段的跨频段融合具有传输特性和成员频谱可用状态动态变化的特点,设计合理的自适应控制机制,适应各成员谱段的动态特性,并进行自适应调度及功率和速率适配,从而充分利用可能的分集增益来提高各成员频谱融合传输的容量和可靠性。

2.2 C/U面分离的高铁移动通信系统架构

考虑到在异构网日趋密集化的现状下,耦合的控制面与用户面架构已暴露出的问题,未来高铁5G系统在提高网络传输容量进行不同频段融合时,应考虑将重要的控制面甚至列控与列调用户面信息与传统意义上的用户面信息解耦设计,合理利用GSM-R系统中的现有带宽,均衡不同频段的差异,对系统频段弹性设计。为此,必须研究高铁移动场景下基于分离的控制面与用户面架构。具体研究包括:

(1)控制面与用户面解耦架构的研究,即基于现有在功能上控制面与用户面已分离的LTE/SAE架构,再进一步研究如何在物理传输上彻底分离控制面与用户面。

(2)基于解耦架构的频谱融合研究,即通过解耦的控制面与用户面架构将拥有较宽连续频谱的高频频段与GSM-R遗留的、拥有良好传输特性的低频频段融合。由于控制面信息甚至列控、列调用户面信息对传输可靠性要求较高,可以由拥有良好传输特性的宏小区有限低频频带来承载;旅客业务的用户面对传输容量需求较高,可以由拥有较宽连续频谱的小小区高频频段承载,即将控制面与用户面根据各自的需求放置在拥有不同特性的频段传输,并在频域上分离两个平面,均衡不同频段的差异。

(3)解耦架构对信息传输可靠性影响的研究。在解耦架构中,列控、列调信息及旅客业务的控制面信息

仍由原有的、传输特性良好的低频频段承载,因此保持着原有的传输可靠性。但由于旅客业务的用户面数据被转移到了高频频段,需要联合考虑旅客业务的控制面及用户面的频谱传输特性来分析解耦架构对旅客业务传输可靠性的影响。

(4)新型帧结构的设计,即研究解耦架构下的信道映射及物理帧结构。在解耦架构中,由于控制面与用户面在物理上就被分离到了不同的小区基站,因此两个平面在信道映射过程中是完全分离的,在无线传输过程中两个平面也将占用帧结构的不同资源位置。

2.3 与现有 LTE/LTE-A 系统兼容

对比公众移动通信场景,高铁移动通信系统存在很多特殊性,这给 5G 无线通信技术如云无线接入架构的实施和应用带来一些优势。基于此,我们需要研究基于频谱融合的与现有 LTE/LTE-A 系统兼容的网络架构,具体包括:

(1)高铁场景下云无线接入架构的研究。通过将全部铁路沿线基站的基带处理单元(BBU)集中到统一的 BBU 池,实现对资源的全局控制和分配,这样不但可以提高处理资源的利用率、增强频谱融合的灵活性,还可以简化远端射频单元(RRU)的结构和功能,降低网络升级及演进成本。此外,我们可以考虑在回传网段采用技术日渐成熟的毫米波实现频谱融合,节约光纤,增强布网灵活性。

(2)基于云接入架构的群小区构造方法研究。云无线接入架构集中了全部的处理资源,可以实现灵活的资源配置,当列车需要从服务 RRU 切换到目标 RRU 时,通过将目标 RRU 的处理资源配置到当前服务 RRU 的 BBU 中,即将两个 RRU 构造为一个群小区,就可以避免复杂的切换流程,降低切换耗时,提高列控信息的无线传输可靠性。

(3)切换信令及流程的设计,基

于(1)和(2)研究云无线接入网络架构下的群小区构造方法,并设计相应的切换信令流程。

2.4 多频段干扰协调

我们需要研究评估公网系统和高铁专网系统在占用非许可证频段之后对现有非许可证频段的系统的干扰影响,以及非许可证频段的公网系统和高铁专网系统的干扰影响,还需要研究非许可证频段感知方法、适用条件、退出机制等等,以及在使用两类不同频段时的干扰协调方法。

由于非许可证频段为无需授权的公共频段,所以接入非许可证频段后的高铁专网系统与其他使用该非许可证频段系统之间存在干扰问题,这直接影响在非许可证频段上进行通信传输的可靠性。干扰协调方案主要包括 3 个方面:接入及退出机制、可用非许可证频段资源感知方法,以及非许可证频段资源分配方案。这三者之间相辅相成,缺一不可。只有制订了合理的非许可证频段接入及退出机制,才能保证接入可用非许可证频段进行通信时不会受到其他系统的干扰,同时在已接入的非许可证频段上受到其他系统的强干扰时,及时退出该频段以保证通信的可靠性;只有采用更加有效的可用非许可证频段资源感知方法,才能使下一代高铁移动通信系统正确地感应到可用的非许可证频段;相应地,设计更加合理的非许可证频段资源分配方案,才能使有限的非许可证频段得到高效的使用,为系统带来更高的吞吐率。具体包括:

(1)接入及退出机制。通过频谱感应技术对非许可证频段上信道进行干扰强度检测,假设信道是系统进行频谱分配的最小单位(如在长期演进系统中,信道为子载波间隔,宽度为 15 kHz)。接入及退出机制的制订中需要设定合理的干扰门限,干扰门限是在保证该信道通信质量的条件下所能容忍的最大的干扰能量限

度。若检测到还未接入的非许可证频段信道上干扰强度小于干扰门限,则该信道为可接入信道;若检测到已接入的非许可证频段信道上干扰强度高于干扰门限,则该信道已不能进行有效通信,系统应退出该信道。

(2)可用非许可证频段资源感知方法。在实际的通信系统中,频谱感知只能在接收端进行,接收端通过频谱感应检测到可接入非许可证频段资源,并反馈给发送端。发送端根据接收端的反馈指示,在相应的非许可证频段信道上进行信息的发送。具体过程如图 1 所示。

在接收端,系统通过频谱感知检测非许可证频段信道上的干扰强度。并根据自身的接入及退出机制,将不同非许可证频段信道上的干扰强度与干扰门限相对比,选择出可利用的非许可证频段信道。随后,通过反馈信道将可利用的非许可证频段信道发送给发送端,同时需要将各个可利用非许可证信道的干扰强度发送给发送端,作为发送端进行非许可证频段资源管理与分配的指标依据。发送端接收到接收端发送的反馈信息后,通过自身的非许可证频段资源分配方案选择非许可证信道对接收端进行数据发送。由于非许可证频段上干扰的发生在时域以及频域上都具有随机性,所以系统需要周期性地对非许可证频段上的无线环境进行感应以及评估。但是在实际通信中,上行的接收端为基站,发送端为移动台;而下行的接收端为移动台,发送端为基站。由于手持移动台功能上的限制,上行和下行可用非许可证频段资源感知的过程不同。

(3)非许可证频段资源分配方案。小区内不同位置的移动台会受到不同频段、不同强度的干扰,所以不同位置上的移动台频谱感应到可利用非许可证频段也会不同。一个移动台可能会感应到一个或多个可用非许可证频段信道。当拥有多个可用非许可证频段信道时,其中部分

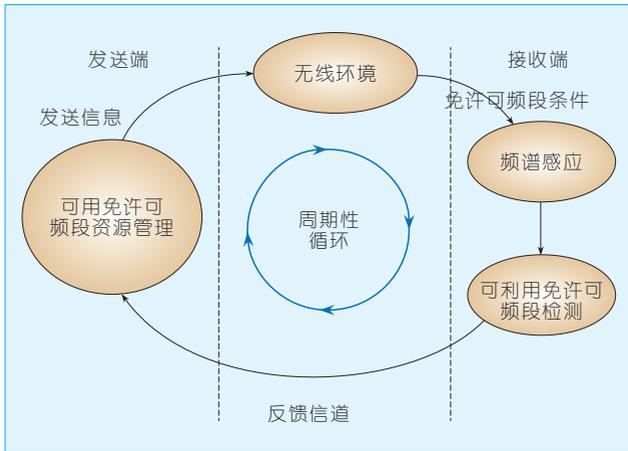


图1
非许可证频段资源感知
及利用循环

非许可证频段信道对于其他移动台一样可用,在这种情况下,基站只有合理地分配和管理这些非许可证频段的信道,才能有效提升系统容量。

3 结束语

文章探讨了高铁5G系统研究中的前瞻问题,特别从架构及相关的频谱融合和干扰协调等方面探讨了其中涉及的关键技术问题及解决思路。对于未来高铁移动通信系统干扰消除和提升系统可靠性,如果采用控制面与用户面分离的架构,再辅之于物理层上的多点协作传输等技术,应该比单纯在物理层上抗干扰处理更加有效。以上研究思路和经验可以为相关领域的研究人员提供参考。

参考文献

- [1] WANG W, ZHANG Z, and HUANG A. Spectrum Aggregation: Overview and Challenges, Network Protocols & Algorithms [J]. Home, 2010, 2(1): 184–196. doi: http://dx.doi.org/10.5296/npa.v2i1.329

- [2] LI J, TAN Z, TAO C, et al.. A new spectrum aggregation algorithm for IMT-Advanced based on cognitive science [C]//International Conference on Wireless Communications and Signal Processing (WCSP), 2010
- [3] RATASUK R, TOLLI D, and GHOSH A. Carrier aggregation in LTE-Advanced [C]//IEEE Vehicular Technology Conference (VTC 2010-Spring), 2010
- [4] MACDONALD V H. Advanced mobile phone service: The cellular concept [J]. Bell System Technical Journal, 1979, 58(1): 15–41
- [5] LOPEZ-PEREZ D, GUVENC I, et al.. Enhanced intercell interference coordination challenges in heterogeneous networks [J]. IEEE Wireless Communications, 2011, 18(3): 22–30. doi: 10.1109/MWC.2011.5876497
- [6] BEMING P, FRID L, HALL G, et al.. LTE-SAE architecture and performance [J]. Ericsson Review, 2007: 98–104
- [7] YAN L, FANG X, and FANG Y. Control and data signaling decoupled architecture for railway wireless networks [J]. IEEE Wireless Communications, 2015, 22(1): 2–9. doi: 10.1109/MWC.2015.7054725
- [8] YAN L, and FANG X. Reliability evaluation of 5G C/U-plane decoupled architecture for high-speed railway [J]. EURASIP Journal on Wireless Communications and Networking, 2014, 2014: 127. doi: 10.1186/1687-1499-2014-127
- [9] SONG H, FANG X, and YAN L. Handover scheme for 5G C/U plane split heterogeneous network in high-speed railway [J]. IEEE Transaction on Vehicular

Technology, 2014, 63(9): 4633–4646. doi: 10.1109/TVT.2014.2315231

- [10] SHOBOWALE Y M, and HAMD K A. A unified model for interference analysis in unlicensed frequency bands [J]. IEEE Transactions on Wireless Communication, 2009, 8(8): 4004–4013. doi: 10.1109/TWC.2009.070276
- [11] HAYKIN S. Cognitive radio: brain-empowered wireless communication [J]. IEEE Journal on Selected Areas in Communications, 2005, 23(2): 201–220. doi: 10.1109/JSAC.2004.839380
- [12] JIANG X, ZHANG Y, and WONG K. On partial spectrum sharing of two licensed networks using cognitive radios [C]// Vehicular Technology Conference (VTC Spring), 2011:1–5. doi: 10.1109/VETECS.2011.5956444
- [13] ZHU X, SHEN L, and PETER T. Analysis of cognitive radio spectrum access with optimal channel reservation [J]. IEEE Communication Letters, 2007, 11(4): 304–306. doi: 10.1109/LCOM.2007.348282
- [14] STOTAS S, and NALLANATHAN A. Enhancing the capacity of spectrum sharing cognitive radio networks [J]. IEEE Transactions on Vehicular Technology, 2012, 60(8): 3768–3779. doi: 10.1109/TVT.2011.2165306
- [15] JIANG X, WONG K, and Y. Zhang. Imperfect spectrum sensing for partial spectrum-shared licensed networks [J]. IET Communications, 2012, 6(17): 2894–2899. doi: 10.1049/iet-com.2012.0065

作者简介



方旭明,西南交通大学信息科学与技术学院教授、博导,通信工程系主任,移动通信省重点实验室、信息编码与传输省重点实验室副主任,IEEE车辆技术成都分会主席,省通信学会无线通信专委会副主任,《IEEE车辆技术汇刊》编委;主要从事轨道交通车地无线通信系统、下一代移动通信系统研究;先后主持或主研“863”计划、“973”计划、自然科学基金等项目60余项;发表研究论文260余篇,完成发明专利20余项,提交国际标准提案7项,主编或参编专著、译著、教材等9部。

综合信息

2019全球IP流量预计将达2 ZB 视频占80%

近日,IPTV News援引思科《可视网络指数(VNI)预测》第十年报告指出:2014—2019年,年度网络IP流量将增加两倍,达到历史性的2 ZB。

视频服务的增长是推动流量增长的因素之一。到2019年,视频将占据IP流量的80%,而2014年,占比仅为67%。高级视频服务(如超高清、球面/360度视频)

以及不断增长的以视频为中心的M2M应用将为服务提供商创造新的宽带及可扩展性需求。高级视频服务的质量、便捷度等成为成功与否的关键因素。

思科预测,到2019年,全球每月的IP流量将由2014年的59.9 EB增至168 EB。预计2019年全年的网络流量相当于先前整个互联网时代(1984—2013年)的流量总和。(转载自《中国信息产业网》)

对无线新技术演进思考

Evolution of Wireless New Technologies

向际鹰/XIANG Jiyong

(中兴通讯股份公司, 深圳 518057)
(ZTE Corporation, Shenzhen 518057,
China)

1 5G 的使用场景

随着移动宽带网络的发展,人们对任何场景下的全连接、扩展场景下的连接、扩展载体的连接需求越来越强烈。第4代通信技术(4G)作为针对移动手持终端和高速数据上网而优化的制式,在满足全场景应用时存在一些天然的缺陷,例如:海量、低耗电量的物联网连接,超低时延的连接(支持实时游戏、车联网)等。而超密集用户群,高质量的数据连接,新数据载体例如虚拟现实终端的需求,以及移动家庭办公所需的快速数据容量提升,这些都是目前的4G所无法满足的。因此,人们对第5代移动通信技术(5G)充满了期待。5G新场景的愿景如图1所示。

2 5G 技术及 Pre5G 概念

我们一般认为,5G的商用将在2020年以后,目前业界对于5G尚缺乏统一的、标准的定义,但一般都认为5G将不再基于单一的关键技术(如3G的码分多址(CDMA)、4G的正交频分复用(OFDM)/多输入多输出(MIMO))等,而将基于一系列技术

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868(2015)03-0050-05

摘要: 介绍了中兴通讯对未来无线新技术走向的整体看法。认为现有的5G候选技术仍然是在传统空间、时间、频率3种自由度的基础上做增强。而在这些增强中,需要尤其关注一些无须改变4G空口就可以直接使用的5G技术,例如大规模多输入多输出(MIMO)、超密网(UDN)等。还认为所有无线新技术都将持续演进。随着5G标准的制订,用户体验将得到本质的提升。

关键词: 多用户共享接入;超密网;大规模MIMO

Abstract: An overview of wireless new technologies over next few years is given. The candidate technologies for 5G are being enhanced in terms of time, frequency, and space diversity. We should focus on 5G technologies that can be used directly and do not require the 4G port to be changed. Such technologies include massive multi-input multi-output (MIMO) and ultra dense network (UDN). As the evolution of the technology, the user experience will be greatly improved in term of throughput and latency.

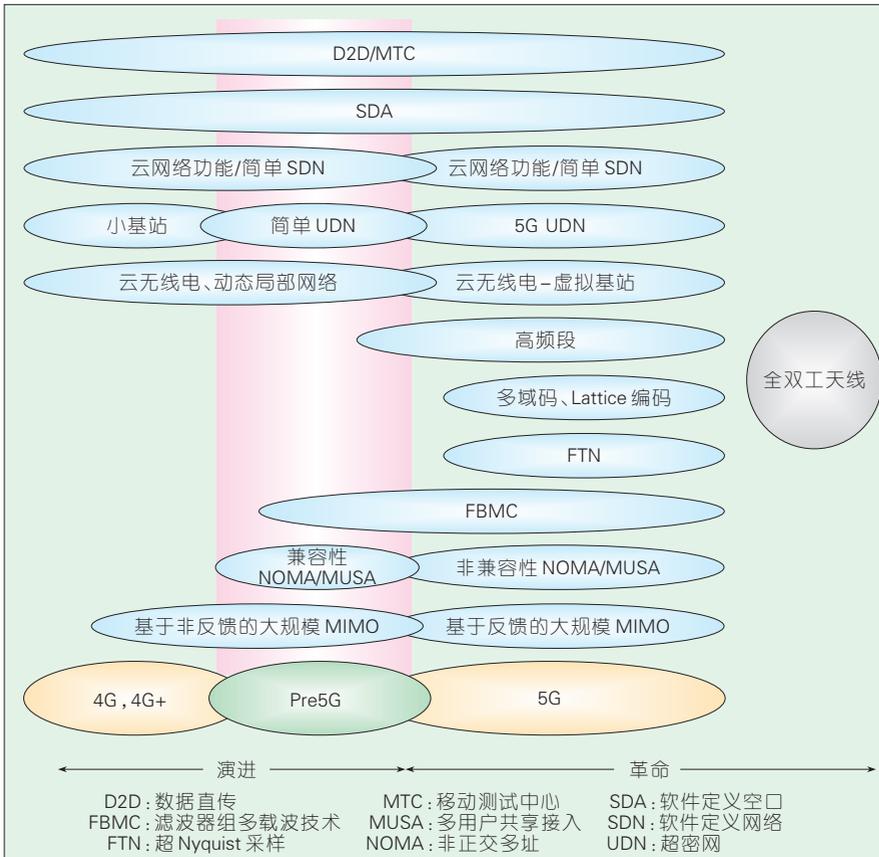
Keywords: multi-user shared access; ultra dense network; massive MIMO

(又称为技术簇),如图2所示。这样的技术簇,目前至少包括大规模MIMO、超密网(UDN)、高频技术,多用户共享接入(MUSA)以及协同组网技术。同时,5G还可能包括一些当

前有争议的技术,例如超Nyquist采样(FTN)、滤波器组多载波技术(FBMC)以及多元域编码等。同时,5G将是一个融合多种无线接入技术(包括现有技术研究和革命性的新技



▲ 图1 5G新场景愿景



▲图2 5G技术演进

术),并包括软件定义网络(SDN)、网络功能虚拟化(NFV)核心网的智能化网络^[1]。

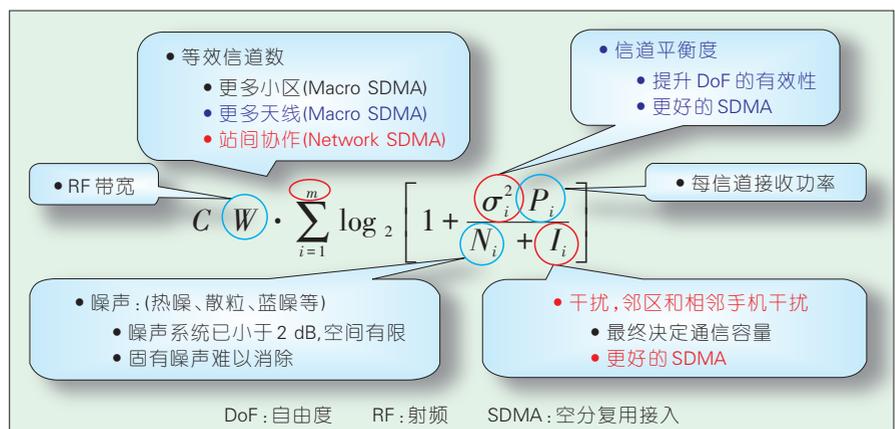
我们把无线新技术大致分为3类:原理性革命技术、革命型技术、演进型技术。其中原理性革命技术在5G的早期阶段研究得比较多,有很多相关技术被提出,这些技术多数宣称可以在传统的自由度(DoF),即时间、空间、频率之外发现新自由度类型,从而从根本上成倍提升通信性能。然而经过进一步理论研究后发现,上述技术本质上并没有创造新的自由度,而是原有的传统自由度的数学变型,因此在本质上不可能带来容量的提升。

一些技术理论宣称可以大幅度超越香农极限,经过研究我们一致认为:香农极限是超越具体技术的一个普适公式,类似于通信界的能量守恒定律,所有的技术都不可能超越香农

极限^[2]。

另外我们应当看到,所有5G候选技术都是经典电磁学理论范围内的技术。非经典电磁理论范围的技术并不在5G时间窗内。

经过空间多信道扩展之后的香农公式如图3中所示。根据上述公式,理论容量极限主要取决于以下6



▲图3 通信容量的制约因素

个因素:

- 更宽的带宽(W)。在5G中,带宽将向高频毫米波扩展。
- 空间信道数(m)。可通过更多物理小区(物理空分,如5G超密网即超空集网络)。或更多天线(逻辑空分,如5G大规模MIMO)来提升空间信道数。
- 空间平衡度。可通过更好的空分算法保证空间平衡度,并确保各个空间信道尽可能正交,从而最大程度地提升通信容量。
- 功率(P)。可适当提升功率,但功率的提升是有限的,因其有成本、体积、电池寿命等因素约束。
- 噪声(N)。主要是热噪,由于热噪声只与环境温度有关,因此无法减少其对通信性能的影响。
- 干扰(I)。与噪声不同,干扰是人为产生的,例如不同用户间的干扰,不同小区之间的干扰等。干扰具有有色性、方向性、空间选择性,这些都是我们加以利用的已知信息,通过这些已知信息,我们可以有效地降低干扰,甚至把干扰的能量利用起来为我们服务。

由此可见,在未来5G新技术中,更好的空分(包括物理空分和逻辑空分)和干扰抑制技术是关键。几乎所有的5G关键技术都是围绕这两点开展研究的。

无线新技术中的革命性技术,是指相对来说对空口改动较为巨大,但

仍然基于传统自由度(空、时、频)的技术;而演进型技术是指基于目前的通信手段,做一些局部增强之后形成的技术。

对于某项技术到底是演进型还是革命型,业界有着不同的观点。中兴通讯则认为这一现象是正常的,因为大多数5G核心技术都介于演进与革命之间的边缘地带,而演进与革命其实是个主观判断,因此会存在不同观点。

为绕过“演进、革命”之争,我们从标准和实现角度,把落入5G时间窗内的技术又分为3类:4G或4G+中已有的技术;介于4G和5G之间阶段的技术,如中兴通讯提出的Pre5G技术;5G技术,相对于4G标准来说改动比较大的技术。

Pre5G技术是由中兴通讯提出的,它包含4个要素:它一定是采用5G的技术;能够带给用户远远高于4G,接近于5G的用户体验,例如成倍的吞吐率提升,成倍的延迟降低等等;商用时间点远远早于2020年;可以基于现有空口,甚至直接采用4G终端。

根据Pre5G的上述特征,我们可以较为清楚地了解Pre5G和4G+、5G之间的区别。Pre5G的性能明显超出4G+标准中的定义性能,并且不需要依赖5G的标准中定义的性能。因此,即使标准中不出现Pre5G的阶段,也会在实现层面上出现一个介于4G+和5G之间的Pre5G阶段。属于Pre5G阶段的技术有非反馈模式的大规模MIMO、MUSA以及UDN的一部分技术。

大规模MIMO是5G中最重要的一项核心技术之一,甚至可以说是唯一成倍提升频谱效率的技术(其他多数技术只提升空间利用效率,例如更密集地建站,使用更多的频谱资源等)。大规模MIMO的天线数量大幅高于4G,有上百根之多,通过更多的天线之间的联合发送接收可以提升系统的容量和覆盖^[1]。

原理上,大规模MIMO主要有两个方面的作用:对广播信道可以形成半动态的针对性覆盖,而传统天线只能形成静态的覆盖,因此大规模MIMO的覆盖更好,更有针对性;对业务信道(PDSCH),可以形成完全动态的数字波形,从而可以大幅度提升小区容量。

仿真表明,相比于8天线,容量提升达到4~6倍之多,这是以往任何技术不能达到的。一般认为,有100倍左右的容量提升来自于更多小区和更多的频谱,只有8~10倍来自于频谱效率的提升。因此可以说大规模MIMO的采用,使频谱效率的体验迅速达到接近5G的水平^[2]。

大规模MIMO的采用使天线的端口数从传统的8个,提升到接近甚至超过100个。当天线数增加到上百个时,采用4G传统的信道反馈机制必然产生大量的开销,甚至仅仅参考信号(RS)就能占到整体资源的80%以上,为此,5G中针对信道反馈做了大量研究,达成的一个共识是:必须大幅度修改4G的信道反馈机制。进一步研究表明,在时分双工(TDD)模式下,可利用上下行对称性,通过上行的信道估计进行下行信道预测,从而在不增加反馈通道的情况下,支持上百个通道的信道测量。相比于直接反馈模式,这种方式的性能更优、更快。

2014年11月,中兴通讯联合中国移动完成了全球首个时分双工长期演进(TD-LTE 3D)/大规模MIMO基站的预商用测试。该测试由中国移动研究院发起和组织,采用中兴通讯最新研制的64端口128天线3D/大规模MIMO的基带射频一体化室外型基站。本次测试重点验证了3D/大规模MIMO对高层楼宇的全面深度覆盖的能力。

在现网中,普通的8天线垂直方向波束固定且垂直覆盖角度较小,使得高层深度覆盖差、高层干扰大、终端接收信号与干扰加噪声比(SINR)

和吞吐率低,导致高层用户体验差,这已成为运营商面临的一大难题。3D/大规模MIMO天线则具有3D波束赋形能力,本次测试表明3D/大规模MIMO基站可全面深度覆盖35层的高层办公楼,且其数据吞吐率远远优于8天线基站,其中在35楼,其数据吞吐率是8天线基站的3.36倍。该测试证明3D/大规模MIMO是一种解决高层覆盖的良好技术,仅用一个站即可解决传统基站多个站才能解决的问题。

2015年1月,中兴通讯又完成了首例外场多流、多用户测试。实测表明,多流、多用户可以在同一时间段、同样的频点同时传输数据,而几乎互相不发生干扰。即使两个用户非常靠近,也不会互相干扰。无论在室外视距环境下,还是在室内散射环境下,都可以观察到这样的空分效果。测试标志着中兴通讯Pre5G和大规模MIMO的理论正确,并已经接近商用,向5G迈出坚实一步。

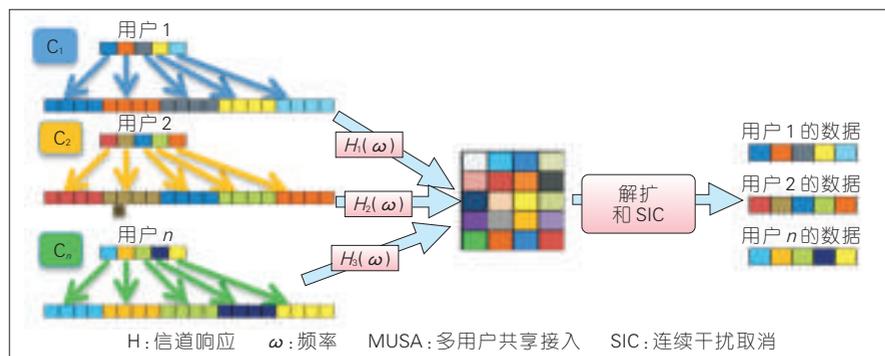
UDN也是5G另一项关键技术。在标准研究组中,人们研究了6种典型的UDN应用场景,例如体育馆、车站、大型办公楼等,都属于超密场景。

在4G中,小基站的数量仍然比较少,因此4G中,涉及小基站的技术更多的是关注与宏网之间的干扰(Hetnet),而没有太关注小基站间的干扰。5GUDN部署超密,因此小基站间的干扰成为主要矛盾。中兴通讯通过研究发现:小基站间的干扰抑制,在原理上可以沿用中兴通讯在4G宏网中的提出的Cloud Radio技术。我们从而可以认为5GUDN技术是中兴通讯4G Cloud Radio的一个自然演进。

这是因为,本质上Cloud Radio间的干扰与Macro-Macro干扰一样,属于同构网组网问题。中兴通讯将Cloud Radio向UDN演进,提出了虚拟基站技术。传统的小区是物理小区,基站ID用于标识小区,UE的所有通信均基于基站ID。而在虚拟基站中,

基站 ID 变得不重要甚至消失,由网络动态生成针对特定用户的“UE ID”,在用户看来,感知上等同于有一个虚拟的逻辑站点一直跟随自己的移动,因此业务的平滑性等都有大幅度提升。

MUSA 是中兴通讯提出的一项 5G 技术。传统的通信技术(例如 4G),都是采用“正交”的方法区分用户,也就是说,不同的用户分配不同的自由度(时间、子载波、或空间),两个用户不能共享同一自由度。而 MUSA 则为每个用户分配一个码序列,然后把这些用户分配到同一个自由度上(时间、子载波、或空间)。与传统的 3G 码分多址不同,MUSA 为用户分配的码可以是不能正交的,只能起到扩频的作用。那么在同一个自由度上,如何区分不同用户的信号?就需要借助于连续干扰取消(SIC)接收技术,例如对于两个用户,一个远一个近。远的用户需要被分配更多的功率,因此对近的用户干扰非常大。常规的接收机不能很好地处理这种情况,非线性的 SIC 接收机可以先解出远端用户的数据,进行干扰消除,从而顺利解出自己的数据。表面上看用户获得了额外的数据,但是并不违反通信规律,只是使数据的流量分配更为均衡。例如,传统通信方法只能在完全牺牲远端用户的情况下获得最大系统容量,但 MUSA 则可以在一个相对较宽松的条件下,保证较大的系统容量,同时保证用户之间的均衡性。



▲图4 MUSA 技术

目前关于非正交通信的研究很多,中兴通讯 MUSA 在复杂度可控的情况下,显著提升性能。另外,由于如图 4 所示的码域方法,可支持大量用户接入,而且由于非正交检测原则上不需要同步,有利于提升电池寿命,因此 MUSA 的上行技术非常适合于移动测试中心(MTC)物联网的一系列相关应用。

此外,中兴通讯几年前投入巨资开发 4G 矢量处理器芯片,由于该芯片平台具有灵活的可软件扩展架构以及超强的处理能力,所以能够在硬件不变的条件下,只简单地调整指令集,就可以更好地满足 Pre5G 甚至 5G 的要求。

3 其他 5G 技术

大规模 MIMO 在 Pre5G 阶段,主要基于 TDD 信道对称性,采用非反馈模式;而到 5G 阶段,它可以不依赖于信道对称性,采用反馈模式。中兴通讯在 5G 大规模 MIMO 技术中,主要研究反馈信息的压缩感知,并取得了不少成果。简单地说,压缩感知就是利用信道在时域、频域、空域上的稀疏性,对 RS、PMI 等信息进行压缩和还原。从而在可以接受的开销下,传送上百个天线的信道信息。

对于高频通信,由于衰落特点、多径特点不同,空口定义需要进行相应调整,例如为了适应更大的多普勒频移,我们需要采用更宽的子载波。相应地,子载波数减小,符号减少,循环前缀(CP)也需要有所减少。中兴

通讯针对高频空口作了深入的分析,已经提出一些提案供业界讨论。有一种观点认为,高频虽然路损大,但天线尺寸小,因此可以补偿路损。中兴通讯则认为,衰减因子 n 往往大于 2,因此天线数量上的优势并不足以弥补路损。还要考虑到在相同面积下,天线数量需要按平方数增加,由此带来平方倍的复杂度。所以在以覆盖为目的的应用场景下,仍然是尽可能低频,即使是传统的大于 6G 的高频,也需要尽量地选择靠近 6G 的一些频谱。

面对 5G 的核心需求,传统链路自适应技术已经无法满足其发展,而新的编码调制与链路自适应技术可以显著地提高系统容量,减少传输延迟,提高传输可靠性,并增加用户的接入数目。中兴通讯提出了软链路自适应(SLA)、物理层包编码(PLPC)、吉比特超高速译码器技术(GHD)等。

SLA 技术提高了信道预测和反馈方法的准确性,解决了开环链路自适应(OLLA)的周期较长、干扰突发对性能的影响,以及 5G 各种新场景对服务质量(QoS)的差异化需求(低延迟或超可靠或高吞吐量或高速移动)等问题。

物理层包编码技术可以有效地解决大数据包与小编码块之间的矛盾。GHD 技术可以显著地提高单用户的速度,满足 5G 需要支持超高速用户数据速率的要求。

传统电信网络专用设备较多,相比 IT 网络则存在着更高的建设费用,更庞杂的运维开支和更封闭的业务形式,使运营商在“收”、“支”两端都面临窘境。近几年兴起的 NFV 和 SDN 技术让运营商看到了曙光。

NFV 的技术基础是虚拟化技术。虚拟化技术提供了将一套服务器的相关资源(如计算、存储和网络)虚拟化成多个不同虚拟机并为不同的用户使用的手段。在电信网络中引入虚拟化技术,可以实现电信网络

硬件资源的共享,提升硬件资源的利用率,也为快速引入第三方新业务开启了一道方便之门。电信网络功能本身支持虚拟化后,与专用硬件设备解除了耦合关系,使得电信网络采用IT化、通用化硬件资源成为可能,有利于运营商降低硬件采购成本。

SDN 技术源于 IP 网络的路由控制,它通过将路由设备的控制和转发相分离,将网络中大量路由器繁杂的路由配置工作转化成通过控制器集中式配置并下发到转发面执行的方式,极大简化了网络路由维护工作。同时 SDN 还可以通过开放北向接口使第三方应用方便地控制网络中的业务路由。

在电信网络中引入 SDN 技术,不但可以提升网络部署的自动化能力,实现基于业务的灵活组件调度,同时通过在移动网络节点(如 SAE GW)内

部引入 SDN 化理念,还可以有效促进整个网络的扁平化,提升报文转发的效率。

4 结束语

文章综述了未来可能得到应用的 5G 候选技术,并从理论上分析了上述技术取得提升的原理,重点分析了一些不需要依赖于空口改动的 5G 技术。这些技术可以提前在 4G 的时间窗内进行部署。同时对于其他 5G 技术,也进行了简要介绍。认为现有的 5G 候选技术仍然是在传统空间、时间、频率 3 种自由度的基础上做增强。而在这些增强中,需要尤其关注一些无须改变 4G 空口就可以直接使用的 5G 技术。

参考文献

- [1] LUO F L. Signal Processing Techniques for 2007. 40th Annual Hawaii International Conference on System Sciences, 2007. HICSS, USA: IEEE, 2007:162-165
- [4] 中华人民共和国工业和信息化部. 中华人民共和国通信行业标准 YD/T 2407-2013 移动智能终端安全能力技术要求 [M]. 北京:人民邮电出版社, 2013
- [5] 潘娟,史德年,马鑫等. 移动互联网形势下智能终端安全研究 [J]. 移动通信, 2012, 36(5):48-51
- [6] 陈尚义. 移动互联网安全技术研究 [J]. 信息安全与通信保密, 2010,16(8):34-37
- [7] 费心恺,顾庆峰. 移动互联网安全研究 [J]. 移动通信, 2011,35(10):66-70
- [8] 杜跃进,李挺. 移动互联网安全问题与对策思考 [J]. 信息通信技术, 2013,7(4):11-15
- [9] 蒋晓琳. 移动互联网安全问题分析 [J]. 电信网络技术, 2009,19(10):4-7
- [10] ROHWER K, KROUT T. Multiple levels of security in support of highly mobile tactical internets-ELB ACTD [C]//Proceedings of the Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE .Vol. 1. USA: IEEE, 2001: 81-86
- [11] CARAGATA D, ASSAD S E, TUTANESCU I, et al. Security of mobile Internet access with UMTS/HSDPA/LTE [C]//Proceedings of the 2011 World Congress on Internet Security (WorldCIS), USA: IEEE, 2011: 27-276
- [12] 陈萍,夏俊杰. 移动互联网安全现状及应对策略 [J]. 电信网络技术, 2010,20(2):35-38
- [13] ZHU W L, YU J P, WANG T. A security and privacy model for mobile RFID systems in the internet of things [C]//Proceedings of the 2012 IEEE 14th International Conference on Communication Technology (ICCT), USA: IEEE, 2012: 726-727

5G: An Overview [J]. ZTE Communications, 2015, 13(2): 20-27. doi: 10.3969/j.issn.1673-5188.2015.01.003

- [2] 余莉,张治中,程方,胡昊南. 第五代移动通信网络体系架构及其关键技术 [J]. 重庆邮电大学学报(自然科学版), 2014, 26(4): 427-433
- [3] 李方健. D2D 通信系统中的最优中继选择及功率分配策略研究 [J]. 重庆邮电学报(自然科学版), 2014, 26(5): 605-610
- [4] 曹卫东,张涛,李福昌. Small Cell 网络部署策略及技术演进研究 [J]. 2014, (10): 37-42

作者简介



向际鹰,华中科技大学博士毕业;中兴通讯股份有限公司无线首席科学家;从事无线通信技术,包括 3G、4G、5G、基带、射频等技术;获得国家科学技术进步奖二项,国家技术发明奖一项,并获得 2013 年度通信产业技术贡献人物奖;发表论文 35 篇。

←上接第 40 页

患,是一个急需解决的问题。移动互联网安全测评是保障移动互联网安全运行的一个重要环节,从源头上阻止安全隐患的爆发,是一项有效的安全保障措施。移动互联网的测评技术会随着应用的发展而逐步完善,从终端安全、应用安全和安全管理等方面制订相应的标准规范,形成一套完整的测评技术指导体系。文章探讨了移动互联网中的存在的安全威胁和漏洞问题,对移动互联网的安全测评提出了技术层面和管理层面的方法和手段,为从事移动互联网安全测评相关人员的研究和工作提供参考。

参考文献

- [1] HAN B, LIU L. Based on Mobile Internet Application Security Sensitive CS-SVM Technology Research [C]//Proceedings of the 2012 Fifth International Symposium on Computational Intelligence and Design (ISCID), Vol. 2. USA: IEEE, 2012:160-164
- [2] 2014 上半年网秦手机安全报告:中国居手机病毒感染榜首 [EB/OL]. [2015-03-01]. http://econ.taiwan.cn/tx/201409/t20140909_7263501.htm,2014-09-09
- [3] TRONT J G, MARCHANY R C. Internet Security: Intrusion Detection and Prevention in Mobile Systems [C]//Proceedings of the

- [14] 孙泽锋. 移动互联网发展技术与安全分析 [J]. 电信科学, 2011,27(S1):98-101
- [15] 胡建明. 移动互联网业务信息安全 [J]. 信息通信, 2013,12(4):258-259

作者简介



范红,公安部第一研究所检测中心研究员;主要研究领域为物联网安全及信息安全;已主持和参加国家项目及省部级项目 10 余项;获得 2 项科研成果奖;已发表论文 40 余篇,其中被 SCI/EI 检索 10 余篇。



杜大海,公安部第一研究所检测中心工程师;主要研究领域为物联网安全及信息安全;已参加国家基金项目及省部级项目 6 项;已发表论文 20 篇,其中被 SCI/EI 检索 6 篇。



王冠,公安部第一研究所检测中心工程师;主要研究领域为信息安全;先后参加基金项目 3 项;已发表论文 10 余篇,被 SCI/EI 检索 2 篇。

HSPA+异构网中信道分离技术的时延补偿研究

Delay Compensation for HSPA+HetNet Decoupling

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2015) 03-0055-006

摘要: 认为异构网的引入有效提高了高速分组接入+(HSPA+)网络的整体性能,但由于构成异构网的宏基站(MNB)和低功率节点(LPN)发射功率不同,造成上下行数据传输的不均衡,这将不可避免地影响到异构网络的整体性能;增强专用信道(E-DCH)分离技术能够有效消除上下行不均衡问题带来的影响,但信道分离技术在实际应用中会有严重的时延问题。基于上述观点,讨论了HSPA+异构网共信道传输中的控制信道时延问题,并针对这个问题提出自适应灰色预测算法(AGP)实现时延补偿。系统仿真验证了算法的正确性和有效性。

关键词: 适应性灰色预测算法; E-DCH分离; 控制信道时延; HSPA+异构网

Abstract: Heterogeneous networking (HetNet) has been introduced to HSPA+ to enhance the system performance in a cost-efficient way. The uplink-downlink (UL-DL) mismatch caused by heterogeneous deployment reduces performance in the HSPA+ system. To mitigate this mismatch, enhanced dedicated channel (E-DCH) decoupling has been proposed. However, control channels for UL cause undesirable reception delay. In this paper, we focus on delay in co-channel HSPA+ HetNet and propose adaptive grey prediction (AGP) for delay compensation. System-level simulations show that our proposed method has some significant advantages.

Key words: AGP; E-DCH; control channel delay; HSPA + heterogeneous network

李红豆/LI Hongdou
王柯/WANG Ke
常永宇/CHANG Yongyu

(北京邮电大学,北京 100876)
(Beijing University of Posts and
Telecommunications, Beijing 100876, China)

于不均衡区内的用户实行上下行分别服务的策略,即MNB服务下行,LPN服务上行。这个方法能够很直接地解决上下行不均衡问题,但在这项技术应用于实践之前还有许多潜在问题需要加以解决。其中时延问题是最主要的问题,特别是对于遗留用户设备(Legacy UE)^[5]。这是由于Legacy UE在上行传输时,需要在MNB和UE之间建立E-DCH绝对授权信道(E-AGCH)和E-DCH相对授权信道(E-RGCH),而E-AGCH信道的建立需要经由无线网络控制器(RRNC),这个过程往往会造成不可忽略的时延^[6]。

在本文中,笔者将首先对共信道HSPA+异构网中的上行传输、E-DCH信道分离技术以及时延问题进行分析。接着将提出基于GM(1,1)灰色模型^[7-8]的自适应灰色预测算法(AGP)时延补偿方案,基于历史数据利用AGP预测和估算当前授权值,对实际当中授权信道建立产生的时延进行有效补偿。最后将对所提出的AGP算法进行仿真评估,并同时证明了AGP时延补偿算法的可行性和有

随着智能手机的迅速普及,基于数据交换的各种业务需求的持续增长,这对大容量的移动通信系统提出迫切需求。异构网的提出对于提高通信系统容量和扩大通信网络覆盖范围有着重要意义。在LTE中,异构网已经成为一项成熟的技术,但对于高速分组接入+(HSPA+)网络的标准化工作还在进行中。在共信道的HSPA+异构网的部署过程中,一些问题仍需加以讨论和解决^[1]。

HSPA+异构网络中共享信道的上下行不均衡问题是最主要的问题,由于低功率节点(LPN)的功率要低于宏基站(MNB),导致上下行传输边界不一致,这就在二者服务域内产生了上下行不均衡区域^[2]。而在这个区域里总是会存在一些潜在的问题,对上下行数据传输性能造成一些不良的影响^[3]。

为了解决异构网中的上下行不均衡问题,相关技术相继提出,其中增强专用信道(E-DCH)信道分离技术(E-DCH decoupling)^[4]是最有望得到广泛应用的有效解决方案。E-DCH信道分离技术本质上就是对处

收稿日期: 2014-10-11

网络出版时间: 2015-02-22

基金项目: 中兴通讯基金资助项目
(HSPA异构网络及新技术研究)

效性。

1 系统模型

本文相关研究及讨论基于一个上行共信道的HSPA+异构网模型,该网络中包含有 M 个常规六边形宏单元(Macro Cell),每一个MNB都是位于六边形宏单元的中心,每一个宏单元被均分成3个 120° 角的近似扇形子域。 K 个LPN随机均匀分布于每一个宏单元中,同时,在每个宏单元子域中随机均匀撒入 N 个用户。模型设定每个基站(包括MNB和LPN)以及用户都有两个天线。每一个用户在MNB和LPN中只能选择一个作为自己的服务节点。

1.1 小区配置

将范围扩展(RE)^[9]考虑在内, UE_i 在选择基站(NodeB) b_i 作为服务节点的时候遵循以下公式:

$$b_i = \arg \max_{b \in M \cup K} (\mu_{i,b} + \Delta b) \quad (1)$$

将其中 M 和 K 分别表示MNB和LPN的集合, $\mu_{i,b}$ 是 UE_i 下行的接收信号功率(RSCP)^[10], Δb 是NodeB b 的附加偏移值并且符合下式:

$$\Delta b = \begin{cases} \delta(\delta > 0), b \in K \\ 0, b \in M \end{cases} \quad (2)$$

1.2 信号与干扰加噪声比模型

这里我们考虑每个NodeB可以在每个调度周期内调度一个UE的场景,当NodeB b_i 调度 UE_i 的时候,下行信干噪比(SINR)是:

$$\gamma_{i,b_i} = \frac{p_i \cdot G_{i,b_i}}{N_0 + \sum_{j=1, j \neq i}^N p_j \cdot G_{i,b_i}} \quad (3)$$

其中 p_i 是 UE_i 的传输功率, N_0 是 UE_i 的白噪声,而 G_{i,b_i} 则表示上行信道的增益。

1.3 服务授权

大的授权(Grants)不仅意味着UE要用更大发送功率和更高的数据传输速率,而且意味着系统将会遭受

更严重的干扰。基于对实时干扰水平的测量,调度节点会对各个终端的授权进行控制从而将小区内干扰保持在一个可以接受的范围内。授权通过HSPA+异构网中的E-AGCH和E-RGCH从NodeB传到UE^[11]。但是在UE由于时延过长等问题不能及时接收授权的情况下,UE就可能会用上一次数据传输中使用过的过期授权,这将导致授权与当前传输环境不符从而影响到整个小区的性能。

2 HSPA+异构网信道分离技术中的时延补偿

我们将首先分析上下行不平衡造成的影响以及E-DCH信道分离技术中上行时延问题,然后提出AGP时延补偿算法。

2.1 上下行不平衡问题

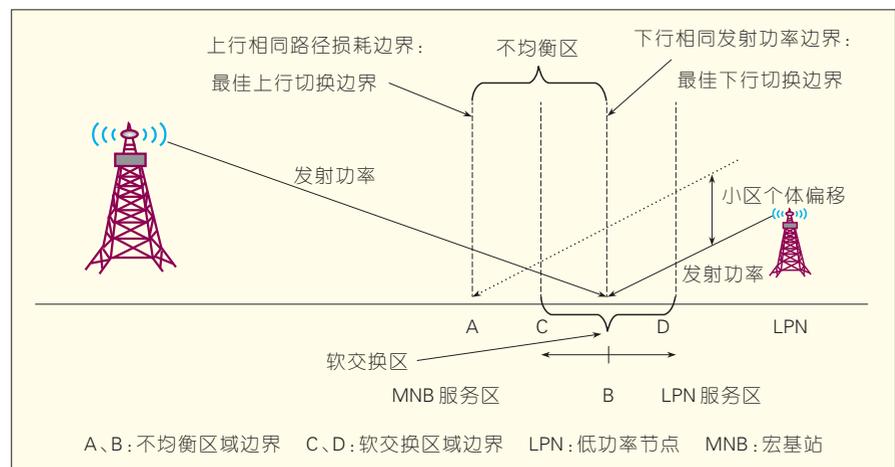
HSPA+异构网中不平衡区的如图1所示。在HSPA+异构网络共信道场景中,由于MNB的功率要比LPN功率大,导致上下行边界位置不同,造成二者之间存在上下行不平衡区域。上行UL边界在MNB和LPN接收到UE功率相同的位置,即为MNB和LPN两个节点中间位置。下行DL边界在UE接收到MNB和LPN发射信号功率相同的位置,而由于MNB的功率要高于LPN,所以DL边界在偏向LPN的位置。这里的系统分析不考

虑范围扩展,即小区个体偏移(CIO)等于0。图1中C、D两点是软切换(SHO)边界,对于在SHO区的UE来说,可以调度它的节点NodeB同时包括MNB和LPN,也就是说,这个情况下的UE是被MNB和LPN两者同时控制的。

因此,不平衡区可以进一步被分为两部分,在没有和SHO重叠的区域AC内,UE只受到MNB的服务和控制,但这种情况下UE实际上是距离LPN更近。因此,上行传输时,作为服务节点的MNB会要求UE有比较大的发射功率,从而造成对LPN的严重干扰。在不平衡区和SHO区重叠的部分CB内,MNB和LPN都可能对UE进行控制和影响。当UE用合适的发射功率对MNB进行上行传输时,会对距离它最近的LPN产生严重的上行干扰,为了减小这种干扰,LPN会要求UE降低它的上行发射功率,但减小了发射功率的UE将会无法和MNB进行可靠的上行数据传输。同时,上行传输的数据中也会包括一些下行传输控制信息,所以,这将影响到下行传输的可靠性。总之,上下行不平衡问题会对上行和下行的数据传输性能均造成不良影响。

2.2 E-DCH信道分离技术

E-DCH信道分离技术其实就是在不平衡区施行这样一个传输策



▲图1 HSPA+异构网中不平衡区示意

略:UE进行上行数据传输时选距离它最近的LPN作为服务节点,在下行传输时仍旧选用原始服务节点MNB。像这样对上下行数据传输分别调用不同服务节点的方法不仅能够保证数据传输质量,也能有效地消除干扰。

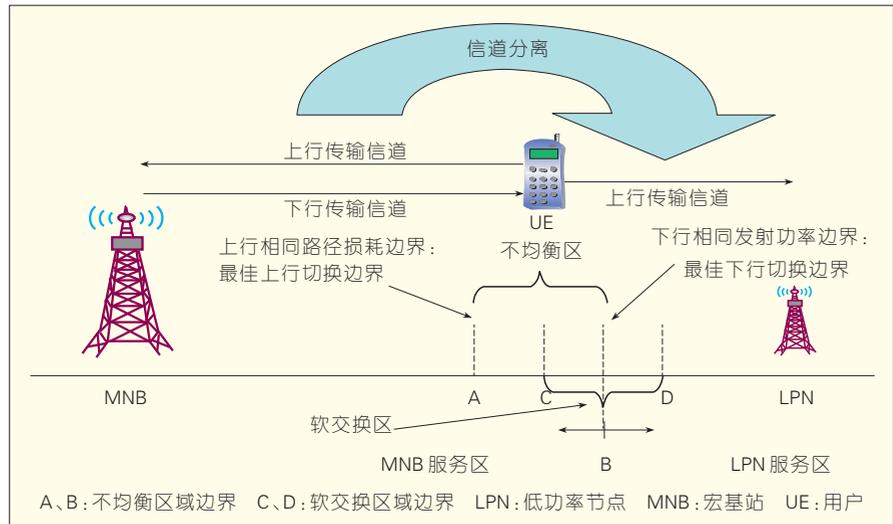
E-DCH信道分离过程如图2所示。在不均衡区的UE传输上行数据时,为了不影响附近的LPN会减小它的发射功率,从而影响UE与MNB的上行传输质量。当应用E-DCH信道分离技术时,LPN会代替MNB作为上行服务节点并且给UE提供上行传输授权,接收UE的上行传输数据。这个授权可以经过适当调整从而实现LPN对上行数据的成功接收并且不会干扰到MNB。

在不均衡区内将UE的上行传输服务节点更换为LPN,可以使上行传输功率调整到能够仅被LPN接收且不会干扰到MNB程度,很好地解决了上下行不均衡问题。同时,由于MNB不需要对不均衡区的UE进行上行传输服务控制,这就释放了很多MNB上行资源,从而提升了宏单元的整体性能。

2.3 遗留用户的时延问题

由上文可知E-DCH信道分离技术能够很好地解决上下行不均衡问题,但是要改变上行传输服务节点需要额外增加相关控制、授权信号的传输。对于Rel-12用户而言,LPN可以直接和用户(UE)之间建立E-AGCH等控制信道,但对于遗留用户来说,LPN需要经由MNB同UE之间建立控制信道,而MNB同用户之间控制信道的建立还要通过RNC。

遗留用户的整个E-DCH信道分离技术实现过程如图3所示。不难看出授权信道的建立是相当耗时,将会造成10~20ms的时延^[12]。在授权接收时,若时延过长将会导致UE接收到的授权很可能是前一次数据传输中应当接收并用于传输控制的授



▲图2 E-DCH信道分离过程示意

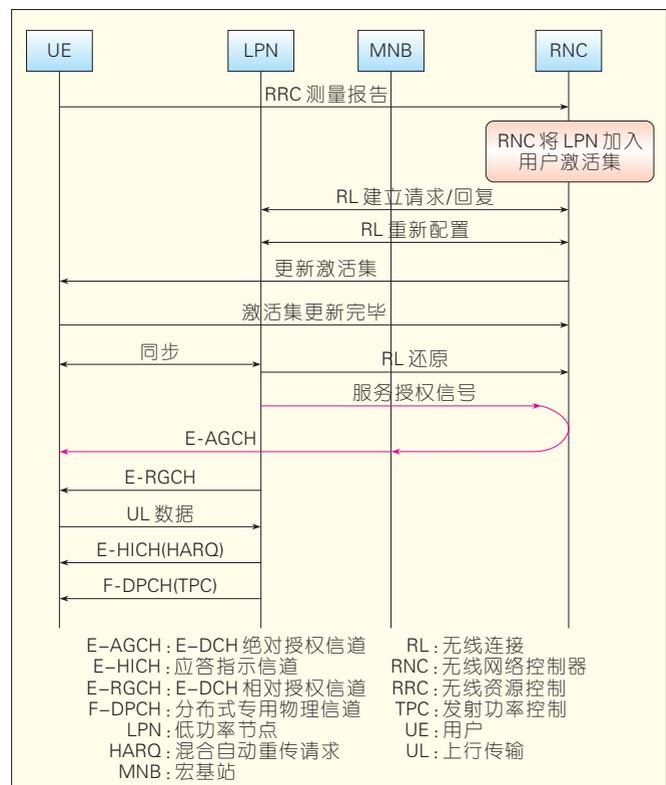


图3 遗留用户E-DCH信道分离信令传递过程

权,对于当前数据传输没有指导意义,也就是与当前传输环境不匹配。授权过大会导致发射功率过大,会给E-DCH信道分离系统带来不可预测的干扰,而授权过小意味着系统资源得不到充分利用。这两种情况都会削弱E-DCH信道分离系统的性能,因此,时延补偿技术的研究对遗留用

户有重要意义。

2.4 AGP算法

AGP是基于对不完整、不确定数据的分析,发现并利用数据间的相关性建立系统模型,从而预测未知数据的算法。这是一种基于数列关联度的算法,它假设所观测的系统中的内

参、系统特性和结构都是未知的,这个系统状态可以根据一个由最近历史数据得到的微分方程进行预测^[13]。

根据AGP算法,时延补偿详细过程如下:

(1) 根据最近测量数据构造原始数列

$$g^{(0)} = \{g^{(0)}(1), g^{(0)}(2), \dots, g^{(0)}(n)\} \\ = \{g^{(0)}(k); k=1, 2, \dots, n\} \quad (4)$$

其中 $g^{(0)}(k)$ 是 k 时刻测得的授权值, n 代表的是整个数列的长度, n 符合如下公式:

$$n = \mu \cdot T_{Delay} \quad (5)$$

其中 T_{Delay} 表示 E-AGCH 的时延, μ 是恒参, μ 越大则测量长度越大,意味着复杂性越大。

(2) 构造一个基于中间变量 $g^{(1)}$ 的累加生成 (AGO)

$$g^{(1)} = \{g^{(1)}(1), g^{(1)}(2), \dots, g^{(1)}(n)\} \\ = \{g^{(0)}(k); k=1, 2, \dots, n\} \quad (6) \\ = \left\{ \left\{ \sum_{i=1}^k g^{(0)}(i) \right\}, k=1, 2, \dots, n \right\}$$

其中上标 (0) 表示原始数据, (1) 表示累加生成数据。累加生成数据能够将一个非负不规则数列变换成一个递增数列。因此,生成数 $g^{(0)}$ 使原始数列 $g^{(0)}$ 固有性质得到加强。

(3) 构造灰色微分方程

$$\frac{dg^{(1)}}{dk} + ag^{(1)} = b \quad (7)$$

由于 $g^{(1)}(1) = g^{(0)}(1)$, 由最小二乘法可以得到 a, b 的值:

$$\hat{a} = \begin{bmatrix} a \\ b \end{bmatrix} = (B^T B)^{-1} B^T Y_N \quad (8)$$

其中

$$B = \begin{bmatrix} -J^{(1)}(2) & 1 \\ -J^{(1)}(3) & 1 \\ \dots & \dots \\ -J^{(1)}(n) & 1 \end{bmatrix}, Y_N = \begin{bmatrix} g^{(0)}(2) \\ g^{(0)}(3) \\ \dots \\ g^{(0)}(n) \end{bmatrix} \quad (9)$$

$$J^{(1)}(k) = \alpha g^{(1)}(k) + (1 - \alpha)g^{(1)}(k-1), \quad (10) \\ k = 2, 3, \dots, n$$

$J^{(1)}$ 是由数列 $g^{(0)}$ 的邻值在生成系数 α 下的邻值生成数,这里由于每个授权有相同权重,故 α 取 0.5。

(4) 计算预测值

利用 (8) 计算得到 a 和 b 的值以后,就可以利用灰色微分方程预测 $g^{(0)}$ 在下时刻的值,首先利用下式得到中间变量:

$$\hat{g}^{(1)}(k+1) = \left[g^{(0)}(1) - \frac{b}{a} \right] e^{-ak} + \frac{b}{a}, \quad (11) \\ k = 0, 1, 2, \dots$$

接下来,通过累加生成逆变换 (IAGO) 计算预测值:

$$\hat{g}^{(0)}(k+1) = \hat{g}^{(1)}(k+1) - \hat{g}^{(1)}(k) = \\ (1 - e^{-a}) \left[g^{(0)}(1) - \frac{b}{a} \right] e^{-ak} \quad (12)$$

(5) 残差检验

预测结果的均方误差、残差均方误差以及方差比计算如下:

$$S_1 = \left(\frac{\sum_{i=1}^n [g^{(0)}(i) - \bar{g}^{(0)}]^2}{n-1} \right)^{\frac{1}{2}} \quad (13)$$

$$S_2 = \left(\frac{\sum_{i=1}^n [\Delta^{(0)}(i) - \bar{\Delta}^{(0)}]^2}{n-1} \right)^{\frac{1}{2}} \quad (14)$$

$$C = \frac{S_1}{S_2} \quad (15)$$

其中 $\bar{g}^{(0)}$ 和 $\bar{\Delta}^{(0)}$ 分别代表授权数列的均值和残差均值, C 是均方误差比。如果:

$$C < \xi \quad (16)$$

则预测结果具有可用性,否则预测结果不可用。这里 ξ 是默认阈值。

(6) 算法实现

本文提出的 AGP 时延补偿方法是利用 MNB 一侧授权的历史数据预测当前授权的。具体实现步骤如下:

- 算法实现流程如图 4 所示。图 4 中 UE_{ij} 表示 MNB 在步骤 i 中调度的第 j 个用户,在 E-DCH 信道分离过程中简称为遗留用户 (LDUE), LDUE 表示第 i 个遗留用户。首先, LDUE 在上行传输信道中加入作为 LUDE 的标识符,一旦服务节点 MNB 检测到标识符,它就会为 LUDE 准备缓存区来存储历史授权。

- LDUE 申请上行传输时,原始服务节点 LPN 通过 RNC 向 MNB 发送授权值,然后 MNB 通过 E-AGCH 将此授权发送给 LDUE 并存入缓存区。此时, LDUE 接收到的授权仍为延迟后的授权。

- 当缓存区已满且 LDUE 要进入下一个服务周期时, MNB 就对缓存区内的历史授权值进行基于 AGP 算法的计算得到预测授权值。如果得到的结果满足 (16) 式, MNB 就立即将其作为当下授权发送,否则就等收到下一个延迟的授权再向 LDUE 发送。

- 将缓存区中最早存入的授权值弹出,并将最新数据压入,如此不断更新缓存区内数据,从而能够连续预测下一个授权。

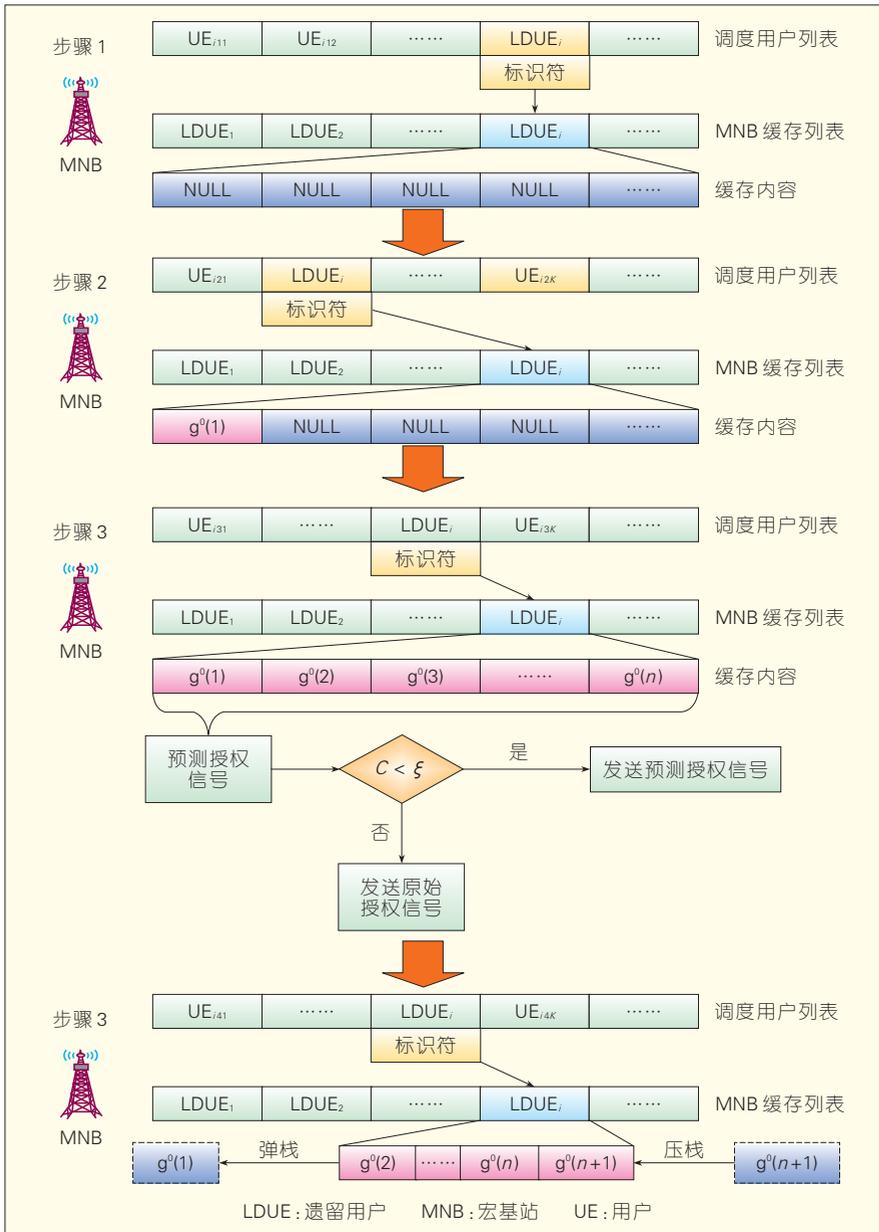
3 系统级仿真

文章将通过系统仿真来验证 AGP 算法在 HSPA+ 异构网上行传输信道分离的过程中所起到的时延补偿作用。

3.1 仿真环境配置

本文中的仿真环境搭建和参数配置都是基于文献[14]。这里研究的是一个由 19 个六边形蜂窝小区组成的 HSPA+ 网络,每个宏基站周围有 3 个扇区,在每个扇区中均匀随机撒入 4 个 LPN 节点。节点的接收器和发射器都配有两个天线。在这个场景中,我们假设每个扇区中有 8 个用户,都是均匀随机分布。其中在热点区 (LPN 覆盖区) 的用户数量与扇区内用户总数量之比为 $P_{hotspot}$,本次仿真中 $P_{hotspot}$ 等于 0.5。LPN 传输功率取 30 dBm,覆盖半径为 35 m。MNB 传输功率取 43 dBm,用户最大传输功率取 24 dBm。遗留用户的 E-AGCH 时延为 10 ms 和 20 ms, (16) 式中 ξ 取值 0.65。

采用 PA3 信道模型^[15],信道衰落符合对数正态阴影衰落。节点 NodeB b 和用户 UE_i 之间的路径衰落计算如下:



▲图4 算法实现流程

$$\ell_{i,b}[dB] = \begin{cases} 128.1 + 37.6 \log_{10}(D_{i,b}), b \in M \\ 140.7 + 36.7 \log_{10}(D_{i,b}), b \in K \end{cases} \quad (17)$$

其中 $D_{i,b}$ 表示 NodeB b 和 UE_i 之间的距离。

其他信道衰落参数如表1所示,详细仿真参数如表2所示。

3.2 仿真结果分析

AGP算法在HSPA+异构网上行传输中的时延补偿效果的仿真结果如图5、图6、图7所示。

图5显示了在不同时延下的用户吞吐量和小区个体偏移量之间的关系曲线。其中绿色曲线表示理想无时延情况下的用户吞吐量曲线,是其他两条曲线的对比曲线;红色曲线表示实际有时延情况下的用户吞吐量曲线,由于E-AGCH建立中10~20ms的时延,这种情况下的预留用户在E-DCH信道分离状态中用到的授权很有可能是不匹配的,可以看出红色曲线和理想无时延情况下的绿色曲

▼表1 其他信道衰落参数

参数	宏小区	低功率小区
基站噪声系数/dB	5	5
基站最大发射功率/dBm	43	30
基站最大天线增益/dBi	14	5
对数正态阴影衰落标准差/dB	8	10

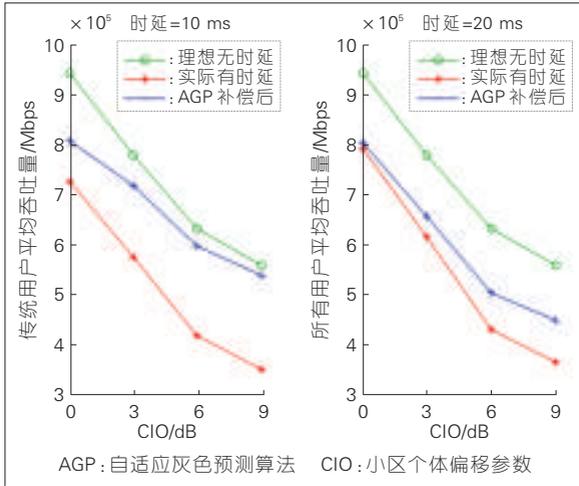
▼表2 详细仿真参数

参数	假定值
载频	2 GHz
系统带宽	5 MHz
基站点间距	宏基站: 500 m 低功率节点: 大于 40 m
最小接入距离	用户到 MNB: 35 m 用户到 LPN: 10 m
用户撒入方式	50%撒入热点区
热噪声上升默认值	6 dB
信道模型	PA3
天线模式	MNB: 3GPP 二维天线 LPN: 全方位天线
用户噪声因数	9 dB
小区个体偏移参数	0/3/6/9 dB
E-AGCH 遗留用户时延	10/20 ms
E-AGCH 用户信道分离差错率	1%
遗留用户百分比	30%

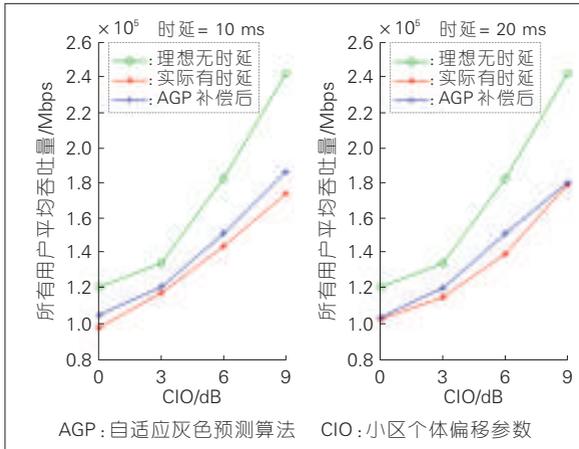
E-AGCH: E-DCH 绝对授权信道

线有明显差距,这就意味着实际应用中时延问题会对用户吞吐量造成严重影响;蓝色曲线表示预留用户在E-DCH信道分离状态中应用AGP算法进行时延补偿后的用户吞吐量情况,可以看出这条曲线有效地缩小了实际情况与理想情况之间的差距,虽然达不到但却更加接近理想无时延的绿色曲线,这就意味着AGP算法在E-DCH信道分离中有效地起到了时延补偿的作用。

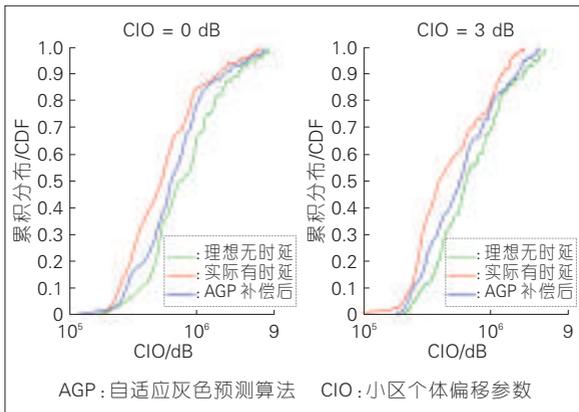
图6显示了在不同时延下所有用户吞吐量和RE偏置值CIO之间的关系曲线,和图5分析类似,可以看出在不同实际时延情况下应用AGP时延补偿算法时,都会明显提升用户吞吐量,改善系统性能,并且缩小和理想无时延状态下系统性能的差距。



▲图5 遗留用户平均吞吐量随CIO变化曲线



▲图6 所有用户平均吞吐量随CIO变化曲线



▲图7 遗留用户吞吐量的累积分布曲线

正如前文所述, AGP算法的应用将会减小系统干扰, 提高整体无线通信系统的性能, 进而使每一个用户的性能都较实际有时延情况下有所提高。

图7显示了在不同CIO下遗留用户吞吐量的累积分布(CDF)函数曲线, 可以看出AGP算法有效地实现了时延补偿, 并提高了系统的整体性能。

4 结束语

本文主要讨论解决的是HSPA+异构网上行链路中应用E-DCH信道分离技术时产生的时延问题。文中首先简要介绍了系统模型, 分析了HSPA+异构网中存在的上下行传输不均衡问题, 接下来提出了解决此问题的E-DCH信道分离技术, 并经分析提出此项技术在实际应用中造成的时延问题。接下来, 为了实现时延补偿有效提高网络性能, 文中提出了AGP算法, 该算法通过准确预测E-AGCH授权值, 可以对时延造成的问题进行有效补偿。最后, 文中通过对该算法进行系统级仿真评估, 验证了该算法不仅能够有效地实现时延补偿, 同时还降低了干扰水平, 提高了系统性能。

参考文献

[1] 3GPP. 3GPP RP-131306. New WI proposal: UMTS Heterogeneous Networks Enhancements [S]. 3GPP TSG RAN, 2013
 [2] 3GPP. 3GPP TR 25.800. Study on UMTS heterogeneous networks (Release 12) [S]. 3GPP TSG RAN, 2013
 [3] 3GPP. 3GPP R1-135621. E-DCH Decoupling for Legacy UE [S]. 3GPP TSG RAN WG1, 2013
 [4] 3GPP. 3GPP R1-134747. Detailed analysis of E-DCH decoupling [S]. 3GPP TSG RAN WG1, 2013

[5] 3GPP. 3GPP R1-133539. Considerations for E-DCH Decoupling in UMTS HetNets [S]. 3GPP TSG RAN WG1, 2013
 [6] 3GPP. 3GPP R1-132529. Introducing E-DCH decoupling in Hetnet deployments [S]. 3GPP TSG RAN, 2012
 [7] CHEN J F, SHI Z G, HONG S H, CHEN K S. Grey prediction based particle filter for maneuvering target tracking [J]. Progress in Electromagnetic Research (PIER), 2009,93 (1): 237-254
 [8] 肖新平, 毛树华. 灰预测与决策方法 [M]. 北京: 科学出版社, 2013
 [9] 3GPP. 3GPP R1-125135. Considerations on Range Expansion [S]. 3GPP TSG RAN WG1, 2012
 [10] 3GPP. 3GPP TS 25.215. Physical layer measurements (FDD) (Release 11) [S]. 3GPP, 2011
 [11] DAHLMAN J S E, PARKVALL S, BEMING P. 3G evolution: HSPA and LTE for mobile broadband [M]. Academic Press, 2008
 [12] 3GPP. 3GPP R1-134676. Considerations on E-DCH decoupling [S]. 3GPP TSG RAN WG1, 2013
 [13] WONG T C, LIN B C, CHENG C T. Fuzzy tracking method with a switching grey prediction for mobile robot [J]. IEEE International Conference on Fuzzy Systems, 2001,22(1): 103-106. doi:10.1109/FUZZ.2001.1007257
 [14] 3GPP. 3GPP R1-135622. Simulation Result for E-DCH Decoupling combined with CIO in UMTS HetNet [S]. 3GPP TSG RAN WG1, 2013
 [15] 3GPP. 3GPP TS 25.101. User Equipment (UE) radio transmission and reception (FDD) (Release 11) [S]. 3GPP, 2012

作者简介



李红豆, 北京邮电大学在读硕士研究生; 主要研究方向为移动通信理论、移动通信系统性能评估及关键技术等。



王柯, 北京邮电大学在读硕士研究生; 主要研究方向为移动通信理论、移动通信系统性能评估及关键技术等。



常永宇, 北京邮电大学信息与通信工程学院教授、博士生导师; 主要从事移动通信理论、移动通信系统性能评估及关键技术研究等方面的工作; 已发表学术论文100余篇, 出版学术著作9部, 申请发明专利10余项。

《中兴通讯技术》杂志(双月刊)投稿须知

一、杂志定位

《中兴通讯技术》杂志为通信技术类学术期刊,通过介绍、探讨通信热点技术,展现通信技术最新发展动态,并促进产学研合作,发掘和培养优秀人才,为振兴民族通信产业做贡献。

二、稿件基本要求

1. 投稿约定

- (1) 作者需登陆《中兴通讯技术》投稿平台: www.zte.com.cn/paper,并上传稿件。第一次投稿需完成新用户注册。
- (2) 编辑部将按照审稿流程聘请专家审稿,并根据审稿意见,公平、公正地录用稿件。审稿过程需要大约1个月左右。

2. 内容和格式要求

- (1) 稿件须具有创新性、学术性、规范性和可读性。
- (2) 稿件需采用WORD文档格式。
- (3) 稿件篇幅一般不超过6000字(包括文、图),内容包括:题名、作者姓名、作者单位、中文摘要、关键词(4~8个)、英文摘要、正文、参考文献、作者简介。
- (4) 中文题名一般不超过20个汉字,中、英文题名含义应一致。
- (5) 摘要尽量写成报道性摘要,包括研究的目的、方法、结果与结论,以150~200字为宜。摘要应具有独立性和自明性,采用第三人称。中英文摘要内容应一致。
- (6) 文稿中的量和单位应符合国家和国际标准。外文字母的正斜体、大小写等须写清楚,上下角的字母、数据和符号的位置皆应明显区别。
- (7) 图、表力求少而精(以8幅为上限),应随文出现,切忌与文字重复。图、表应保持自明性,图中缩略词和英文均要在图中加中文解释。表应采用三线表,表中缩略词和英文均要在表内加中文解释。
- (8) 参考文献以20条左右为宜,未公开发表的资料不宜列入。所有文献必须在正文中引用,文献序号按其在文中出现的先后次序编排。主要种类参考文献的书写格式为:
 - 期刊[序号]作者.题名[J].刊名,出版年,卷号(期号):起止页码
 - 书籍[序号]作者.书名[M].出版地:出版者,出版年:起止页码
 - 论文集中析出文献[序号]作者.题名[C]//论文集编者.论文集名(会议名).出版地:出版者,出版年(开会年):起止页码
 - 学位论文[序号]作者.题名[D].地点:学位授予单位,授予年
 - 专利[序号]专利所有者.专利题名.国别:专利号[P].公布日期
 - 国际、国家标准[序号]标准编号,标准名称[S]
- (9) 作者原则上不超过3人,超过3人时,可以感谢形式在文中提及。作者简介包括:姓名、工作单位、职务或职称、学历、毕业于何校、现从事的工作、专业特长、科研成果、已发表的论文数量等。
- (10) 提供正面、免冠、彩色标准数码照片一张,最好采用JPG格式(文件大小超过100kB)。
- (11) 尽可能标注出研究课题的资助基金或资助项目名称。
- (12) 作者姓名中含有多音字时,应标注作者姓名的汉语拼音。
- (13) 提供联系方式,如:通信地址、电话(含手机)、Email等。

3. 其他事项

- (1) 请勿一稿多投。凡在2个月(自来稿之日算起)以内未接到录用通知者,可致电编辑部询问。
- (2) 为了促进信息传播,加强学术交流,在论文发表后,本刊享有文章的版权(包括英文版、电子版、网络版和优先数字出版)。作者获得的稿费包括版权酬金。如对此持有不同意见,请在投稿时说明。

编辑部地址:安徽省合肥市金寨路329号国轩凯旋大厦1201室,邮政编码:230061

联系电话:0551-65533356,联系邮箱: magazine@zte.com.cn

本刊只接受在线投稿,欢迎访问本刊投稿平台: www.zte.com.cn/paper

中兴通讯技术

ZHONGXING TONGXUN JISHU

双月刊 1995年创刊 总第122期
2015年6月 第21卷第3期

主管:安徽省科学技术厅
主办:安徽省科学技术情报研究所
中兴通讯股份有限公司
编辑:《中兴通讯技术》编辑部

总编:孙枕戈
常务副总编:黄新明
责任编辑:杨勤义
编辑:徐焯,卢丹,朱莉,Paul Sleswick
排版制作:余刚
发行:王萍萍
编务:王坤

ZHONGXING TONGXUN JISHU

《中兴通讯技术》编辑部
地址:合肥市金寨路329号凯旋大厦12楼
邮编:230061
网址:www.zte.com.cn/magazine
投稿平台:www.zte.com.cn/paper
电子信箱:magazine@zte.com.cn
电话:(0551)65533356
传真:(0551)65850139

出版、发行:中兴通讯技术杂志社
发行范围:全球发行
印刷:合肥添彩包装有限公司
出版日期:2015年6月10日
刊号:ISSN 1009-6868
CN 34-1228/TN
广告经营许可证:皖合工商广字 0058
定价:每册 20.00 元,全年 120.00 元