



第三届全国期刊奖百种重点期刊 中国科技核心期刊  
中国科技论文统计源期刊 中国五大文献数据库收录期刊

ISSN 1009-6868  
CN 34-1228/TN

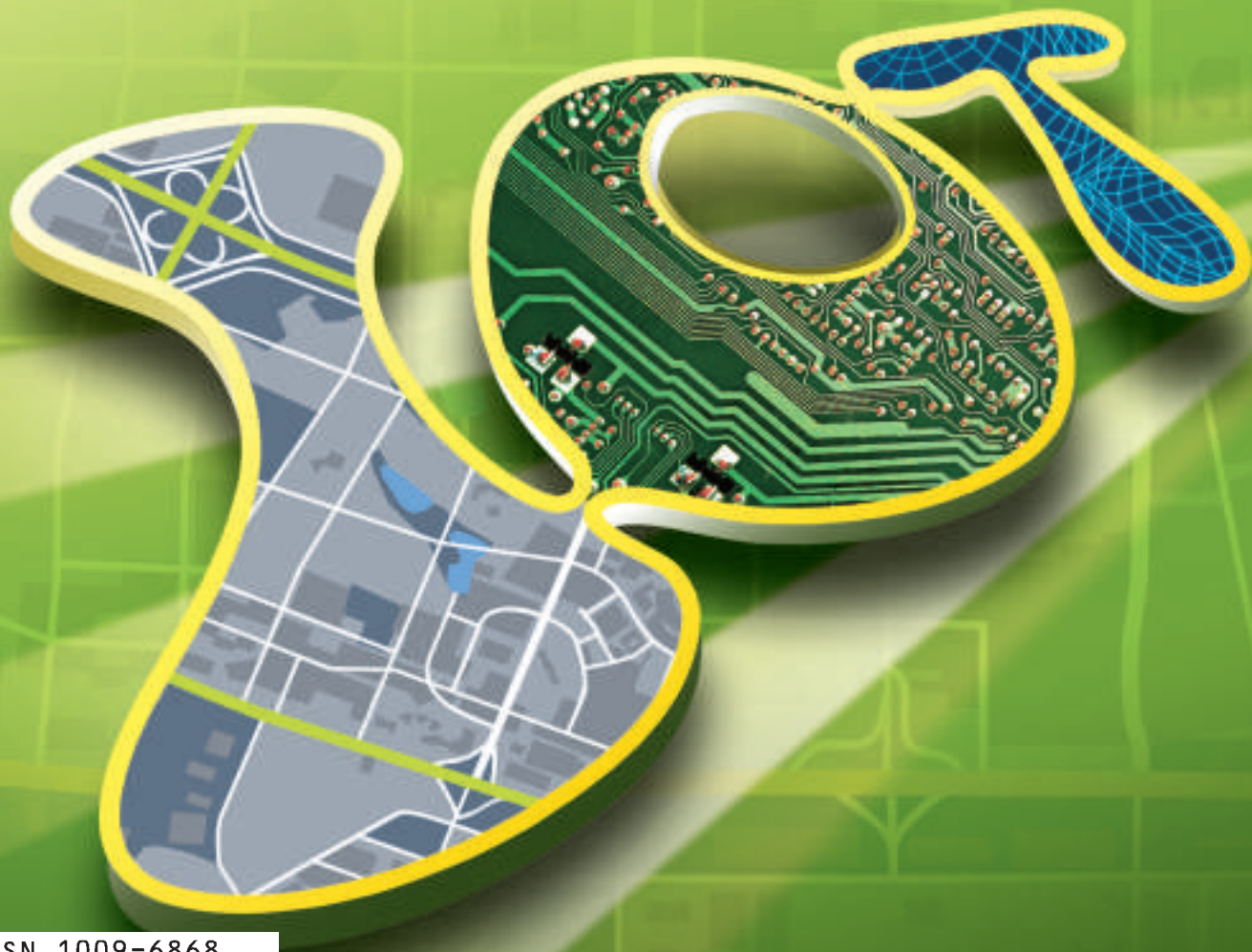
# 中兴通讯技术

## ZTE TECHNOLOGY JOURNAL

[www.zte.com.cn/magazine](http://www.zte.com.cn/magazine)

2011年2月 • 第1期

**专题：物联网技术及其应用**



ISSN 1009-6868



# 中兴通讯 ZXONE 8000 系列通过国家“863”课题全面设备测试

【本刊讯】2010年12月23日消息，国家“863”计划重大课题“大容量光传送网(OTN)关键技术与设备系统”取得重大进展突破，课题相关设备——中兴通讯大容量电交叉光传送平台 ZXONE 8000 系列产品成功通过设备的全面测试，其中包含 ZXONE 8300、ZXONE 8500 产品。

新一代的大容量高可信光传送网是未来可信化网络体系的重要支撑，是国家信息基础设施网络的建设战略之一。课题研究包括：OTN 商用设备与核心芯片研制、OTN 相关业务、组网实验、工程、运维、标准等系列研究。课题旨在全面高质量地达到课题研究目标，包括：研制设备样机，建立实验系统等。

“大容量光传送网(OTN)关键技术与设备系统”是新一代大容量高可信光传送网技术领域的重要支撑研究项目之一，该课题由中兴通讯联合北京邮电大学和中国移动通信集团公司重点参与。

作为课题的共同承担单位，北京邮电大学在光通信领域具有深厚的研究基础，拥有中国领先的研究队伍，

取得了丰富的理论研究及实验研究成果；中国移动集团作为全球知名的电信运营企业，以及研究成果的主要使用者和受益者之一，将最终的用户需求融入课题；中兴通讯作为全球 OTN 技术前沿领先者，截止 2010 年第 3 季度，销售额已跻身光网络全球前三。北京邮电大学、中国移动通信集团以及中兴通讯、通过课题组“产、学、研、运”相结合，发挥各自优势。

经过项目组两年的联合研制，攻克了多项 OTN 和 WASON 系统关键技术，部署了一批先进的 OTN 商用化设备，包括业界最大交叉容量的 OTN 系统——中兴通讯 ZXONE 8000 系列产品。中兴通讯已全面掌握了一系列具有自主知识产权的硬件、软件和协议的核心技术，已申请和取得 50 多项国家发明专利。

中兴通讯承载网产品总经理樊晓兵表示：“非常高兴能够与北京邮电大学以及中国移动通信集团联合参与课题，我们尽力全面优质地完成课题组的各项目标，为增强中国传输设备制造业做出贡献。”

## 中兴通讯在 IETF 牵头成立首个云计算标准工作组

【本刊讯】2010年11月7日，IETF 第 79 次大会首次在中国北京举行，1 200 余名来自全球 65 个国家和地区的 IETF 技术专家参加了本次盛会。

中兴通讯在本次会议上总共提交了 61 篇活动草案，内容涉及传输、路由、业务、安全等领域；同时还牵头发起云计算的 Bar BOF（非正式兴趣组），相关的立项建议在 IAB & IESG（互联网架构董事会&互联网工程指导组）管理层会议上获得通过，并获许成立 Cloud OPS WG（云计算运维工作组）和 Cloud APS BOF（云计算应用兴趣组），成为首家在 IETF 标准组织建立云计算标准工作组的厂商，为云计算在 IETF 的标准推进做出了重大贡献。

其中，Cloud OPS 工作组将致力于开展云计算资源建模、资源管理和资源提供的标准化工作，在面向各种业务需求时，给出安全高效的云资源提供方案，并研究目前云互通所面临的技术问题。

中兴通讯早在 2003 年就开始涉足并行计算模式的研究和探讨，尤其是云计算在电信业的应用。凭借多年在电信行业研发的优势，中兴通讯形成“电信云计算”三大核心技术：中兴通讯分布式结构化存储、中兴通讯云存储分布式文件系统、中兴通讯虚拟化技术。目前，中兴通讯已经开发完成的“彩云”CoCloud 平台正服务于许多电信客户。

中兴通讯标准部副部长袁飞在本次会议上还做了《Opportunities and Challenges for Next Generation Communication Network》的主题英语演讲，吸引了众多 IETF 会员，反响强烈。

近年来，中兴通讯在国际标准领域业绩卓著，已有 30 多名专家在全球各大国际标准组织中担任主席、报告人等领导职务，同时取得了 80 多个国际标准编辑者席位和起草权，贡献的国际提案超过 12 000 篇，对行业标准推进起到了重要作用。

# 中兴通讯技术杂志社迎春联谊会 在北京隆重召开

【本刊讯】2011年1月7日下午,“中兴通讯技术杂志社2011年迎春联谊会”在北京新世纪日航酒店隆重召开。吴佑寿院士、李德毅院士、韦乐平主任、蒋林涛总工、谈振辉教授等78位嘉宾参加会议。他们分别来自通信运营商、高等院校、科研院所、期刊管理部门和新闻媒体等,也代表了刊物编委、审稿人、作者和读者。大家欢聚一堂,共迎新春。

中兴通讯股份有限公司执行副总裁谢大雄(CTO)到会并致欢迎辞。他介绍了中兴通讯2010年在全球市场取得的成就,以及中兴通讯在技术和产品两个方面的最新发展,并感谢与会代表长期以来对中兴通讯的大力支持。随后杂志社常务副总编黄新明总结了杂志创刊15年来刊物走过的3个发展阶段,以及中英文两刊下一个五年计划的发展目标及举措,并对中兴通讯产学研合作论坛2010年项目执行情况及论坛管理工作进行了总结。中兴通讯技术总监张军做了题为“通信行业发展趋势与思考”的专题报告。

联谊会由刊物编委会主任、北京邮电大学钟义信教



授主持。在轻松愉快的氛围中,代表们或对通信热点问题发表见解,或对中兴通讯及刊物发展建言献策。

一年一度的杂志社迎春联谊会,既是专家座谈会,又是一个交流和合作的平台。它对中兴通讯刊物和产学研论坛的发展起到了良好的促进作用。

## 中兴通讯首家打通LTE网络 与2G/3G现网IMS语音电话 引领VoLTE部署

【本刊讯】2010年11月17—18日,Mobile Asia Congress在香港举行。在本次大会上,中兴通讯通过CSL的LTE网络,成功展示了基于IMS的IP语音通话,不但实现了IMS软终端之间的VoLTE通话,同时实现了IMS软终端与2G/3G现网手机之间的IP语音,通话效果清晰、稳定,这是业界首次成功实现LTE网络与2G/3G现网之间的互通。

中兴通讯为CSL提供了Uni-CORE核心网络解决方案,为CSL打造一个智能、融合、高性能的核心网络,实现2G/3G/4G的全融合。EPC网络支持精确的业务控制和内容计费功能,强大的数据吞吐能力确保CSL从容应对数据流量爆炸式增长和业务日益纷繁复杂的挑战。同时,IMS网络的部署能够不断提升CSL的LTE/EPC网络潜力,为用户提供更加丰富的多媒体业务。此次展示的基于IMS的宽带语音解决方案,有效推动了CSL传

统业务向LTE的迈进。后续随着SRVCC演进语音解决方案的进一步部署,将实现LTE和2G/3G语音的完美融合。中兴通讯持续创新的融合语音解决方案有助于CSL继续保持领先地位,并为用户创造更加简单、便捷的生活方式。

中兴通讯是支持全制式接入的核心网设备供应商,中兴通讯All-IP的Uni-CORE核心网络解决方案覆盖固网软交换、移动软交换、IMS等各个领域。近日,中兴通讯面向全球发布了其最新的基于IMS的zMILE桌面多媒体应用解决方案,该方案是由IMS核心网、RCS标准的APP应用平台、基于Android操作系统的多媒体桌面终端(ZTE Light)组成的端到端IMS方案,助力运营商部署电信级多媒体/流媒体业务,为终端用户带来非同凡响的通信体验。截至2010年第3季度,中兴通讯核心网产品用户数达13.4亿,服务于全球110个国家。



## 专题:物联网技术及其应用

# 专 | 题 | 导 | 读

2009年8月,温家宝总理访问无锡中科院高新微纳传感网工程技术研发中心,提出“在激烈的国际竞争中,迅速建立中国的传感信息中心或感知中国中心”,在11月3日《让科技引领中国可持续发展》的讲话中,温家宝总理再次提出“要着力突破传感网、物联网关键技术,及早部署后IP时代相关技术研发,使信息网络产业成为推动产业升级、迈向信息社会的‘发动机’”,从而在神州大地大大加快了“物联网”技术发展与应用的热潮。

2003年,美国《技术评论》提出传感器网络技术将是未来改变人们生活的十大技术之首。传感器网络是由许多分布式自动装置组成的一种计算机网络,这些装置根据应用使用各种传感器,相互协调地监控不同位置的物理或环境状况(比如环境温度、物体声音、振动、压力、运动或污染物),并将采集的数据通过由无线传输方式组成的通信网络,传输到远端控制节点。人们利用传感器网络或射频自动识别技术实现对各种物品的自动识别,并通过通信网络实现物与物或物与人之间信息的互联与共享。

2005年在突尼斯举行的信息社会世界峰会上,国际电信联盟发布了《ITU互联网报告2005:物联网》,正式提出了“物联网(the Internet of Things)”的概念。物联网(IoT)是以传感网为末梢以信息智能应用为目的,对通信网络特别是互联网应用的进一步拓展和延伸。

IoT的应用非常广泛,可以应用到军事、工业、农业、电网和水网、交通、物流、节能、环保、医疗卫生、公共安全、智能家居等各个领域,在改造传统产业、引领新兴产业、提升人民生活、提供国家安全保障等方面都将起到重要作用。中国正处于经济结构转型的关键时期,重视并着力培育包括物联网在内的新一轮信息技术创新,进一步发挥信息技术的经济增长发动机作用,是必由之路。

本期专题一共收集8篇文章,分别涉及物联网体系研究、物联网和移动网的信息完全架构和技术、物联网的技术发展与标准化工作、物联网应用之一——车载物联网、物联网的海量数据智能管理等问题的研究。

感谢各位作者的大力支持,使本专题能够收集从不同角度探讨IoT热点问题的文章,希望有助于读者加深对物联网/传感网的理论、技术、应用和发展趋势的了解。

## 本期专题策划人



## 杨震

南京邮电大学校长、教授、博士生导师,第十、十一届全国人大代表,中国农工民主党中央副主席,中国通信学会副理事长和学术工作委员会主任,工业和信息化部电信经济专家委员会副理事长,中国通信企业协会常务理事,江苏省通信学会理事长,亚太通信会议 APCC Steering Committee 副主席;长期从事信号与信息处理、通信理论与技术的教学科研工作;主持和参加完成了国家科技支撑计划、国家“863”、国家自然科学基金、省部级等科研项目20多个;在国内外学术刊物和会议上发表学术论文近200篇;目前研究领域为无线通信网络、物联网和传感网、基于网络的分布式信号处理等。

## 2011年第1—6期专题计划

- 1 物联网技术及其应用**  
杨震 南京邮电大学校长
- 2 未来网络**  
侯自强 中国科学院声学研究所教授
- 3 车辆自组织网络及其应用**  
乐光新 北京邮电大学教授
- 4 三网融合演进技术与业务**  
李红滨 北京大学教授
- 5 新一代宽带移动通信创新技术**  
李少谦 电子科技大学教授
- 6 Pbit/s 光交换网络**  
徐安士 北京大学教授



## 中兴通讯技术

ZHONGXINGTONGXUN JISHU

双月刊 1995年创刊 总第96期

2011年2月 第17卷第1期

主管：安徽省科学技术厅

主办：中兴通讯股份有限公司

安徽省科学技术情报研究所

编辑：《中兴通讯技术》编辑部

总编：谢大雄

副总编：邓新

常务副总编：黄新明

责任编辑：杨勤义

编辑：朱莉, 卢丹, 徐辉, Paul Sleswick

排版制作：余刚

发行：王萍萍

编务：王坤

《中兴通讯技术》编辑部

地址：合肥市荣事达大道450号

邮编：230041

网址：http://www.zte.com.cn/magazine

投稿平台：http://www.zte.com.cn/paper

电子信箱：magazine@zte.com.cn

电话：(0551)5533356

传真：(0551)5850139

出版、发行：中兴通讯技术杂志社

发行范围：国内外发行

印刷：合肥中建彩色印刷厂

出版日期：2011年2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10.00元，全年60.00元

# 目次

## 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。

### 卷首特稿

01 中国三网融合的特点与挑战 ..... 邬贺铨

### 专题:物联网技术及其应用

03 从云计算到海计算:论物联网的体系结构 ..... 孙利民, 沈杰, 朱红松

08 物联网技术架构 ..... 沈苏彬

11 IoT/CPS的安全体系结构及关键技术 ..... 丁超, 杨立君, 吴蒙

17 基于物联网的网络信息安全体系 ..... 刘宴兵, 胡文平, 杜江

21 移动网络安全防护技术 ..... 胡爱群, 李涛, 薛明富

27 物联网技术及其标准 ..... 诸瑾文

32 车载物联网技术探讨 ..... 俞波, 须成忠, 过敏意

38 IoT的数据管理与智能处理 ..... 李玲娟

### 专家视点

42 向未来互联网演进 ..... 何宝宏

### 运营应用

45 分布式智能开放运营架构及关键技术 ..... 董晓渝, 张云勇, 房秉毅

### 研究论文

49 基于业务感知的认知网络 QoS 自适应控制技术 ..... 顾成杰, 张顺颐, 孙雁飞

### 开发园地

53 LTE 网络覆盖规划技术研究 ..... 顾军, 盛韧

### 系列讲座

57 分组通信网的同步与定时技术(1) ..... 王文翥, 王斌, 糜正琨

### 综合信息

中兴通讯发布基于IMS的zMILE桌面多媒体应用解决方案(2) 中兴通讯为日本UQC规模部署WiMAX Pico商用基站(7) 《中兴通讯技术》杂志更改英文刊名公告(10) 中兴通讯荣膺《亚洲电信》“最佳年度宽带网络供应商”(31) 广告索引(37) 中兴通讯已拥有235项LTE基本专利(41)

期刊基本参数: CN 34-1228/TN \* 1995 \* b \* 16 \* 64 \* zh \* P \* ¥10.00 \* 15000 \* 14 \* 2011-02

# Contents

ZTE TECHNOLOGY JOURNAL Vol.17 No.1 Feb. 2011

## Guest Paper

01 Features and Challenges of Converged Networks in China ..... WU Hequan

## Special Topic: Internet of Things and Its Applications

03 From Cloud Computing to Sea Computing:  
The Architecture of the Internet of Things ..... SUN Limin, SHEN Jie, ZHU Hongsong

08 The Technology Framework of IoT ..... SHEN Subin

11 Security Architecture and Key Technologies  
for IoT/CPS ..... DING Chao, YANG Lijun, WU Meng

17 Network Information Security Architecture Based  
on Internet of Things ..... LIU Yanbing, HU Wenping, DU Jiang

21 Security Service Technology for Mobile Networks ..... HU Aiqun, LI Tao, XUE Mingfu

27 Internet of Things: Technologies and Standard ..... ZHU Jinwen

32 Vehicular Networks : A Case for the Internet of Things ..... YU Bo, XU Chengzhong, GUO Minyi

38 Data Management and Intelligent Processing in IoT ..... LI Lingjuan

## Expert View

42 Evolving Towards the Future Internet ..... HE Baohong

## Operational Application

45 Architecture and Key Technology of Distributed Intelligent  
Open Systems ..... TONG Xiaoyu, ZHANG Yunyong, FANG Bingyi

## Research Paper

49 QoS Self-Adaptive Control in Cognitive Networks Based  
on Service Awareness ..... GU Chengjie, ZHANG Shunyi, SUN Yanfei

## Development Field

53 Research into LTE Network Coverage Planning ..... GU Jun, SHENG Ren

## Lecture Series

57 Synchronization and Timing Technology  
of Packet Communication Networks (1) ..... WANG Wennai, WANG Bin, MI Zhengkun

## 《中兴通讯技术》编辑委员会

主 任 钟义信

副主任 侯为贵 糜正琨

编委(按姓氏拼音顺序排列)

艾 波 曹淑敏 常金芸 陈常嘉  
陈建平 陈 杰 陈锡生 程时端  
程时昕 高 文 龚双瑾 古永承  
顾晚仪 郭云飞 侯为贵 何士友  
洪 波 纪越峰 江 华 蒋林涛  
雷震洲 李红滨 李建东 李乐民  
李少谦 李 星 孟洛明 糜正琨  
倪 勤 史立荣 谈振辉 田文果  
王晓明 王晓云 王育民 韦乐平  
卫 国 谢大雄 谢希仁 徐安士  
须成忠 续合元 杨义先 杨 震  
殷一民 尤肖虎 乐光新 张同须  
张智江 赵厚麟 赵慧玲 赵先明  
钟义信 周苏苏 朱近康

## 敬告读者

一、本刊享有所有发表文章的版权,包括英文版、电子版和网络版权,所支付的稿酬已包含上述各版本的费用。

二、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,请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。

三网融合,已成为继3G、物联网、云计算之后的又一热门话题,越来越多地引起人们关注,世界各国也纷纷将三网融合作为培育战略性新兴产业的重要工程。值此新年来临之际,本刊荣邀中国工程院院士、中国著名通信专家邬贺铨先生就中国三网融合的发展特点与挑战发表观点。

邬院士认为,发达国家已经实现或正在深入推进三网融合,而中国的三网融合有其特色,既能引出新的管理模式也能带来新的挑战。

邬院士指出,在中国三网融合进程中需要新的管理模式,而集成播控平台的引入给管理模式带来新的挑战,并需要合作创新来适应。

邬院士强调,新业务的开发和商业模式的设计将成为三网融合成败的关键。

# 中国三网融合的特点与挑战

邬贺铨/WU Hequan



邬贺铨,中国工程院院士,长期从事数字和光纤通信系统的研究开发工作,近年负责组织下一代互联网和3G及LTE的研发项目。曾任中国工程院副院长,现为国家信息化专家咨询委员会副主任、工业和信息化部通信科技委顾问、中国电子学会副理事长、中国通信学会副理事长、中国通信标准化协会理事长、国务院三网融合专家组组长、CNGI项目专家委员会主任。

2010年政府工作报告中关于三网融合有如下注释,“三网融合是电信网、广播电视网和互联网融合发展,实现三网互联互通,资源共享,为用户提供话音、数据和广播电视等多种服务”。三网融合试点已经启动,其任务是推动广电与电信业务双向进入,加快网络建设改造和统筹规划,强化网络信息安全和文化安全的监管,切实推动产业发展。

一些发达国家已经实现或正在深入推进三网融合,但中国的三网融合有其特色,既能引出新的管理模式也能带来新的挑战:

一是中国目前广电网络的数字化、双向化比例还比较低,广电要进入电信业务的前提是借三网融合加快实现网络数字化和双向化,广电部门提出要用中国下一代广播电视网(NGB)来完成这一改造。NGB采用IP技术强化了对电信业务的支持,但在广播式视频传送中采用分组技术则是一种新的尝试,其技术经济性还有待验证。

二是中国特别重视三网融合的安全问题。当电视机成为上网终端时,原来不会遭遇黑客和病毒攻击的广电网也不再是世外桃源。开放互联网中难以清除的各种不良信息内容,也有可能出现在手机乃至家中的电视机屏幕上。广电网现有安全平台、技术手段、保障机制难以适应融合后激增的网络视频流量,电视台现有播控机制也需要改进以适应多业务运营下的业务集成环境。总之,信息内容安全与网络安全任务任重。

三是需要有新的管理模式。出于内容安全的角度考虑,电信进入广电业务的准入条件是视频业务须由广电部门的集成播控平台管理,内容管理到什么程度还需要有明确和合理的规定,集成播控平台的接口与功能要求还有待标准来明确。交互式网络电视(IPTV)的效益体现在与之伴随的基于互联网的增值服务上,这些业务可能不是视频业务,并不需要通过集成播控平台。增值服务如何与需要通过集成播控平台的IPTV配



合,这是中国三网融合必须面对的问题。此外集成播控平台不仅要管理内容,在试点方案中还要求对用户与计费进行管理。这意味着用户在一次接入中可能同时涉及电信与广电两方面的运营管理,这对网管系统和客户管理体制带来了挑战。如

何从用户出发协调广电与电信运营商的管理及服务责任也是新的考验。总之集成播控平台的引入带来管理模式上新的命题,需要合作创新来适应。这些问题的解决既与管理体制的改革有关,也与服务模式有关。

四是试点方案对接入带宽有明确要求。2012年入户广播下行带宽超过2 Gbit/s,宽带接入能力则超过了100 Mbit/s,电信下行接入能力超过1 Gbit/s,入户能力超过100 Mbit/s。中国城市人口居住密集,光纤到楼/光纤到小区(FTTB/FTTZ)的成本会比发达国家低得多,它已成为中国三网融合的主要接入方式。电信运营商可

能采用FTTB/FTTZ+数字用户线路/局域网(DSL/LAN),广电运营商可能采用FTTB/FTTZ+EoC。在FTTB/FTTZ中EPON或GPON(或二者的结合)适合中国用户密集的情况。由于三网融合涉及海量用户,开发低成本PON等接入系统仍然是使三网融合成功

的重要因素。虽然100 Mbit/s的入户能力对光纤接入系统不算难题,但每用户100 Mbit/s接入将对核心网特别是城域网产生很大的压力。中国100 Mbit/s入户这一要求走在一些发达国家之前,但与此同时高带宽需要高价值和高回报,这就需要我们探索适合中国接入网环境的先进、合理的技术,并开发新型宽带业务和商业模式,即对用户有价值且能够使运营商有可持续发展的回报。根据中国互联网络信息中心(CNNIC)的统计,网民上网费用占网民可支配收入的4%左右,如果再加上移动通信的支出,通信的费用占收入的比例超过发达国家的水平。尽管如此电信运营商

仍感到缺乏可赢利模式,因此新业务的开发和商业模式的设计将成为三网融合成败的关键。

五是组播问题。本来这是其他国家在部署IPTV业务时都遇到的问题,但中国用户数之多是其他国家无法比拟的。现有电信网需要改造为能支持大规模组播的可管理IP网,但基于路由器的网络层组播实现复杂,基于终端的应用层组播虽不用改变原来的网络基础设施,易于部署应用,但稳定性和效率不如网络层组播,另外存在组播视频源欺骗、非法用户注册报文欺骗等多种风险,这就要求开发大容量安全易管理的IPTV组播解决方案。

六是目前广电与电信的监管体制、广电企业的性质与规模等与其他国家不同,在网络技术、业务和维护管理上将会反映出体制的影响。

三网融合被作为深化电信体制改革、培育战略性新兴产业和惠及民生的重要工程,寄予推动电信业和广电业科学发展的重任,需要电信业和广电业产业链上下游共同努力。三网融合任重道远,2011年甚为关键。

收稿日期:2010-12-20

## 综合信息

### 中兴通讯发布基于IMS的zMILE桌面多媒体应用解决方案

【本刊讯】中兴通讯面向全球发布了基于IMS的zMILE多媒体应用解决方案,帮助运营商基于现网平滑部署多媒体和流媒体业务,为传统固定电话用户带来非同凡响的多媒体和流媒体应用体验。

中兴通讯在业界首创的zMILE方案基于IMS全业务端到端方案构建,包含IMS核心网、RCS标准的APP应用平台、基于Android操作系统并支持RCS标准的多媒体终端。除传统的语音和短信业务外,zMILE提供丰富多彩的多媒体和流媒体业务,包括:IPTV、rich calls、媒体共享、高清多媒体会议、监控、Web IMS applications、即时消息、多媒体彩铃/彩像、好友列表等。

zMILE采用划时代革命性的多媒体桌面终端ZTE

Light替代现有传统PSTN/ISDN/SIP桌面终端。ZTE Light 7英寸大小屏幕,全触摸屏式应用,时尚、直观、便携,并附带手持移动拨号手柄,用户能够像普通话机一样拨打和接听电话,完全顺应传统用户的语音业务使用习惯,支持3G、Wi-Fi、FTTx、xDSL等各种接入方式。

中兴通讯是业界领先的IMS端到端综合方案提供商,创新的zMILE方案采用业界标准的IMS核心网和RCS规范的APP构建,IMS核心网为多媒体/流媒体业务提供电信级QoS保证,在安全、计费、支持固定和移动接入以及和现网互联互通方面提供完善的方案。RCS是业界广泛认同的多媒体业务规范,采用RCS标准的APP和终端具有良好的互通性和升级能力。zMILE作为在业界具有里程碑意义的多媒体应用解决方案,必将给用户和运营商带来全新的变革。



# 从云计算到海计算: 论物联网的体系结构

## From Cloud Computing to Sea Computing: The Architecture of the Internet of Things

中图分类号:TN91 文献标志码:A 文章编号:1009-6868(2011)01-0003-05

**摘要:** 基于对物联网概念的理解,文章介绍了物联网的特征,特别是其底层感知信息的时空特性和局部实时交互性,以及对物理世界的感知、感知信息的传输和处理、对物理空间的反馈控制的开放式循环过程。基于云计算到海计算再到云海结合,从信息存储和处理的角度出发,文章探讨了物联网承载和处理巨海量信息的方式和结构,以及物联网体系结构需要考虑的问题,如开放性式循环结构和智能终端。

**关键词:** 物联网;体系结构;云计算;海计算;智能终端;开放式循环结构

**Abstract:** The most salient features of IoT are its spacial and temporal perception of information and the local real-time interaction, the open-cycle of perceiving, transmitting, and processing perceived information, and feedback control of the physical world. This paper considers sea computing and the combination of sea and cloud computing in discussing the architecture needed to bear and process mass information in IoT. Some proposals on the design of open-cycle structure and intelligent terminals are also made.

**Keywords:** Internet of things; architecture; cloud computing; sea computing; intelligent terminals; open-cycle structure

孙利民/SUN Limin<sup>1</sup>

沈杰/SHEN Jie<sup>2</sup>

朱红松/ZHU Hongsong<sup>1</sup>

(1. 中国科学院软件研究所,北京 100190;

2. 无锡物联网产业研究院,江苏 无锡

214135)

(1. Chinese Academy of Sciences Institute of Software, Beijing 100190, China;

2. Wuxi SensingNet Industrialization Research Institute, Wuxi 214135, China)

物联网实现全球亿万种物品之间的互连,将不同行业、不同地域、不同应用、不同领域的物理实体按其内在关系紧密地关联在一起,对小到螺丝、铅笔,大到飞机、轮船等巨量物体进行联网与互动。物联网能够实现社会活动和人们生活方式的变革,被预言为继互联网之后新的全球信息化产业浪潮,受到各国政府、企业和学术界的广泛重视。

从信息技术角度看,物联网是指具有感知和智能处理能力的可标识的物体,基于标准的可互操作的通信

**基金项目:** 基金项目:国家重点基础研究发展(“973”)规划(2011CB302900);国家科技重大专项(2009ZX03006-001-01)

协议,在宽带移动通信、下一代网络和云计算平台等技术的支撑下,获取和处理物体自身或周围环境的状态信息,对事件及其发展及时做出判断,提供对物体进行管理和控制的决策依据,从而形成信息获取、物体管理和控制的全球性信息系统。物体能够在人类直接干预或无需人工干预条件下感知事件、触发动作和生成服务,通过协同的感知和互动来影响甚至控制事件向有利的方向发展。物联网充分体现了物理世界和信息空间的深度融合,使人类可以融入到一体化的智能生态环境中,实现人、机、物的协同统一。

作为崭新的综合性信息系统,物

联网并不是单纯的网络概念,它包括信息的感知、传输、处理决策、服务等多个方面,呈现出自身显著的特点。首先是对客观物理世界的全面感知,它不仅表现在对单一的现象或目标进行多方面的观察获得综合的感知数据,也表现在对现实世界各种物体现象的普遍感知;其次是物联网实体间的泛在互联,表现在各种物体经由多种接入模式实现异构互联,也突出表现在物联网不仅包括互联网、电信网等公共网络,还包括电网和交通网等专用网络,错综复杂,形成“网中网”的形态;第三是智慧的信息处理和决策,它体现在物联网中从感知到传输到决策应用的信息流,并最终为控制提供支持,也广泛体现出物联网中大量的物体和物体之间的关联和互动。物体互动经过从物理空间到信息空间,再到物理空间的过程,形成感知、传输、决策、控制的开放式的循环。

物联网不同于感知信息收集的传感器网络,也不同于信息传输的互联网。它包含亿万种多样的物体,承

载和处理巨海量的感知信息,容纳各种模式的接入和通信模式,实现从感知、处理到控制的循环过程。其系统架构如何构成,采用什么样的体系结构,现已成为物联网研究的核心问题之一。

## 1 从云计算到海计算

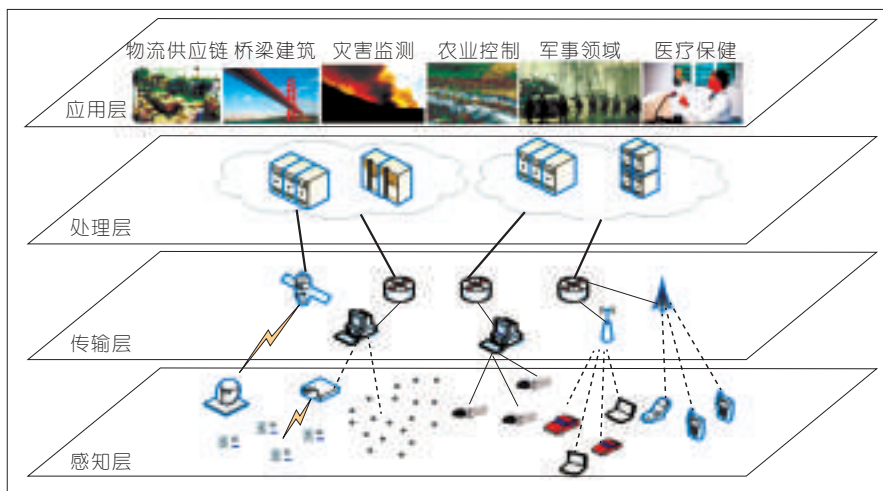
### 1.1 云计算

云计算是互联网发展带来的一种新型计算和服务模式,它是通过分布式计算和虚拟化技术建设数据中心或超级计算机,以租赁或免费方式向技术开发者或企业客户提供数据存储、分析以及科学计算等服务。广义上讲,云计算是指厂商通过建立网络服务集群,向多种客户提供硬件租赁、数据存储、计算分析和在线服务等不同类型的服务。云计算的主要服务形式有以亚马逊公司为代表的基础设施即服务,以 Salesforce 为代表的平台即服务,以及以微软代表的软件即服务等。

云计算的“云”就是存在于互联网的服务器集群上的服务器资源,包括硬件资源(如服务器、存储器和处理器等)和软件资源(如应用软件、集成开发环境等)。本地终端只需要通过互联网发送一条请求信息,“云端”就会有成千上万的计算机为你提供需要的资源,并把结果反馈给发送请求的终端。每个提供云计算服务的公司,其服务器资源分布在相对集中的世界上少量几个地方,对资源基本采用集中式的存放管理,而资源的分配调度采用分布式和虚拟化技术。云计算强调终端功能的弱化,通过功能强大的“云端”给需要各种服务的终端提供支持。如同用电用水一样,我们可以随时随地获取计算、存储等信息服务。

### 1.2 物联网

图1所示是欧盟发展框架7的CASAGRAS<sup>[1]</sup>工作组给出的物联网体



▲图1 物联网体系架构

系架构,包括感知层、传输层、处理层和应用层4个层次。在感知层中,嵌入有感知器件和射频标签(RFID)的物体形成局部网络,协同感知周围环境或自身状态,并对获取的感知信息进行初步处理和判决,以及根据相应规则积极进行响应,同时,通过各种接入网络把中间或最终处理结果接入到传输层;传输层包括宽带无线网络、光纤网络、蜂窝网络和各种专用网络,在传输大量感知信息的同时,对传输的信息进行融合等处理;在处理层提供存储和处理功能,表现为各种各样的数据中心以中间件的形式采用数据挖掘、模式识别和人工智能等技术,提供数据分析、局势判断和控制决策等处理功能。云计算的“云端”就在处理层,主要通过数据中心来提供服务;最上层的应用层建立不同领域中的各种应用。

互联网也可以看成存在类似的架构,底层是数据传输的网络支撑层,中间是数据中心的处理层和上层是各种互联网应用。从层次架构来看,物联网不同于互联网的原因在于它的感知层。感知层获取数据的特性决定了物联网的上层相应要发生一些变化。

### 1.3 海计算

物联网具有显著的异构性、混杂

性和超大规模等特点。异构性表现在不同制造商、不同拥有者、不同类型、不同级别、不同范畴的对象网络共存于物联网中,网络之间在通信协议、信息属性、应用特征等多个方面存在差异性,并形成混杂的异构网络或“网中网”形态;混杂性表现在网络形态和组成的异构混杂性,多信息源的并发混杂性,场景、服务和应用的混杂性等多个方面;物联网是物理世界与信息空间的深度融合系统,是涉及全球的人、机、物的综合信息系统,其规模之大无所不包。

物联网的上述特点决定了感知层数据的特性,即异构的、混杂的、大规模的实时流感知数据。同时,感知数据还具有一个显著特点就是时空特性,就是感知数据在特定时间和特定空间内才有意义,如果不在这个地点或过了这个时间,数据的意义可能就不大了。如中关村大街的交通相关信息,这些交通信息通过很多节点实时采集,是大数据量的随时间不断采样的实时流信息。这些信息谁需要?是在这个区域的人车才真正需要了解当时的详细拥塞或停车信息等,以便及时掌握交通动态,调整行车路线或停止地方。其他地方的人们可能不关心这个区域的交通信息,或仅仅只需要了解大概情况,实时性要求也不是很高,如了解中关村大街

的历史交通信息等。另外,物联网的物体之间需要协同交互,对事件及时做出反应,这就需要实时性采集、处理和控制,如在中关村大街上前后行驶的两辆车需要实时交互,既要保持畅通行驶,又要通过保持一定的车距来保证安全性,这就需要在当前场景下局部空间内车辆之间实时通信和决策处理。

为此,我们针对物联网这些数据的特性提出了哑铃式的存储和计算模式。大量的感知信息在采集和使用的本地进行存储,经过处理后的中间或最后结果存储在互联网上(后端),放到云中的数据中心。感知信息的预处理、判断和决策等信息处理主要在当前场景下的前端完成,必要的需要大运算量的计算才通过“云端”的数据中心来处理。只有这样,才能节省通信带宽,否则网络很难传输这么多的感知数据;才能节省存储空间,数据中心再大也难存下实时流的原始感知数据,也没有必要存储原始感知数据;才能满足实时性的交互处理,如果通过互联网或云计算来做出处理和决定,就不能满足很多实时性的应用;更重要的是能够满足物联网的大规模的扩展性。物联网一定是分布式的系统,局部空间内的高度动态自治管理才有利于扩展性。

中科院现在提出“海计算”<sup>[2]</sup>这个新的计算模式,实质是把智能推向前端。智能化的前端具有存储、计算和通信能力,能在局部场景空间内前端之间协同感知和判断决策,对感知事件及时做出响应,具有高度的动态自治性。海计算的每个“海水滴”就是全球的每个物体,它们具有智能,能够协助感知互动。亿万种物体组成物联网系统,就如同海水滴形成大海一样。

#### 1.4 云海结合

物联网涉及到全球的物体(包括人)规模,以及其应用需求和感知层数据的特性,决定了物联网的架构需

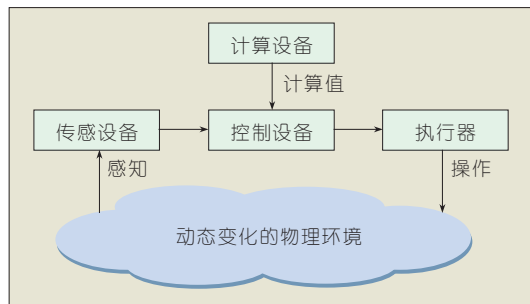
要“云”和“海”相结合。一方面,在局部应用场景中,感知数据存储在局部现场,智能前端在协同感知的基础上,通过实时交互共同完成事件判断、决策等处理,及时对事件做出反应。另一方面,云计算的“云”的后端提供面向全球的存储和处理服务。物联网的各种前端把处理的中间或最后结果存储到云的后端。前端在本地处理过程中,在必要时需要后端的存储信息和处理能力的支持,及时发送服务请求获得云的后端支持。这具有良好的扩展性,既满足前端实时交互,又满足全球物体的互联互通。

## 2 物联网体系结构

除了获取、承载和处理超海量的感知信息这个显著特征外,物联网的另一个显著特征就是具有决策和控制功能,能够影响物体周围的环境或控制事件的进程;就是通过对物理世界的感知,对感知信息的传输和处理,到对事件的判断和决策,再回到控制执行器进行执行动作,从而对事件产生作用来影响事件的进程,形成从物理世界到信息空间再到物理世界的循环过程。

### 2.1 开放式循环结构

物联网形成人机物的协调环境系统,包含从感知、传输、处理和控制的循环过程。物联网由亿万种物体、设备和人参与形成或与物理环境共存,这些对象之间存在极其复杂的关系(或称为关系链)。一个事件往往受到多种因素影响,这些因素本身也是动态变化的。如移动车辆在移动过程中所处局部环境具有高度动态性,因为车况、路况、周围车辆、无线接入网络等一直在变化。多种因素均会影响车辆间产生碰撞,造成交通事件,通过智能的感知、通信和控制人们可以避免车辆碰撞。这使得物联网的信息循环不同于传统的闭环控



▲图2 物联网开放式循环结构

制,而是开放式的循环过程<sup>[3]</sup>。物联网开放式循环结构如图2所示。传感设备的感知信息包括物理环境的信息和物理环境对系统的反馈信息,执行器改变物理实体状态和实现系统对物理环境的反馈。系统会预先设定控制语义。计算设备对物理信息进行计算和判断,当判断值在控制语义下满足一定的触发条件时,控制设备会发送命令给执行器。

由于物理环境、感知目标存在混杂性,信息设备存在一定的误差,以及其状态、行为存在不确定性等,对于循环结构而言,会带来获取的感知信息的不准确性,以及物体控制的不可靠性。因此,如何全面准确地获取感知信息,以及如何保证控制过程和结果符合设计要求,是开放式循环结构的两个重要方面。

### 2.2 智能前端

随着微电子、计算和通信等技术的发展,在物体中嵌入微型的感知、处理和通信等功能部件成为可能。越来越多的物体成为物联网的智能前端,带动物联网逐步应用和发展。智能前端兼有感知信息的获取、决策操作的执行,以及诸多的处理和交互功能,是局部自治环境中的终端实体,也是物联网的基本单元。

下面结合物联网的典型应用之一智能交通来说明前端的智能化。车辆安全系统能在人工干预或无需人工干预情况下,保证高速车辆的安全行驶,是智能交通的核心内容。图3所示是车辆安全协作系统架构<sup>[4]</sup>示



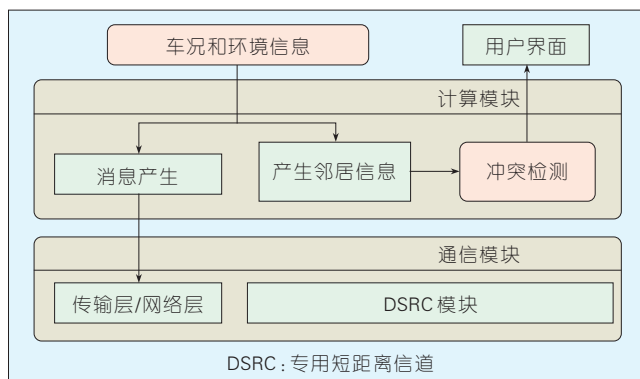


图3  
车辆安全协议系统架构

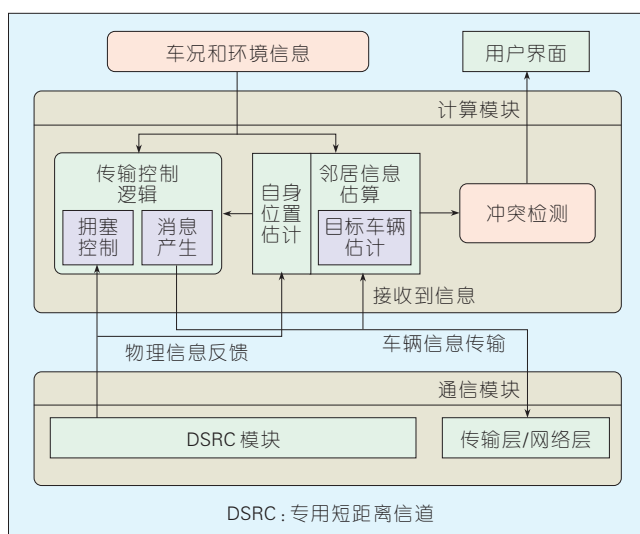


图4 更智能化的  
车辆安全协议系统架构

意图。车辆通过传感器、全球定位系统(GPS)等设备收集车辆自身与周围环境的信息。计算模块中的消息产生机制产生车辆状态信息,并通过无线车载网络将状态消息广播给周围车辆。车辆通过专用短距离信道(DSRC)接收邻居车辆的状态信息,根据自身和多个邻居车辆的状态信息,预测车辆之间及车辆与周围环境之间的位置关系,以及可能发生的碰撞,及时调整车辆操作参数来提高车辆行驶的效率 and 保障安全。

图3所示的架构仅仅把车辆状态信息及时广播出去,在车辆多的情况下,有可能产生信息传输延迟较大,甚至信息丢失。Fallah<sup>[6]</sup>等人考虑无线网络的通信状态,给车辆赋予更智能的功能,如图4所示。与传统的车辆安全协作系统架构不同之处在于,传输控制单元根据无线车载网络的

信道情况和状态信息,调整发送的频率和消息长度,根据自身位置估计模

型和实际位置决定是否发送自身位置信息,从而提高了系统的鲁棒性和扩展性。

### 2.3 融合系统体系结构

体系结构是对系统的抽象描述。物联网系统既涉及规模庞大的智能电网,又包含智能医疗的医疗设备。目前世界各国都在结合具体行业推广物联网的应用,离形成全球的物联网系统还需要非常长的时间。提出面向全球物联网、适应各种行业应用的体系结构,与下一代互联网体系结构相比,具有更巨大的困难和挑战。现在研究人员通常只是从具体行业或小的系统去探索物联网的体系结构。

物联网与物理信息融合系统(CPS)<sup>[6-9]</sup>密切相关,这两个概念目前越来越趋向一致。Tan.Y<sup>[10]</sup>等人提出了一种CPS体系结构的原型,如图5所示。图5表示了物理世界、信息空间和人的感知的互动关系,给出了感知事件流、控制信息流的流程。

CPS体系结构原型的几个组件描述如下:

#### (1) 物理世界

物理世界包括物理实体(诸如医

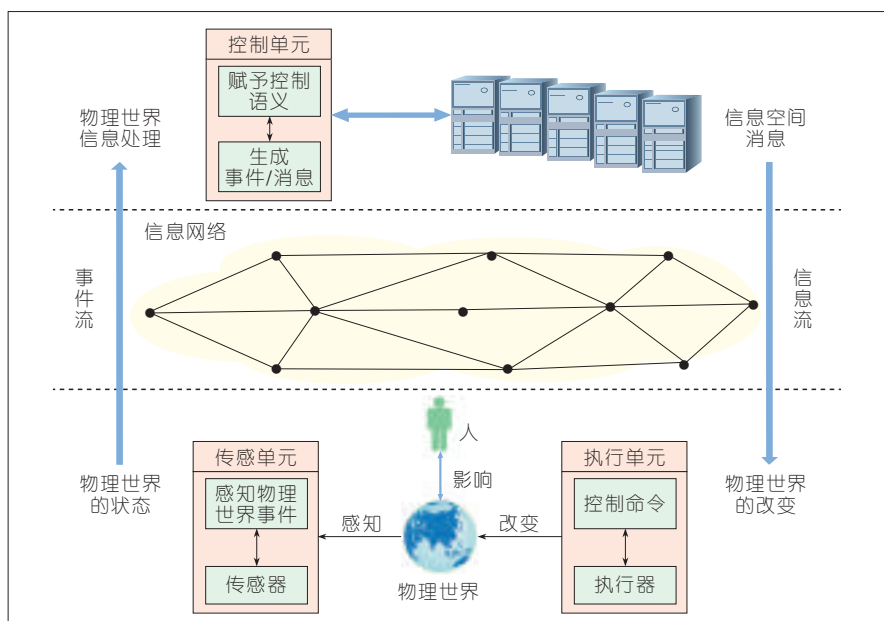


图5 CPS体系结构原型

疗器械、车辆、飞机、发电站)和实体所处的物理环境。

#### (2) 传感器

传感器作为测量物理环境的手段,直接和物理环境或现象相关。传感器将相关的信息传输到信息世界。

#### (3) 执行器

执行器根据来自信息世界的命令,改变物理实体设备状态。

#### (4) 控制单元

基于事件驱动的控制单元接受来自传感单元的事件和信息世界的信息,根据控制规则进行处理。

#### (5) 通信机制

事件/信息是通信机制的抽象元素。事件既可以是传感器表示的“原始数据”,也可以是执行器表示的“操作”。通过控制单元对事件的处理,信息可以抽象地表述物理世界。

#### (6) 数据服务器

数据服务器为事件的产生提供分布式的记录方式,事件可以通过传输网络自动转换为数据服务器的记录,以便于以后检索。

#### (7) 传输网络

传输网络包括传感设备、控制设备、执行设备、服务器,以及他们之间的无线或有线通信设备。

### 3 结束语

虽然人们提出物联网这个词已有一段时间,但物联网的概念一直在不断的发展和演变。从最早的传感器网络和基于RFID的物体不断被跟踪记录,现已发展到物体的智能化,能够协同感知和交互,以及全球物体之间的深度互联和互动。目前,人们从不同行业探讨物联网的应用,进行“竖井式”的研发和推广应用。但是,到跨行业、跨领域,直到全球物体之间的互联互动,还有相当长的艰苦道路要走,现在只是勾画出人类信息发展的一个美好前景。

就像互联网改变人们的交流方式和商业模式一样,物联网也会改变人、信息空间和和物理世界的交互方

式。它将人们所在物理世界和虚拟世界桥连起来,实现人与人、人与物、物与物的紧密耦合,形成一个智能、绿色、和谐的世界。物联网需要我们长期研究和探索其中的理论和技术问题。

### 4 参考文献

- [1] Coordination and Support Action for Global RFID-Related Activities and Standardization [EB/OL]. [2008-01-01]. <http://www.eeca-ict.eu/successstories/s13.pdf>.
- [2] 孙凝晖,徐志伟,李国杰.海计算:物联网的新型计算模型[J].中国计算机学会通讯,2010(2):39-43.
- [3] ASTROM K J, MURRAY R M. Feedback Systems: An Introduction for Scientists and Engineers [M]. Princeton, NJ, USA: Princeton University Press, 2008.
- [4] XU Q. Vehicle-to-Vehicle Safety Messaging in DSRC [C]//Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET'04), Oct 1, 2004, Philadelphia, PA, USA. New York, NY, USA: ACM, 2004:19-28.
- [5] FALLAH Y P, HUANG C L, SENGUPTA R, et al. Design of Cooperative Vehicle Safety Systems based on Tight Coupling of Communication, Computing and Physical Vehicle Dynamics [C]//Proceedings of the 1st ACM/IEEE International Conference on Cyber-physical Systems (ICCPs'10), May 25-28, 2010, Stockholm, Sweden. New York, NY, USA: ACM, 2010:159-167.
- [6] GROUP C S. Cyber-Physical Systems: Executive Summary [R/OL]. [2008-03-06] <http://varma.ece.cmu.edu/Summit>.
- [7] LEE E A. Cyber Physical Systems: Design Challenges [C]//Proceedings of the 11th IEEE International Symposium on Object/Component/Service-Oriented Real-time Distributed Computing (ISORC'08), May 5-7, 2008, Orlando, FL, USA. Piscataway, NJ, USA: IEEE, 2008:363-369.
- [8] LEE E A. Cyber-Physical Systems: Are Computing Foundations Adequate [R/OL]. [2006-10-16-17]. <http://citeseerx.ist.psu.edu/viewdoc/download>.
- [9] STANKOVIC J A. Opportunities and Obligations for Physical Computing Systems [J]. Computer, 2005,38(11):23-31.
- [10] YING T, VURAN M C, GODDARD S. Spatio-Temporal Event Model for Cyber-Physical Systems [C]//Proceedings of the 29th International Conference on Distributed Computing Systems (ICDCS'09), Jun 22-26, 2009, Montreal, Canada. Piscataway, NJ, USA: IEEE, 2009:44-50.

收稿日期:2011-12-13

#### 作者简介



孙利民,中国科学院软件研究所研究员、博士生导师,中国计算机学会高级会员,计算机学会传感器网络专业委员会副主任,计算机学会互联网专业委员会委员,中关村物联网产业联盟副理事长,国家物联网基础标准工作组组长;主要研究方向为无线传感器网络和物联网;主持和参与基金项目10项;已发表论文100篇,出版学术著作3部,申请国家专利30项。



沈杰,无锡物联网产业研究院研究总监,全国信标委传感器网络标准化工作组主要筹建人之一及“标准体系与系统架构”项目组组长,ISO/IEC JTC1传感器网络系统架构国际标准主编,CCSA 泛在网技术工作委员会(TC10)副主席;主要研究方向为物联网、传感网系统架构、网络通信等;主持和参与基金项目10项;获上海市科技进步一等奖1项,已申请国家发明专利13项;已发表论文10余篇。



朱红松,中国科学院软件研究所高级工程师;主要研究方向为无线自组织网络、分布式系统控制等;主持和参与基金项目5项;已发表SCI/EI检索论文10篇。

### 综合信息

#### 中兴通讯为日本UQC规模部署WiMAX Pico商用基站

【本刊讯】2010年12月1日,日本第二大移动运营商KDDI旗下UQC正式宣布:中兴通讯和本土服务伙伴日立将为其在全国范围内部署WiMAX Pico。该项目首期建设规模超过1200个基站,并将逐步在日本全境商用。此次部署是中兴通讯无线系统设备首次规模突破日本这一世界上以进入资质严苛著称的电信市场。中兴通讯、日立和UQC在WiMAX网络建设上的合作证实了中兴通讯在无线宽带领域的技术领先性及客户认可度。

# 物联网技术架构

## The Technology Framework of IoT

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0008-03

**摘要:** 文章基于物联网的三维概念模型, 提出了一个由信息物品、自主网络和智能应用技术构成的物联网技术架构, 并且分析了这3类物联网技术的特征, 建议物联网研究和开发不仅需要关注信息物品的标识和传感技术, 还需要关注自主网络和智能应用中的核心技术。

**关键词:** 物联网; 技术架构; 信息物品; 自主网络; 智能应用

**Abstract:** This paper proposes a technical framework for IoT based on a three dimensional concept model and consisting of digital things, autonomic network, and intelligent application technologies. It analyses the features of these three classes of technologies and suggests that R&D of IoT will focus on those technologies that can identify and sense things, and on technologies for autonomic network and intelligent applications.

**Keywords:** Internet of things; technology framework; digital things; autonomic network; intelligent applications

沈苏彬 / SHEN Subin

(南京邮电大学 计算机学院/软件学院, 江苏  
南京 210003)  
(School of Computer/Software, Nanjing  
University of Posts and Telecommunications,  
Nanjing 210003, China)

性的失误, 加速中国物联网研究和开发的进程。

### 1 物联网技术分类方法

物联网是一项正在研究和开发的系统, 目前并不存在ITU定义的物联网系统, 即客观上目前并不存在物联网技术架构。本文介绍的物联网技术架构也仅仅是基于目前对物联网认识的一种推测, 为了保证这种推测的客观性和合理性, 本节将介绍这种推测的过程以及对物联网技术分类的方法。

根据我们研究的结论<sup>[2]</sup>, 物联网主要解决物品到物品(T2T)、人到物品(H2T)、人到到(H2H)之间的互连。T2T、H2T、H2H这3个层面的互连是物联网不可缺少的, 单纯物品与物品之间的互连并不构成一个物联网, 单纯在局部范围之内连接某些物品也不构成物联网, 物联网一定是由物品可以自然连接的因特网。这里有两个概念是在讨论物联网中不可忽略的: 其一, 物联网一定属于未来因特网, 物联网一定是未来网络社会的基础设施, 即物联网一定可以自然扩展到全球的系统; 其二, 物联网中物品的连接一定是“自然连接”, 也就是保留了物品在物理世界中时间和空间特性的连接。如果我们把某些物品

物联网的研究与开发存在一些有争议的话题, 其中一个就是: 物联网是否具有自身的技术架构? 针对这个话题, 存在多种不同的观点。一种“物联网无技术论”观点认为, 物联网仅仅是现有技术的集成, 没有自身的技术架构; 另一种“物联网泛技术论”观点认为, 物联网技术遍布应用信息技术的各行各业, 涉及到信息技术研究和开发的各个领域。本文认为, 物联网虽然具有计算机、通信、网络、控制和电子等方面技术特征, 但现有这些技术的简单集成无法构成一个灵活、高效、实用的物联网。物联网是在融合现有计算机、网络、通信、电子和控制等技术的基础上, 通过进一步的研究、开发和应用, 形

成自身的技术架构。

物联网还是一种新技术, 虽然国际电信联盟(ITU)在2005年就提出了物联网技术<sup>[1]</sup>, 描绘了物联网应用的美好场景, 并且预测这项技术可以推动全球的发展, 特别是推动发展中国家的。但迄今为止并没有研究和开发成功完整的物联网技术, ITU定义的物联网目前并没有实现。局部范围内某些具有物联网特征的系统并不是真正意义上的物联网, 具有某种感知物品信息的系统也不是物联网系统。物联网技术尚处于研究和开发阶段, 这个阶段讨论物联网的技术架构必定存在某些主观的推测。这些推测是否正确, 学术界和工业界都可能存在一定的疑虑, 可能产生某些学术观点方面争论。但争论的结果应该能够较为准确地把握物联网技术发展的客观规律, 减少战略

基金项目: 国家重点基础研究发展  
("973")规划(2011CB302903)



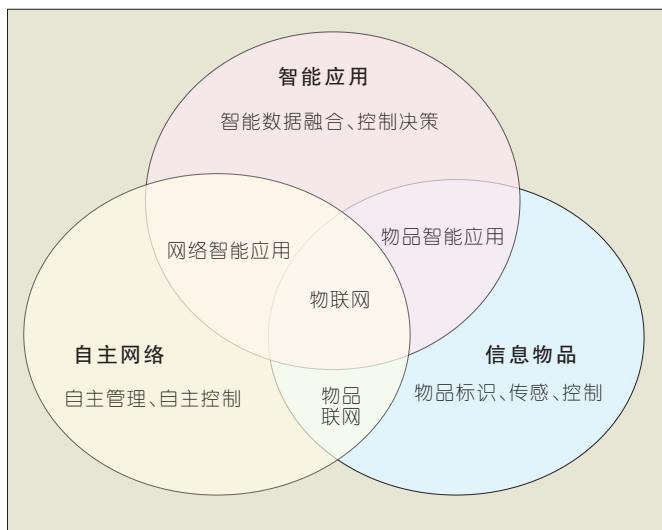


图1  
物联网三维概念模型

连接上网,既无法确定这个物品当前的位置,也无法确定该物品的状态信息属于什么时刻的,则这样连接物品的网络不属于物联网。

由于人类目前还没有研究成功真正的物联网系统,所以,对于物联网的构成也有不同的说法。我们把物联网的组成架构称为物联网的概念模型,不同物联网的概念模型可以产生不同的物联网技术架构。根据我们对物联网概念模型的研究<sup>[1]</sup>,物联网概念模型已经无法采用传统的分层模型进行描述。我们采用了物品、网络、应用三维模型建立了物联网的概念模型,构成由信息物品、自主网络、智能应用为构件的物联网概念模型,如图1所示。这种物联网三维概念模型在每个维度内还是可以采用分层模型描述,例如,自主网络本身可以由分层模型描述。

我们最初也试图采用了分层模型构造物联网的体系结构以及实现模型,但得出结果是一个较为零散的、需要进一步分类的物联网体系结构及其实现模型。这从理论上可以说明,物联网是一个复杂的系统,无法采用二维分层模型构造其逻辑模型。事实上,现在有关物联网研究和开发中存在的一些有争议的问题都是由于物联网复杂性造成的。采用物联网三维概念模型,可以部分解释

这些争议。由于从字面理解,物联网与现有互联网的最大差异在于“物品”,所以,目前与物品相关的网络和应用都可以被纳入到物联网的范畴。有些物品联网技术仅仅是一个局部的联网技术,无法满足大范围、自然连接网络的需求;有些物品应用技术仅仅适用于现有信息技术对物品管理的应用,无法构成一种T2T连接的应用系统。本文讨论的物联网技术是适用于物联网三维概念模型的技术。

## 2 物联网技术架构

按照物联网三维概念模型,物联网由信息物品、自主网络和智能应用3个部分构成。这3个部分有其各自技术架构。这三类技术构成了物联网技术架构,如图2所示。即物联网技术架构由信息物品技术、自主网络技术和智能应用技术构成。

信息物品技术主要指物品的标

识、传感和控制技术,也就是指现有的数字化技术。信息网络技术属于物理世界与网络世界融合的接口技术。目前国际上研究的网络化物理系统(CPS)<sup>[4]</sup>就是属于信息物品技术。如果把人也看作是一个物品,则信息物品技术也包括了佩戴式计算装置技术。

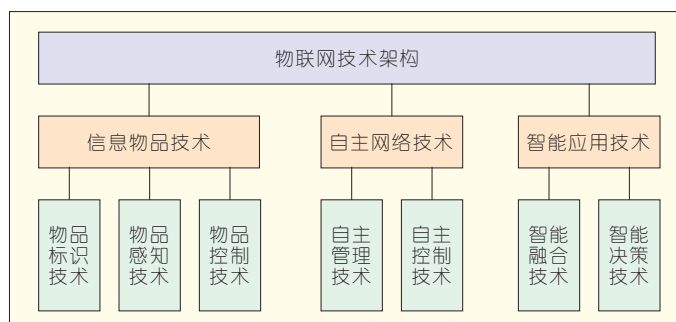
欧洲物联网研究者一般把射频标识(RFID)技术、近距离通信(NFC)、无线传感器和执行器网络(WSAN)作为构成连接现实世界与数字世界的基本技术<sup>[5]</sup>,北美研究网络化物理系统(CPS)的研究者通常把嵌入式系统作为现实世界与网络系统关联的基本技术。这种差异源于研究角度的差异。

本文认为,RFID技术属于物品标识技术,NFC属于物品感知类技术,WSAN属于物品感知和控制类技术。如果需要通过物品感知和控制,都需要运用嵌入式系统技术。

物联网还涉及到自主网络,自主网络就是具备自我管理能力的网络系统,自我管理能力具体表现为自配置、自愈合、自优化、自保护能力<sup>[6]</sup>。从物联网未来应用需求看,需要扩展现有自主网络的定义,使得自主网络具备自控制能力。物联网中的自主网络技术包括自我管理技术和自主控制技术。自主网络管理类技术包括:网络自配置技术、网络自愈合技术、网络自优化技术、网络自保护技术,自主网络控制类技术包括:基于空间语义的控制技术、基于时间语义的控制技术。

支撑物联网的自主网络应该是

图2  
物联网技术架构



具有自主网络能力的因特网。这样,自主网络技术应该是具有自主网络能力的因特网技术。这种技术属于下一代因特网技术。下一代因特网技术将把“任何时间、任何地点传递任何类型信息”的理念扩展到“任何时间、任何地点,连接任何物品,传递任何类型信息”,并且未来的因特网传递的大量信息是来自于物品的信息,这就需要因特网具有自配置、自愈合、自优化和自保护的自主管理能力,以及具有时间语义和空间语义处理的自主控制能力。

承载物品信息传递的因特网已经不再是传统意义上的因特网,它必须保证查询物品状态信息具有时间标记和空间标记,操纵物品的指令必须是具有时间和空间语义的指令。这就要求承载物品信息传递的因特网具有与物理世界关联的时钟体系和坐标体系,这是下一代因特网必须扩展的能力。这类因特网我们称为物理化网络系统(PCS)。物联网不仅需要侧重于物品端的CPS技术,同时还需要侧重于虚拟网络世界端的PCS技术。

本文认为,物联网技术的发展将改变学术界和工业界对下一代网和下一代互联网的认识,一定会打破因特网仅仅是端到端的数据传输管道的观点<sup>[7]</sup>,真正把当前对互联网技术的研究推进到下一代互联网技术研究的轨道上。

物联网把现代社会的人和物都包罗在系统中,所以,物联网的应用涉及到社会的各行各业。物联网的应用可以分成:交通与后勤类应用、医疗类应用、智能环境类应用、个人与社会类应用,以及未来类应用。这里未来类应用是指在目前尚不具备部署条件的应用,包括机器人出租车、智慧城市等;交通与后勤类应用包括物流和仓储管理,轨道交通、公路和航空的辅助驾驶系统,面向公共交通工具、基于个人标识自动缴费的移动购票系统,环境监测系统,以及

电子导航地图;医疗类应用包括医疗对象的跟踪、身份标识和验证、身体症状感知,以及数据采集系统;智能环境类应用包括舒适的家庭/办公环境的智能控制,工厂的智能控制,博物馆和体育馆的智能控制应用;个人与社会类应用包括人与人之间实时交互网络、物品轨迹或人的行踪的历史查询、遗失物品查找,以及防盗等应用。

这些物联网应用中特有的技术是智能应用技术,其中包括智能数据融合和智能决策控制技术。智能数据融合技术包括基于策略的数据融合、基于位置的数据融合、基于时间的数据融合、基于语义的数据融合;智能决策控制技术包括基于智能算法的决策、基于策略的决策、基于知识的决策,这些决策技术需要数据挖掘技术、知识生成、知识更新、知识检索等技术的支撑。

智能应用技术涉及到传统的人工智能方面的理论和算法,并且融入了现代网络环境下的智能控制理论和方法,这类技术的研究和开发,有可能突破桎梏人工智能发展的理论障碍,使得人类进入智能化时代。

### 3 结束语

本文在讨论物联网的定义以及物联网三维概念模型的基础上,提出了一个包括信息物品、自主网络和智能应用三类技术的物联网的技术架构,论述了单纯依赖信息物品类技术无法构成一个真正意义上的物联网,强调了物联网的研究和开发必须重视满足物联网应用需求的自主网络

和智能应用技术的研究和开发,特别是应该重视支持时间语义和空间语义的、具有自主能力的下一代因特网的研究和开发。

本文仅仅是在目前的物联网认识阶段提出了一些关于物联网概念、原理和技术架构的个人观点,不代表所在研究团队的观点,仅供中国物联网研究和开发领域的同行参考。

### 4 参考文献

- [1] ITU Internet report 2005: The Internet of Things [R/OL]. [2005-11-17]. <http://www.itu.int/osg/spu/publications/internetofthings/>.
- [2] 沈苏彬, 范曲立, 宗平, 等. 物联网的体系结构与相关技术研究 [J]. 南京邮电大学学报, 2009, 29(6): 1-11.
- [3] 沈苏彬, 毛燕琴, 宗平, 等. 物联网概念模型与体系结构 [J]. 南京邮电大学学报, 2010, 30(4): 1-8.
- [4] WOLF W. Cyber-Physical Systems [J]. IEEE Computer, 2009, 42(3): 88-89.
- [5] ATZORI L, IERA A, MORABITO G. The Internet of Things: A Survey [J]. Computer Networks, 2010, 54(15): 2787-2805.
- [6] 沈苏彬, 毛燕琴. 自主网络特征与模型 [J]. 中国计算机学会通讯, 2010, 6(4): 53-62.
- [7] SCHWARZ D A, SILVA J. Future Internet Research: The EU Framework [J]. Computer Communication Review, 2007, 37(2): 85-88.

收稿日期: 2010-11-21

#### 作者简介



沈苏彬, 南京邮电大学计算机学院/软件学院信息网络技术研究所研究员、博士生导师, 中国计算机学会高级会员, 中国通信学会高级会员, 中国通信学会通信软件专业委员会副主任委员; 主要研究方向为计算机网络、网络安全、信息网络。

### 《中兴通讯技术》杂志更改英文刊名公告

《中兴通讯技术》杂志英文刊名“ZTE COMMUNICATIONS”从2011年第1期起变更为“ZTE TECHNOLOGY JOURNAL”,其他登记项目不变。

# IoT/CPS 的安全体系结构及关键技术

## Security Architecture and Key Technologies for IoT/CPS

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0011-06

**摘要:** 物联网(IoT)和信息物理融合系统(CPS)作为下一代网络的核心技术,被业界广泛关注。与传统网络不同,IoT/CPS 异构融合、协同自治、开放互连的网络特性带来了巨大的系统安全方面的挑战。挑战包括安全协议的无缝衔接、用户隐私保护等。研发新的安全模型、关键安全技术和方法是 IoT/CPS 发展中的重点。文章基于 IoT/CPS 安全需求和威胁模型,提出了一种层次化的安全体系结构,并针对隐私保护、跨网认证和安全控制等 IoT/CPS 的关键安全技术展开讨论。

**关键词:** 物联网;信息物理融合系统;安全体系结构;隐私保护;安全控制;跨网认证

**Abstract:** Internet of Things (IoT) and Cyber-Physical Systems (CPS) are core technologies of next generation networks, and are the focus of research in both academia and industry. IoT/CPS has unique characteristics including heterogeneous integration, collaborative autonomy, and open interconnection that raise a number of issues for system security. These issues include seamless connection between security protocols, and preservation of user privacy. Developing novel security models, key technologies, and approaches is therefore critical in the development of IoT/CPS. This paper proposes an hierarchical security architecture based on threat analysis and security requirements and discusses key technologies associated with privacy preservation, secure control, and cross-network authentication.

**Keywords:** Internet of things; cyber-physical systems; security architecture; privacy preservation; secure control; cross-network authentication

丁超<sup>1</sup>/DING Chao杨立君<sup>1</sup>/YANG Lijun吴蒙<sup>2</sup>/WU Meng

(1. 南京邮电大学 计算机学院,江苏 南京, 210003;

2. 南京邮电大学 通信与信息工程学院, 江苏 南京, 210003)

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. College of Telecommunications &amp; Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

CPS 在继承 IoT 无处不在通信模式的基础上,更强调物体间的感知互动,强调物理世界与信息系统间的循环反馈。CPS 在感知物理世界之后,能够通过计算、通信和控制对物理世界作出调整,也能够根据感知信息调节系统自身的状态。IoT 和 CPS 是相容的概念。CPS 是 IoT 的理论核心和技术内涵,而 IoT 是 CPS 初级阶段的外在表现形式。随着技术的进步,IoT 和 CPS 必将趋于统一。

与互联网不同,IoT/CPS 大多应用于国民经济的关键领域,要求承载网络具备电信级的服务质量(QoS),对网络的安全可信、可控可管都提出了很高的要求<sup>[1]</sup>。目前业界已针对 IoT/CPS 的安全协议、算法等方面开展了大量的研究,并建立了相应的 IoT/CPS 演示系统。然而这些演示系统受到网络规模、连通性等因素的影响,受到攻击的种类和数量都很有有限,潜在的安全问题尚未充分暴露,一旦大规模投入使用,当前看似安全的网络体系结构将面临巨大的威胁。因此,在 IoT/CPS 建设之初就必

物联网和信息物理融合系统作为下一代网络通信的核心技术,正逐渐成为业界关注的焦点。根据国际电信联盟(ITU)和美国总统科学技术顾问委员会(PCAST)的定义,物联网(IoT)是通过信息传感设备,按照约定的协议,把任何物品与互联网相连接,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的泛在网络<sup>[1]</sup>。信息物理融合系统(CPS)是一个综合了计算、通信和物理

环境的多维复杂系统,通过通信、计算机和消费电子(3C)技术的有机融合和深度协作,实现工程系统中的实时感知、动态控制和信息服务<sup>[2]</sup>。IoT 和 CPS 将地理分布的异构嵌入式设备通过高速稳定的网络连接起来,实现信息交换、资源共享和协同控制,具有广阔的市场前景和巨大的经济效益,是未来网络演进的必然趋势。

作为泛在网络,IoT 与 CPS 具有相同的内涵和外延。IoT 和 CPS 均利用短距离无线通信技术将附着在物品上的感知设备互连,将人与人的交互(H2H)扩展到物与物的互动(T2T)。

**基金项目:** 国家重点基础研究发展(“973”)规划(2011CB302903);江苏省高校自然科学研究重点项目(10KJA510035)



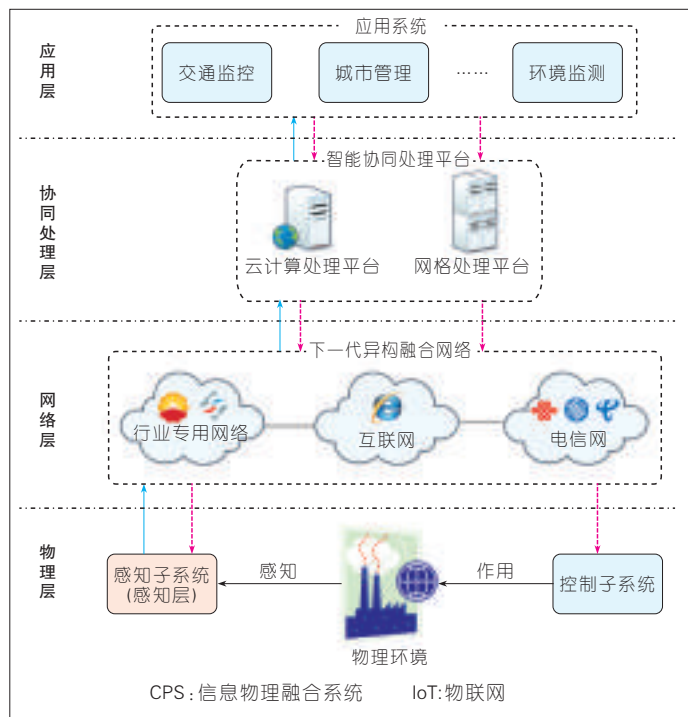


图1  
IoT/CPS 系统模型

须设计严格规范的安全体系结构。本文将在分析和总结现有研究成果的基础上,构建一种IoT/CPS安全体系结构,探索隐私保护、安全控制、跨网认证等安全关键技术,以提高IoT/CPS的安全保障能力。

## 1 IoT/CPS 安全体系结构

### 1.1 网络模型

IoT/CPS是由感知、控制和决策3个模块构成的分布式系统。系统通过网络协调各模块的操作时序,从而实现自我感知、自我判断、自我调节和自我控制。IoT/CPS的系统模型如图1所示。系统模型包括物理层、网络层、协同处理层、应用层。

物理层由感知子系统和控制子系统构成,主要负责从物理世界采集原始信息,并根据系统指令改造物理世界。典型的物理层设备包括RFID装置、各类传感器、图像采集装置、执行器单元以及全球定位系统(GPS)。

网络层保证感知数据在异构网络中的可靠传输,其功能相当于TCP/IP结构中的网络层和传输层。构成

该层的要素包括网络基础设施、通信协议以及通信协议间的协调机制。

协同处理层由多个具有不同功能的智能处理平台组成,并采用网格或云的方式组织这些平台的计算能力。协同处理层根据应用需求将原始感知数据处理成不同的格式,从而实现同一感知数据在多个应用系统间的共享,同时根据感知数据和来自应用层的用户命令智能决策、调整控制子系统内部的预设规则,改变控制子系统的运行状态。

应用层面向用户提供个性化业务、身份认证、隐私保护和人机交互接口,面向协同处理层提供用户操作指令。通过应用层提供的接口,用户可以使用电视、个人电脑、移动设备等多终端设备访问IoT/CPS。

为表述方便,在讨论物理层中的感知子系统相关的问题时本文将使用术语“感知层”。

### 1.2 IoT/CPS 的安全威胁

IoT/CPS的安全威胁主要来自3个方面:

(1)IoT/CPS的感知层由无线传感

器网络(WSN)构成,其节点的计算、通信、存储能力有限,无法直接使用跳频通信、公钥密码等传统安全机制。在IoT/CPS网络环境下,来自外部网络的攻击加剧了感知层的安全问题。

(2)由于IoT/CPS采用下一代网络作为核心承载网络,网络规模的增长和分布式的信息处理环境使得网络更容易受到拒绝服务/分布式拒绝服务(DoS/DDoS)攻击。同时异构网络之间的数据交换将带来全新的安全问题,如网间认证、安全协议的无缝衔接等。

(3)由于IoT/CPS将网络特性引入控制系统,攻击者可以通过阻塞、哄骗、拒绝服务等手段使控制命令延迟或失真,导致系统无法进入稳定状态。发生在IoT/CPS网络各个逻辑层的安全威胁如图2所示。

其中,固有的安全威胁<sup>[4-5]</sup>主要有:

(1)被动攻击

攻击者使用密码学工具分析网络中的信息,或者分析用户的行为模式。典型的被动攻击如窃听、流量分析、节点类型分析等。

(2)节点控制

通过节点控制,入侵者掌握了网内节点的共享密钥或是网关节点与远程信息处理平台共享密钥,入侵者能够通过控制传感器节点获取传感网与该节点交互的所有信息,还能在网络上散布错误信息。

(3)节点捕获

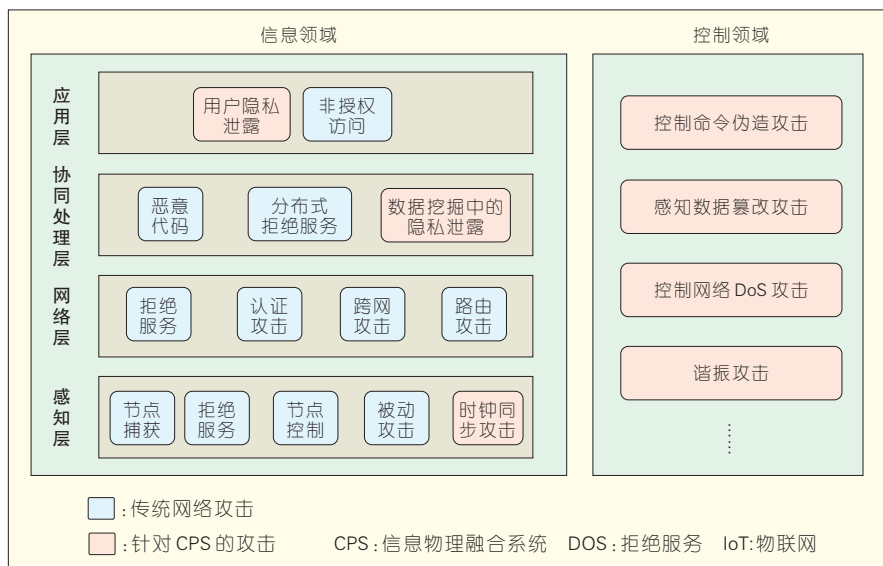
与节点控制不同,节点捕获并不掌握节点的密钥。这种攻击只能通过阻断节点破坏网络的连通性,或是通过鉴别传感器类型和推测网络的运行模式获得网络隐私。

(4)拒绝服务

拒绝服务有两种方式,一种是占用系统资源,导致其他节点停止工作,如网络层的阻塞攻击;另一种是强迫节点持续工作,导致该节点提前失效,如感知层的剥夺睡眠攻击。

(5)认证攻击

认证攻击是通过伪造身份,非法



▲ 图2 IoT/CPS 系统的安全威胁

接入网络,或是恶意提高节点的声誉,达到散布虚假信息、扰乱网络正常运行目的的行为。常见的认证攻击包括针对网络层的中间人攻击、异步攻击、串谋攻击和针对感知层的Hello洪泛攻击等。

#### (6)路由攻击

利用路由攻击,攻击者通过重放、修改、伪造路由信息扰乱正常的路由行为。常见的路由攻击如重放攻击、选择转发攻击、Sybil攻击、Sinkhole攻击和Wormhole攻击。

#### (7)隐私攻击

利用隐私攻击,攻击者通过分析数据隐含的语义,获取用户的身份、偏好、行为习惯等隐私信息。典型的隐私攻击可能发生在感知层的网内数据处理、协同处理层的数据挖掘和应用层的用户认证等过程中。

此外,IoT/CPS的网络特性还引入了新的安全威胁<sup>[6-7]</sup>:

#### (1)时钟同步攻击

对于IoT/CPS这样严格时序的系统,攻击者通过散布虚假时钟消息,破坏系统的统一时钟。

#### (2)谐振攻击

攻击者通过捕获传感器或控制器,强迫物理系统在指定频率附近产生谐振。

#### (3)针对控制系统的攻击

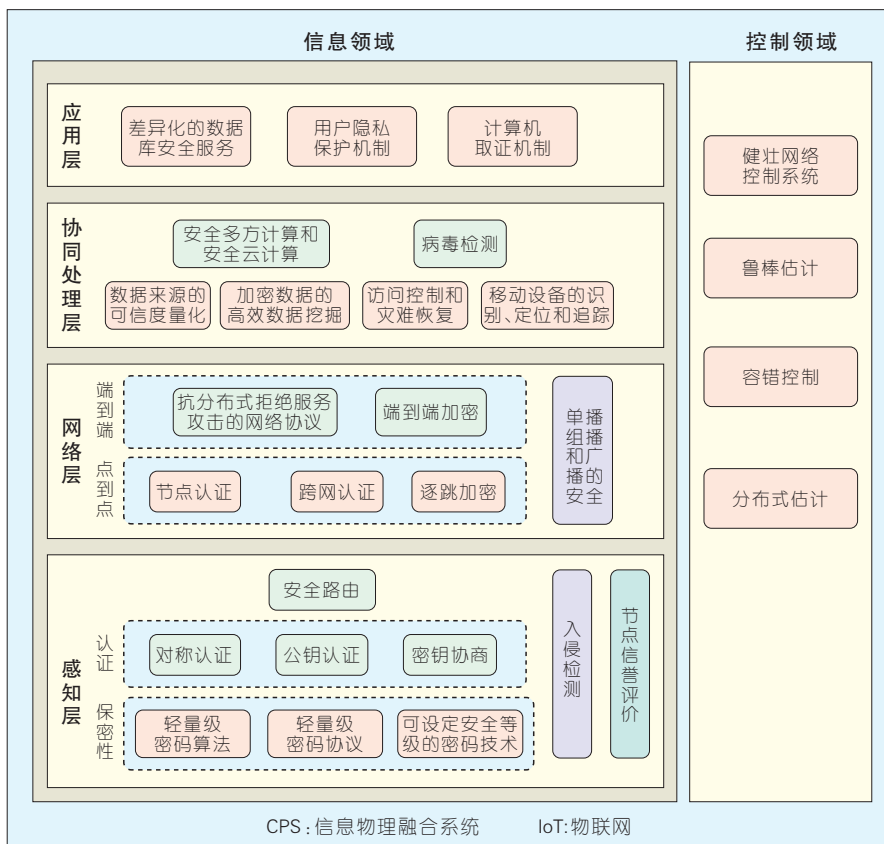
攻击者干扰控制系统对网络状态的估计,伪造或重放控制命令。针对控制系统的攻击包括控制命令伪造攻击、感知数据篡改攻击和控制网

络DoS攻击。

### 1.3 安全结构

目前关于IoT/CPS的安全研究可分为信息安全和控制安全两大类。信息安全主要解决在大规模、高混杂、协同自治的网络环境下信息的安全采集、处理和共享。其研究热点集中于提升现有安全机制的等级、用户隐私保护、海量加密数据的高效处理等方面;控制安全主要解决在开放互联、松散耦合的网络化系统结构下的安全控制问题,其研究的热点集中于克服攻击对控制系统估计和控制算法的影响。

图3所示为本文提出的一种IoT/CPS安全体系结构。在信息领域,我们采用分层的网络结构,从每一个逻辑层次入手,为同一个安全问题设置多重安全机制,从而实现系统的深度防御;在控制领域,由于尚未形成成熟的理论分析模型,目前只能借用传



▲ 图3 IoT/CPS 安全体系结构

统的时延、干扰和故障模型研究控制领域的安全威胁,并使用容错控制、分布式估计、鲁棒估计等方法实现安全控制。

### 1.3.1 感知层的安全结构

IoT/CPS 的感知层是一个由无线传感器网络构成的封闭系统,该层与外部网络的所有通信都必须通过网关节点,因此感知层安全结构的设计只需考虑传感器网络本身的安全问题。感知层的节点硬件结构简单,计算、通信存储能力弱,无法满足传统保密技术的需求。降低密码协议的开销是感知层安全的重要问题。在 IoT/CPS 环境下,感知层更容易受到外部网络的攻击,例如外部访问可能直接针对传感网内部节点展开 DoS 攻击,进而导致整个网络的瘫痪。建立入侵检测和入侵恢复机制,提高系统的鲁棒性,是感知安全的另一重要问题。入侵者可能通过控制网内节点、散布恶意信息扰乱网络正常运行。建立信誉模型,对可疑节点进行行为评估,降低恶意行为的影响是感知层安全的一项重要任务。此外,感知层安全设计还需要考虑建立感知节点与外部网络的互信机制,保障感知信息的安全传输。

感知层的安全机制包括:轻量级的密码算法与协议、可设定安全等级的密码技术、传感器网络的密钥协商、节点的身份认证和数据完整性验证、安全路由、入侵检测和异态检测、节点信誉评价。

### 1.3.2 网络层的安全结构

网络层安全结构的设计必须兼顾高效性、特异性和兼容性。在 IoT/CPS 中,感知数据和控制指令都具有时效性,在设计密码协议时可以考虑适当降低密码的安全等级以获得更高的处理效率。IoT/CPS 由大量异构网络构成,这些网络性能各不相同,对网络攻击的防御能力也存在着巨大的差异。相对于通用安全结构,针

对网络特异性设计专用安全协议更为合适。此外,安全结构的设计还必须考虑到安全协议的一致性与兼容性,实现异构网络的平滑过渡、无缝衔接。

网络层的安全结构可以分为两个子层:点对点安全子层和端到端安全子层。其中,点对点安全子层保证数据在逐跳传输过程中的安全性,对应的安全机制包括:节点间的相互认证、逐跳加密、跨网认证。端到端子层主要实现端到端的机密性并保护网络可用性。安全机制包括:端到端的认证和密钥协商、密钥管理和密码算法选取、拒绝服务和分布式拒绝服务攻击的检测与防御。另外,根据网络通信模式的不同,还应设计针对单播、广播、组播的专用安全机制。

### 1.3.3 协同处理层的安全结构

协同处理层实现海量数据的高效处理以及网络行为的智能决策,其最大的特点是“智能”和“协同”。“智能”的核心是信息的自动处理,只有自动处理技术才能实现海量数据的分类、过滤、识别和处理。然而智能处理技术对恶意信息的检测能力有限,提高恶意信息的识别能力是本层安全结构设计的一个重要挑战;“协同”的核心是异构平台的协作计算,在协作的过程中系统可能泄露数据所有者的隐私,实现信息内容与信息来源的分离,是本层安全结构设计的另一个重要挑战。此外,根据数据的时效性、来源的可靠程度建立数据的可信度量化机制,实现加密数据的高效挖掘等,也都是本层安全机制所必须解决的问题。

协同处理层的安全机制包括:恶意代码和垃圾信息的检测和过滤、安全多方计算和安全云计算、计算平台的访问授权和灾难备份、数据的可信度量化、隐私保护和数据安全挖掘。

### 1.3.4 应用层的安全结构

应用层安全结构的设计必须遵

循差异化服务的原则。基于 IoT/CPS 的应用系统种类繁多,安全需求各不相同,同一安全服务对于不同用户涵义也可能完全不同。例如,用户隐私保护服务对于移动用户而言可能是用户位置信息的保密,对于医疗系统可能是病历信息与病人身份的分离,对于在线选举系统则可能是实现用户匿名。因此根据用户需求提供具有针对性的安全服务,是应用层安全结构设计核心理念。

应用层面面临的安全挑战主要有:

#### (1) 感知数据的分级访问

在 IoT/CPS 系统环境下,多个应用系统共享同一感知数据,而不同应用对感知数据的精度需求不同。以道路监控信息为例,交通调度系统只需要了解某一特定路段车辆的拥堵的大致情况,但交通事故处理系统则需要现场的录像以便确定事故发生的基本过程,而刑侦机关则可能需要更高分辨率的现场图片以便准确获得车牌号等信息。只提供一种精度的信息,将增加隐私泄露的风险。如何针对不同应用提供适宜精度的信息,是应用层安全的重要挑战。

#### (2) 用户认证过程中的隐私保护

在很多应用场景中,系统的认证过程要求用户提交个人信息,如何防止对这些个人信息的非法访问,有效保护用户的隐私,是应用层安全技术所必须解决的安全问题。

应用层的安全机制主要包括:数据库的访问控制、用户隐私保护、计算机取证等。

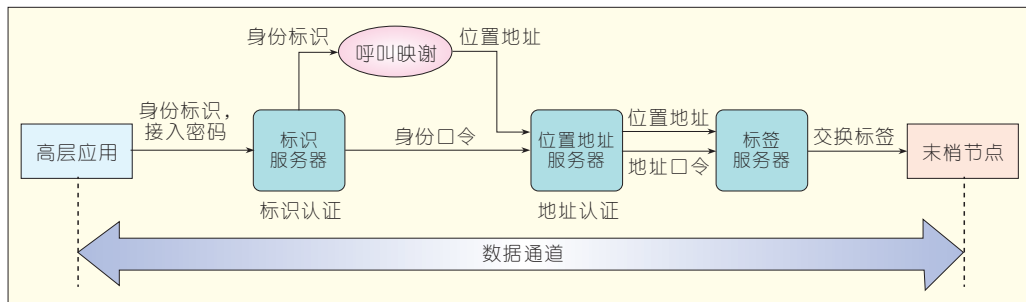
### 1.3.5 控制系统的安全结构

IoT/CPS 控制系统的安全研究处于起步阶段,针对 IoT/CPS 的攻击模式、作为范围和危害程度尚未形成严格规范的描述。目前控制系统的安全技术包括:健壮网络控制、鲁棒估计、分步式估计、容错控制。

## 2 IoT/CPS 安全关键技术

在 IoT/CPS 体系结构中,有些安





▲图4 高层应用与末梢节点会话建立过程

全问题在新的网络环境下并没有发生本质的变化,解决此类问题只需提升现有技术的安全等级;另外一些问题(如控制系统、协同处理平台的安全)对于安全研究而言是全新的,解决这类问题需要全新的安全技术。关于传统的安全技术,如加密、认证、入侵检测和安全路由,文献[4, 8-11]作出了充分的讨论,本文不再赘述。下面针对隐私保护、安全控制、跨网认证等 IoT/CPS 特有的安全技术展开讨论。

### 2.1 大规模实体身份标识和认证技术

IoT/CPS 系统功能的实现依赖于高层应用对末梢网络实体的实时感知和精确控制,这就要求二者之间必须建立互信机制。可以使用双向认证技术来实现这一机制。但是在 IoT/CPS 网络环境下,外部网络与末梢网络节点间的双向认证存在两个问题:认证过程中必须充分地考虑末梢网络资源的有限性,认证机制的计算和通信开销必须尽可能小;对外部网络而言,其连接的末梢网络数量巨大,结构不尽相同,必须建立一个高效的识别机制,以区分这些网络及其内部节点,并赋予唯一的身份标识。

文献[12]提出了一种树形的身份标识和寻址结构,并在此基础上设计了轻量级认证方案。身份标识和寻址结构包括身份标识(ID)、位置地址(LOC)和交换标签(Tag)3类标识体系。节点的身份标识由节点与其他网络实体的社会组织关系决定;位置地址由节点在网络中的位置和网络

的拓扑结构决定;而交换标签,其结构类似于异步传输模式(ATM)的虚路经标识符/虚通道标识(VPI/VCI),为通信双方提供面向连接的服务。高层应用访问末梢节点的过程如图4所示。高层应用以末梢节点的身份标识为目标发起呼叫,标识服务器将身份标识映射为位置地址,同时认证高层应用的合法性,如果认证成功则将位置地址和连接口令发送至位置服务器发起路由查询,最后获得高层应用于末梢节点之间的交换标签,建立数据通道。图4中,高层用户与末梢节点间会话的建立必须通过身份标识和位置地址的双重认证。

为了保证 IoT/CPS 网络的运行效率和可扩展性,认证采用分段加密口令实现。节点在接入 IoT/CPS 时获得自身的 ID/LOC 分量和对应的密钥,通过 RSA 加密算法,节点生成口令密文,再与其祖先节点的口令密文分量级联构成完整的口令密文序列。

### 2.2 安全控制技术

IoT/CPS 将控制系统引入信息网络的同时也带来了新的安全问题,目前关于 IoT/CPS 控制系统安全的研究尚未形成成熟的研究模型和安全策略。现有的研究主要集中在攻击行为模式分析和鲁棒网络控制系统(RNCS)构建两个方面。文献[6]将 DoS 攻击类比为网络拥塞产生的丢包,并用 Bernoulli 和 Gilbert-Elliott 丢包模型分析控制系统遭受 DoS 攻击时的性能;同时使用测量噪声来模拟篡改攻击,并提出使用 MinMax 滤波器补偿

篡改攻击造成的影响。文献[6]将受到攻击的 IoT/CPS 控制系统表示为 Kalman 滤波器的形式。文献[13]在此基础上设计了一种考虑 IoT/CPS 通信限制的分布式 Kalman 滤波器,实现多个控制器对网络状态的协同估计。文献[14]讨论了容错控制(FTC)问题,指出在设计阶段考虑节点冗余,可增强网络的容错性能,将攻击危害降到最低。文献[15]提出了一种控制系统异态检测技术的设想,指出通过建立系统输出对控制命令的反馈模型,异态检测机制可以产生控制命令的估计,并根据控制命令的观察值与估计值的距离判断系统是否受到篡改攻击。

### 2.3 隐私保护技术

隐私保护是 IoT/CPS 安全的一个重要问题。在 IoT/CPS“无处不在”的网络环境下,用户在享受个性化服务的同时也可能泄露自身的隐私信息;另一方面 IoT/CPS 的任务通常由多个节点协作完成,协作过程中节点的输出也可能造成隐私泄露。因此,如何在保持用户隐私机密性的同时不降低数据分析处理的效率是必须解决的安全问题。

以往关于 IoT/CPS 隐私保护的研究集中于无线多媒体传感网(WMSN)视频隐私数据的加密,通过多媒体信息的隐藏、加密和多径传输,保障数据的机密性。文献[16]总结了 WMSN vision-rich 的一些成果,包括 NeST<sup>[17]</sup>、Ubisense<sup>[18]</sup>等支持隐私保护的无线视频监控系統。文献[19]在总结现有 IoT/CPS 隐私保护技术的基础上,给出了两种技术路线:用户匿名和安全多方计算(SMC)。

用户匿名是指利用数据变换,随机化等手段实现用户信息的隐藏。文献[20]提出了一种经典的  $k$ -匿名算法,当数据包包含有  $k$  个以上用户的隐私信息时,该算法保证任意一个用

户的隐私信息都是不可区分的。 $k$ -匿名算法可以有效抵御身份重构攻击,目前被广泛地应用于 Datafly、 $\mu$ -Argus、 $k$ -Similar 等实际隐私保护系统。

安全多方计算是指各实体均以私有数据参与协作计算,当计算结束时,各方只能得到正确的最终结果,而不能得到他人的隐私数据。安全多方计算存在两种算法原型:安全累加协议和隐私同态。安全累加协议是指网络中的个用户在协作完成累加运算的过程中,保持自身数据的机密性;隐私同态是满足同态性质的一类加密算法。

传统安全多方计算方案的运算效率低,同时要求参与计算的资源可计算、可通信,这一点大大限制了安全多方计算在 IoT/CPS 隐私保护领域的应用。文献[21]提出了一种基于“理想格”的同态加密算法,该算法可以使用电路实现,具有良好的可行性和较高的运算效率。

### 3 结束语

安全性是 IoT/CPS 发展过程中不容忽视的问题,系统安全与否将最终决定用户对 IoT/CPS 的认可程度。IoT/CPS 独特的开放性和泛在性为系统安全带来了新的挑战。本文在分析系统的安全需求和威胁模型的基础上,初步建立了 IoT/CPS 的安全体系结构,并在此结构的基础上针对隐私保护、安全控制、跨网认证等 IoT/CPS 特有的安全技术展开了初步的探讨。值得关注的是:IoT/CPS 作为一个整体,各逻辑层安全机制的简单相加并不能实现系统的深度防御,因此构建控制与信息相结合的安全体系,并实现个层次简单安全技术的无缝衔接,是 IoT/CPS 安全研究发展的重要方向。

### 4 参考文献

- [1] ITU Internet Report 2005: The Internet of Things [R/OL]. [2005-11-17]. <http://www.itu.int/osg/spu/publications/internetofthings/>.

- [2] OHN H, MARBURGER J H, KVAMME E F, et al. Leadership Under Challenge: Information Technology R&D in a Competitive World [R/OL]. [2005-11-17]. An Assessment of the Federal Networking and Information Technology R&D Program.2007-08. [http://ostp.gov/pdf/nitrd\\_review.pdf](http://ostp.gov/pdf/nitrd_review.pdf).
- [3] 蒋林海. 单一 IP 技术很难满足物联网的需求 [C]//2000 年中国通信产业发展形势报告会, 北京. 2010.
- [4] KARLOF C, WAGNER D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures [C]//Proceedings of the 1st International Workshop on Sensor Network Protocols and Applications (SNPA'03), May 11, 2003, Berkeley, CA, USA. Los Alamitos, CA, USA: IEEE Computer Society, 2003: 113-127.
- [5] STALLINGS W. Cryptography and Network Security: Principles and Practice [M]. 4th ed. Boston, MA, USA: Prentice Hall, 2006.
- [6] CARDENAS A A, AMIN S, SASTRY S. Secure Control: Towards Survivable Cyber-Physical Systems [C]//Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS'08), Jun 17-20, 2008, Beijing, China. Piscataway, NJ, USA: IEEE, 2008: 495-500.
- [7] ABDELZAHER T. Research Challenges in Distributed Cyber-Physical Systems [C]//Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC'08):Vol 1, Dec 17-20, 2008, Shanghai, China. Piscataway, NJ, USA: IEEE, 2008:5.
- [8] DJENOURI D, KHELLADI L, BADACHE A N. A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks [J]. IEEE Communications Surveys & Tutorials, 2005, 7 (4): 2-28.
- [9] WANG Yong, ATTEBURY G, RAMAMURTHY B. A Survey of Security Issues in Wireless Sensor Networks [J]. IEEE Communications Surveys & Tutorials, 2006, 8(2): 2-23.
- [10] PERRIG A, STANKOVIC J, WAGNER D. Security in Wireless Sensor Networks [J]. Communications of the ACM, 2004, 47(6): 53-57.
- [11] YANG Hao, LUO Haiyun, YE Fan, et al. Security in Mobile Ad Hoc Networks: Challenges and Solutions [J]. IEEE Wireless Communications, 2004, 11(1): 38-47.
- [12] ZHANG Jinxin, LIANG Mangui. A new architecture for converged Internet of things [C]//Proceedings of the 2010 International Conference on Internet Technology and Applications (ITAP'10), Aug 20-22, 2010, Wuhan, China. Piscataway, NJ, USA: IEEE, 2010:4p.
- [13] OLFATI-SABER R. Distributed Kalman Filter with Embedded Consensus Filter [C]//Proceedings of the 44th IEEE Conference on Decision and Control and 2005 European Control Conference (CDC-ECC'05), Dec 11, 2005, Seville, Spain. Los Alamitos: IEEE Computer Society, 2005:8179-8184.
- [14] BLANKE M, KINNAERT M, LUNZE M, et al. Diagnosis and Fault-Tolerant Control [M]. New York, NY, USA: Springer-Verlag, 2003.
- [15] CARDENAS A A, AMIN S, SASTRY S S. Research Challenges for the Security of Control Systems [C]//Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), Jul 29, 2008, San Jose, CA, USA. Berkeley, CA, USA: USENIX Association, 2008:6p.
- [16] LUO Hong, LIU Yonghe, Das S K. Routing Correlated Data in Wireless Sensor Networks: A Survey [J]. IEEE Network, 2007, 21(6): 40-47.
- [17] KUNDUR D, LUH W, OKORAFOR U N, et al. Security and Privacy for Distributed Multimedia Sensor Networks [J]. Proceedings of the IEEE, 2008, 96(1): 112-130.
- [18] AKKAYA K, YOUNIS M. A Survey on Routing Protocols for Wireless Sensor Networks [J]. Ad Hoc Networks, 2005, 3(3): 325-349.
- [19] OLESHCHUK V. Internet of Things and Privacy Preserving Technologies [C]//Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology(Wireless VITAE'09), May 17-20, 2009, Aalborg, Denmark. Piscataway, NJ, USA: IEEE, 2009: 336-340.
- [20] SWEENEY L. K-anonymity: A Model for Protecting Privacy [J]. International Journal of Uncertainty, Fuzziness, and Knowledge-based Systems, 2002, 10(5): 557-570.
- [21] GENTRY C. Fully Homomorphic Encryption Using Ideal Lattices [C]//Proceedings of the 41st Annual ACM Symposium on Theory of Computing(STOC'09), May 31 - Jun 2, 2009, Bethesda, MD, USA. New York, NY, USA: ACM, 2009:169-178.

收稿日期:2010-11-05

### 作者简介



丁超,南京邮电大学计算机学院在读博士研究生;主要研究方向为无线传感器网络中的入侵检测和网络安全。



杨立君,南京邮电大学计算机学院在读博士研究生;主要研究方向为无线网络中的隐私保护。



吴蒙,南京邮电大学通信与信息工程学院教授,博士生导师,南京邮电大学海外教育学院院长;主要研究领域为无线通信、信息安全和 DSP 技术;主持和参与基金项目 8 项;已发表论文 70 篇(其中 EI 检索 20 篇),申请国家级发明专利 5 项。

# 基于物联网的网络信息安全体系

## Network Information Security Architecture Based on Internet of Things

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0017-04

**摘要:** 物联网是计算机、互联网与移动通信网等相关技术的演进和延伸,其核心共性技术、网络与信息安全技术以及关键应用是物联网的主要研究内容。物联网感知节点大都部署在无人监控环境,并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台,传统网络安全措施不足以提供可靠的安全保障。物联网安全研究将主要集中在物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律法规的制订等方面。

**关键词:** 物联网;安全结构;射频识别;隐私保护

**Abstract:** Internet of Things (IoT) is seen as the evolution of related technologies and applications such as Internet and mobile networks. Future research into IoT will focus on generic technology, information security, and critical applications. Sensor nodes in IoT are deployed in an unattended environment, and the IoT platform is extended on the basis of the sensor network and application platforms in the existing infrastructure. So traditional network security measures are insufficient for providing reliable security in IoT. Future research into IoT security will focus on security architecture, privacy protection mode, law-making, and terminal security.

**Key words:** Internet of things; security architecture; radio frequency identification; privacy protection

刘宴兵/LIU Yanbing  
胡文平/HU Wenping  
杜江/DU Jiang

(重庆邮电大学,重庆 400065)  
(Chongqing University of Posts and  
Telecommunications, Chongqing 400065,  
China)

每一次大的经济危机背后都会悄然催生出一些新技术,这些技术往往会成为经济走出危机的巨大推力。

2009年,3G在中国正式步入商业化阶段,各大电信运营商、设备制造商、消费电子厂商都将目光集中在3G市场的争夺。随着3G时代的到来,涌现的一些新技术解决了网络带宽问题,极大地改变了网络的接入方式和业务类型。其中物联网被认为是继计算机、互联网与移动通信网之后的又一次信息产业浪潮,代表了下

**基金项目:** 信息网络安全公安部重点实验室开放课题(C09608);重庆市自然科学基金重点项目(2009BA2024);重庆高校优秀成果转化资助项目(Kjzh10206)

一代信息技术的方向。

物联网除与传统的计算机网络和通信网络技术有关外,还涉及到了许多新的技术,如射频技术、近距离通信和芯片技术等。物联网正以其广泛的应用前景成为人们研究的热点,同时,云计算作为一种新的计算模式,其发展为物联网的实现提供了重要的支撑。

“物联网”最早由MIT Auto-ID中心Ashton教授1999年在研究射频标签(RFID)技术时提出。2003年,美国《技术评论》提出传感网络技术将是未来改变人们生活的十大技术之首,从此物联网逐渐走进了人们的视野。2005年国际电信联盟发布《ITU互联网报告2005:物联网》。报告引

用了“物联网”的概念并指出无所不在的“物联网”通信时代即将来临,世界上所有的物体都可以通过因特网进行信息交互,射频识别技术、传感器技术、纳米技术、智能嵌入技术将得到更加广泛的应用。2009年,美国总统奥巴马与美国工商业领袖举行了一次圆桌会议,对IBM首席执行官彭明盛提出的“智慧地球”这一概念给予了积极评价,并把它上升至美国的国家战略。2009年8月,温家宝总理在无锡考察时提出“感知中国”的发展战略,之后物联网被写入政府工作报告并被正式列为中国五大国家新兴战略性新兴产业之一。

随着物联网在国家基础设施、自然资源、经济活动、医疗等方面的广泛应用,物联网的安全问题必然上升到国家层面。

### 1 物联网相关概念

由于物联网还处于发展初期,业界对物联网定义尚未达成共识。维基百科中物联网被描述为把传感器装备到电网以及家用电器等各种真实物体上,通过互联网连接起来,进而运行特定的程序,达到远程控制或者实现物与物的直接通信的网络。

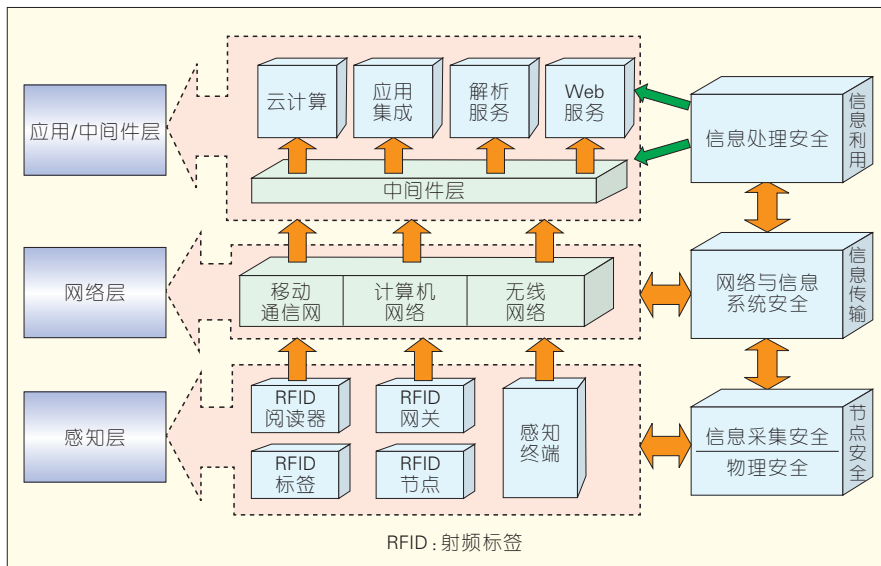


2010年中国政府工作报告把物联网定义为通过信息传感设备,按照约定的协议,把任何物品与互联网连接起来,进行通信和信息交换,以实现智能化识别、定位、跟踪、监控和管理的一种网络<sup>[1]</sup>。而中国工程院邬贺铨院士认为物联网相当于互联网上面面向特定任务来组织的专用网络,即原有通信网络中的一个应用拓展,其突出的特点是包含了一个原有通信网中不存在的底层感知层<sup>[2]</sup>。

按照人们对物联网的理解,物联网是指在物理世界的实体中部署具有一定感知能力、计算能力和执行能力的嵌入式芯片和软件,使之成为“智能物体”,通过网络设施实现信息传输、协同和处理,从而实现物与物、物与人之间的互联。物联网应该具备3个特征:一是全面感知,即利用RFID、传感器等随时随地获取物体的信息;二是可靠传递,通过各种电信网络与互联网的融合,将物体的信息实时准确地传递出去;三是智能处理,利用云计算、模糊识别等各种智能计算技术,对海量数据和信息进行分析和处理,对物体实施智能化的控制,其中智能处理和全面感知是物联网的核心内容。另外,物联网可用的基础网络有很多,根据其应用需要可以用公网也可以用专网,通常互联网被认作是最适合作为物联网的基础网络。

## 2 物联网安全问题

随着物联网建设的加快,物联网的安全问题必然成为制约物联网全面发展的重要因素。在物联网发展的高级阶段,由于物联网场景中的实体均具有一定的感知、计算和执行能力,广泛存在的这些感知设备将会对国家基础、社会和个人信息安全构成新的威胁。一方面,由于物联网具有网络技术种类上的兼容和业务范围上无限扩展的特点,因此当大到国家电网数据小到个人病例情况都接到看似无边界的物联网时,将可能导致



▲图1 物联网的安全层次结构

更多的公众个人信息在任何时候,任何地方被非法获取;另一方面,随着国家重要的基础行业和社会关键服务领域如电力、医疗等都依赖于物联网和感知业务,国家基础领域的动态信息将可能被窃取。所有的问题使得物联网安全上升到国家层面,成为影响国家发展和社会稳定的重要因素。

物联网相较于传统网络,其感知节点大都部署在无人监控的环境,具有能力脆弱、资源受限等特点,并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台,传统网络安全措施不足以提供可靠的安全保障,从而使得物联网的安全问题具有特殊性。所以在解决物联网安全问题时候,必须根据物联网本身的特点设计相关的安全机制。

## 3 物联网的安全层次模型及体系结构

考虑到物联网安全的总体需求就是物理安全、信息采集安全、信息传输安全和信息处理安全的综合,安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性,因此结合物联网分布式连接和管理(DCM)模式,本文给出相应的安全层

次模型(如图1所示),并结合每层安全特点对涉及的关键技术进行系统阐述<sup>[3]</sup>。

### 3.1 感知层安全

物联网感知层的任务是实现智能感知外界信息功能,包括信息采集、捕获和物体识别,该层的典型设备包括RFID装置、各类传感器(如红外、超声、温度、湿度、速度等)、图像捕捉装置(摄像头)、全球定位系统(GPS)、激光扫描仪等,其涉及的关键技术包括传感器、RFID、自组织网络、短距离无线通信、低功耗路由等。

#### (1) 传感技术及其联网安全

作为物联网的基础单元,传感器在物联网信息采集层面能否如愿以偿完成它的使命,成为物联网感知任务成败的关键。传感器技术是物联网技术的支撑、应用的支撑和未来泛在网的支撑。传感器感知了物体的信息,RFID赋予它电子编码。传感网到物联网的演变是信息技术发展的阶段表征<sup>[4]</sup>。传感技术利用传感器和多跳自组织网,协作地感知、采集网络覆盖区域中感知对象的信息,并发布给向上层。由于传感网络本身具有:无线链路比较脆弱、网络拓扑动态变化、节点计算能力、存储能力

▼表1 传感网组网技术面临的安全问题

层次	受到的攻击
物理层	物理破坏、信道阻塞
链路层	制造碰撞攻击、反馈伪造攻击、耗尽攻击链路层阻塞
网络层	路由攻击、虫洞攻击、女巫攻击、陷洞攻击、Hello 洪泛攻击
应用层	去同步、拒绝服务流等

和能源有限、无线通信过程中易受到干扰等特点,使得传统的安全机制无法应用到传感网络中。传感技术的安全问题如表1所示。

目前传感器网络安全技术主要包括基本安全框架、密钥分配、安全路由和入侵检测和加密技术等。安全框架主要有 SPIN(包含 SNEP 和 uTESLA 两个安全协议), Tiny Sec、参数化跳频、Lisp、LEAP 协议等。传感器网络的密钥分配主要倾向于采用随机预分配模型的密钥分配方案。安全路由技术常采用的方法包括加入容侵策略。入侵检测技术常常作为信息安全的第二道防线,其主要包括被动监听检测和主动检测两大类。除了上述安全保护技术外,由于物联网节点资源受限,且是高密度冗余散布,不可能在每个节点上运行一个全功能的入侵检测系统(IDS),所以如何在传感网中合理地分布 IDS,有待于进一步研究<sup>[5]</sup>。

### (2)RFID 相关安全问题

如果说传感技术是用来标识物体的动态属性,那么物联网中采用 RFID 标签则是对物体静态属性的标识,即构成物体感知的前提<sup>[6]</sup>。RFID 是一种非接触式的自动识别技术,它通过射频信号自动识别目标对象并获取相关数据。识别工作无须人工干预。RFID 也是一种简单的无线系统,该系统用于控制、检测和跟踪物体,由一个询问器(或阅读器)和很多应答器(或标签)组成。

通常采用 RFID 技术的网络涉及的主要安全问题有:(1)标签本身的访问缺陷。任何用户(授权以及未授权的)都可以通过合法的阅读器读取 RFID 标签。而且标签的可重写性使

得标签中数据的安全性、有效性和完整性都得不到保证。(2)通信链路的安全。(3)移动 RFID 的安全。主要存在假冒和非授权服务访问问题。目前,实现 RFID 安全性机制所采用的方法主要有物理方法、密码机制以及二者结合的方法。

## 3.2 网络层安全

物联网网络层主要实现信息的转发和传送,它将感知层获取的信息传送到远端,为数据在远端进行智能处理和分析决策提供强有力的支持。考虑到物联网本身具有专业性特征,其基础网络可以是互联网,也可以是具体的某个行业网络。物联网的网络层按功能可以大致分为接入层和核心层,因此物联网的网络层安全主要体现在两个方面。

(1)来自物联网本身的架构、接入方式和各种设备的安全问题

物联网的接入层将采用如移动互联网、有线网、Wi-Fi、WiMAX 等各种无线接入技术。接入层的异构性使得如何为终端提供移动性管理以保证异构网络间节点漫游和服务的无缝移动成为研究的重点,其中安全问题的解决将得益于切换技术和位置管理技术的进一步研究。另外,由于物联网接入方式将主要依靠移动通信网络。移动网络中移动站与固定网络端之间的所有通信都是通过无线接口来传输的。然而无线接口是开放的,任何使用无线设备的个体均可以通过窃听无线信道而获得其中传输的信息,甚至可以修改、插入、删除或重传无线接口中传输的消息,达到假冒移动用户身份以欺骗网络端的目的。因此移动通信网络存在

无线窃听、身份假冒和数据篡改等不安全的因素。

(2)进行数据传输的网络相关安全问题

物联网的网络核心层主要依赖于传统网络技术,其面临的最大问题是现有的网络地址空间短缺。主要的解决方法寄希望于正在推进的 IPv6 技术。IPv6 采纳 IPsec 协议,在 IP 层上对数据包进行了高强度的安全处理,提供数据源地址验证、无连接数据完整性、数据机密性、抗重播和有限业务流加密等安全服务。但任何技术都不是完美的,实际上 IPv4 网络环境中大部分安全风险在 IPv6 网络环境中仍将存在,而且某些安全风险随着 IPv6 新特性的引入将变得更加严重<sup>[7]</sup>:首先,拒绝服务攻击(DDoS)等异常流量攻击仍然猖獗,甚至更为严重,主要包括 TCP-flood、UDP-flood 等现有 DDoS 攻击,以及 IPv6 协议本身机制的缺陷所引起的攻击。其次,针对域名服务器(DNS)的攻击仍将继续存在,而且在 IPv6 网络中提供域名服务的 DNS 更容易成为黑客攻击的目标。第三,IPv6 协议作为网络层的协议,仅对网络层安全有影响,其他(包括物理层、数据链路层、传输层、应用层等)各层的安全风险在 IPv6 网络中仍将保持不变。此外采用 IPv6 替换 IPv4 协议需要一段时间,向 IPv6 过渡只能采用逐步演进的办法,为解决两者间互通所采取的各种措施将带来新的安全风险。

## 3.3 应用层安全

物联网应用是信息技术与行业专业技术的紧密结合的产物。物联网应用层充分体现物联网智能处理的特点,其涉及业务管理、中间件、数据挖掘等技术。考虑到物联网涉及多领域多行业,因此广域范围的海量数据信息处理和业务控制策略将在安全性和可靠性方面面临巨大挑战,特别是业务控制、管理和认证机制、中间件以及隐私保护等安全问题显

得尤为突出。

#### (1) 业务控制和管理

由于物联网设备可能是先部署后连接网络,而物联网节点又无人值守,所以如何对物联网设备远程签约,如何对业务信息进行配置就成了难题。另外,庞大且多样化的物联网必然需要一个强大而统一的安全管理平台,否则单独的平台会被各式各样的物联网应用所淹没,但这样将使如何对物联网机器的日志等安全信息进行管理成为新的问题,并且可能割裂网络与业务平台之间的信任关系,导致新一轮安全问题的产生。传统的认证是区分不同层次的,网络层的认证负责网络层的身份鉴别,业务层的认证负责业务层的身份鉴别,两者独立存在。但是大多数情况下,物联网机器都是拥有专门的用途,因此其业务应用与网络通信紧紧地绑在一起,很难独立存在。

#### (2) 中间件

如果把物联网系统和人体做比较,感知层好比人体的四肢,传输层好比人的身体和内脏,那么应用层就好比人的大脑,软件和中间件是物联网系统的灵魂和中枢神经。目前,使用最多的几种中间件系统是:CORBA、DCOM、J2EE/EJB以及被视为下一代分布式系统核心技术的Web Services。

在物联网中,中间件处于物联网的集成服务器端和感知层、传输层的嵌入式设备中。服务器端中间件称为物联网业务基础中间件,一般都是基于传统的中间件(应用服务器、ESB/MQ等),加入设备连接和图形化组态展示模块构建;嵌入式中间件是一些支持不同通信协议的模块和运行环境。中间件的特点是其固化了很多通用功能,但在具体应用中多半需要二次开发来实现个性化的行业业务需求,因此所有物联网中间件都要提供快速开发(RAD)工具。

#### (3) 隐私保护

在物联网发展过程中,大量的数

据涉及到个体隐私问题(如个人出行路线、消费习惯、个体位置信息、健康状况、企业产品信息等),因此隐私保护是必须考虑的一个问题。如何设计不同场景、不同等级的隐私保护技术将是物联网安全技术研究的热点问题<sup>[8]</sup>。当前隐私保护方法主要有两个发展方向:一是对等计算(P2P),通过直接交换共享计算机资源和服务;二是语义Web,通过规范定义和组织信息内容,使之具有语义信息,能被计算机理解,从而实现与人的相互沟通<sup>[9]</sup>。

### 4 物联网安全的非技术因素

目前物联网发展在中国表现为行业性太强,公众性和公用性不足,重数据收集、轻数据挖掘与智能处理,产业链长但每一环节规模效益不够,商业模式不清晰。物联网是一种全新的应用,要想得以快速发展一定要建立一个社会各方共同参与和协作的组织模式,集中优势资源,这样物联网应用才会朝着规模化、智能化和协同化方向发展。物联网的普及,需要各方的协调配合及各种力量的整合,这就需要国家的政策以及相关立法走在前面,以便引导物联网朝着健康稳定快速的方向发展。人们的安全意识教育也将是影响物联网安全的一个重要因素。

### 5 结束语

物联网安全研究是一个新兴的领域,任何安全技术都伴随着具体的需求应运而生,因此物联网的安全研究将始终贯穿于人们的生活之中。从技术角度来说,未来的物联网安全研究将主要集中在开放的物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律法规的制订等几个方面。

### 6 参考文献

- [1] 2010年政府工作报告 [EB/OL]. [2010-03-15]. [http://www.china.com.cn/policy/txt/2010-03/15/content\\_19612372\\_8.htm](http://www.china.com.cn/policy/txt/2010-03/15/content_19612372_8.htm).

- [2] 郭贺铨. 物联网是互联网运用的拓展 更具专业性 [EB/OL]. [2010-03-15]. <http://news.163.com/10/1028/15/6K3H05RP00014JB5.html>.
- [3] 刘宴兵, 胡文平. 物联网安全模型及其关键技术 [J]. 数字通信, 2010, 37(4): 28-29.
- [4] 传感器: 物联网成引擎 新技术催生新机遇 [N]. 中国电子报, 2010-07-13.
- [5] 李晓维. 无线传感器网络技术 [M]. 北京: 北京理工大学出版社, 2007: 241-246.
- [6] 张福生. 物联网: 开启全新生活的智能时代 [M]. 太原: 山西人民出版社, 2010: 175-184.
- [7] 王帅, 沈军, 金华敏. 电信IPv6网络安全保障体系研究 [J]. 电信科学, 2010, 26(7): 10-13.
- [8] MEDAGLIA C M, SERBANATI A. An Overview of Privacy and Security Issues in the Internet of Things [C]//The Internet of Things: Proceedings of the 20th Tyrrhenian Workshop on Digital Communications, Sep 2-4, 2009, Sardinia, Italy. Berlin, Germany: Springer-Verlag, 2010: 389-394.
- [9] SAVRY O, VACHERAND F. Security and Privacy Protection of Contactless Devices [C]//The Internet of Things: Proceedings of the 20th Tyrrhenian Workshop on Digital Communications, Sep 2-4, 2009, Sardinia, Italy. Berlin, Germany: Springer-Verlag, 2010: 409-418.

收稿日期: 2010-11-10

#### 作者简介



**刘宴兵**, 重庆邮电大学教授、博士; 主要研究领域为网络接入控制和网络安全; 先后主持基金项目 10 项, 获得国家科技进步奖 1 项、省部级奖励 2 项; 已发表学术论文 50 篇(其中 SCI 收录 9 篇, EI 收录 22 篇), 出版专著 2 部, 申请发明专利 5 项。



**胡文平**, 重庆邮电大学通信工程专业在读硕士研究生; 主要研究领域为物联网以及移动互联网安全技术。



**杜江**, 韩国仁荷大学计算机学院硕士毕业; 重庆邮电大学副教授; 研究方向为信息安全; 已在核心期刊发表论文 20 篇。



# 移动网络安全防护技术

## Security Service Technology for Mobile Networks

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0021-06

**摘要:** 移动网络向着高速率、全 IP 方向发展, 承载的业务种类也越来越多, 这就对移动网络的安全提出了新的要求。传统的安全方案并不能适应新的安全需要。文章分析了 3G/4G 移动网络的安全威胁和需求, 从移动网络的整体架构出发, 提出了基于安全服务的安全防护方案。该方案在移动终端上构建可信计算环境, 将软件合法性验证与访问控制相结合, 在服务管理中心对移动终端提供完整性检查和软件合法性验证等安全服务, 从而在很大程度上保护了移动终端以及移动网络的安全。进一步, 文章给出了未来需研究的问题及发展方向。

**关键词:** 移动网络安全; 安全服务; 可信计算; 访问控制

**Abstract:** As mobile networks become high speed and attain an all IP structure, more and more services are possible. This brings about many new security requirements that traditional security programs cannot adapt to. This paper analyzes security threats and the needs of 3G/4G mobile networks. It proposes a novel protection scheme for mobile networks encompassing the whole structure of the mobile network. Trusted computing is built into mobile terminals—a scheme in which software validity verification is combined with access control, and validity and integrity are checked in the security management center in order to secure the mobile terminal. In this way, terminals and the network as a whole is secured to a much greater extent. This paper also highlights problems to be addressed in future research and development.

**Keywords:** mobile network security; security service; trusted computing; access control

胡爱群/HU Aiqun

李涛/LI Tao

薛明富/XUE Mingfu

(东南大学 信息安全研究中心, 江苏 南京, 210096)  
(Information Security Center of Southeast University, Nanjing 210096, China)

随着移动网络的迅速发展, 无线通信技术和计算机技术不断融合, 移动设备朝着智能化的方向发展, 其所支持的功能越来越多, 使得人们可以享受各类丰富多彩的服务。然而, 网络的开放性以及无线传输的特性, 使得终端设备暴露在开放式的全 IP 化的网络中, 各种敏感信息的防护面临着来自各种恶意攻击的挑战, 安全问题已成为整个移动网络的核心问题之一。

本文在研究 3G 和 4G 移动通信系统的安全目标、安全原则及相应的威胁基础上, 对现有各种安全防护方案进行讨论和分析, 提出一种基于终端可信的、面向安全服务的统一安全防护体系, 并给出其在移动网络中的具体应用。

### 1 移动通信系统的安全架构和面临的安全威胁

#### 1.1 3GPP 的安全机制

WCDMA、CDMA2000、TD-SCDMA 是第三代移动通信的三大主流技

术。3GPP 制订的 3G 安全功能分为 5 个安全特征组<sup>[1]</sup>, 分别属于 3 个不同的层面, 如图 1 所示。它们分别是:

#### (1) 网络接入安全

该安全特征集提供用户安全接入 3G 业务, 特别能抗击在无线接入链路上的攻击。

#### (2) 网络域安全

该安全特征集使在服务提供者域中的节点能够安全地交换信令数据, 抗击在有线网络的攻击。

#### (3) 用户域安全

该安全特征集确保移动平台接入安全。

#### (4) 应用域安全

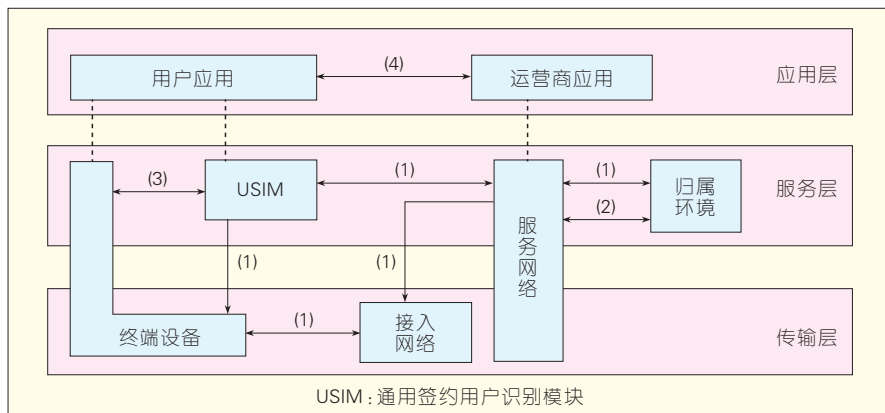
该安全特征集使在用户域和在提供者域中的应用能够安全地交换信息。

#### (5) 安全的可视性和可配置性

该安全特征集使用户能知道一个安全特征集是否在运行, 而且业务的应用和设置是否应依赖于该安全特征。

3GPP 提出的 3G 安全结构中重点描述了网络接入安全机制, 包括双向鉴权、通用移动通信系统陆地无线接入网 (UTRAN) 加密和信令数据的完整性保护在内的安全机制。网络接入

基金项目: 国家高技术研究发展 (“863”) 计划 (2009AA01Z427)



▲图1 3G系统安全结构图

机制包括3种：使用临时身份识别(TMSI)、使用永久身份识别(IMS I)、认证和密钥协商(AKA)，其中认证与密钥协商机制(AKA)是3G网络安全机制的核心，也是3G网络安全机制的研究热点。AKA机制用于完成移动台和网络的相互认证，并建立新的加密密钥和完整性密钥。3G网络的安全机制还包括数据加密和数据完整性。数据加密机制采用F8算法对用户终端(ME)与无线网络控制器(RNC)之间的信息加密。数据完整性机制采用F9算法对信令消息的完整性、时效性进行认证。

总的来说，3G系统使用了双向身份认证，增加了密钥长度，使用了高强度的加密算法和完整性算法，增加了信令完整性保护机制，并提出了保护核心网络通信节点的机制<sup>[9]</sup>。但是面对新的业务、全开放式的IP网络和不断升级的攻击技术，移动网络仍面临较大的安全威胁。

## 1.2 4G网络的安全机制

根据3G网络所暴露出的安全问题和4G网络所面临的主要威胁，可以将4G网络的安全要求简要概括为4个方面<sup>[9]</sup>。

### (1)网络接入安全

保护用户安全接入到4G网络，防止无线链路的攻击。

### (2)网络域安全

保护运营网络安全交互数据，防

止来自有线网络和网络实体的攻击。

### (3)用户域安全

为访问移动实体/通用签约用户识别模块(USIM)提供安全保护，以及构建移动实体/USIM的安全环境。

### (4)应用安全

为用户和运营应用提供安全保障，保障它们之间安全交换消息。

根据以上安全需求，4G网络的安全结构分为4个功能特征组，即网络接入安全、网络域安全、用户域安全和应用安全。各功能特征组的基本内容类似于3G网的功能特征组。4G网络安全体系结构如图2所示。

与3G网络最大的不同是，4G对ME/USIM侧的安全要求增加了“保证移动平台的软件、硬件和操作系统的完整性”，为移动实体构建可信计算环境。只有移动终端的平台安全了，才有可能保证用户信息的安全。但研究表明，要想保证移动终端平台的

安全，只靠移动终端本身是做不到的，还必须依赖移动网络中的安全服务器的安全管理和服务。

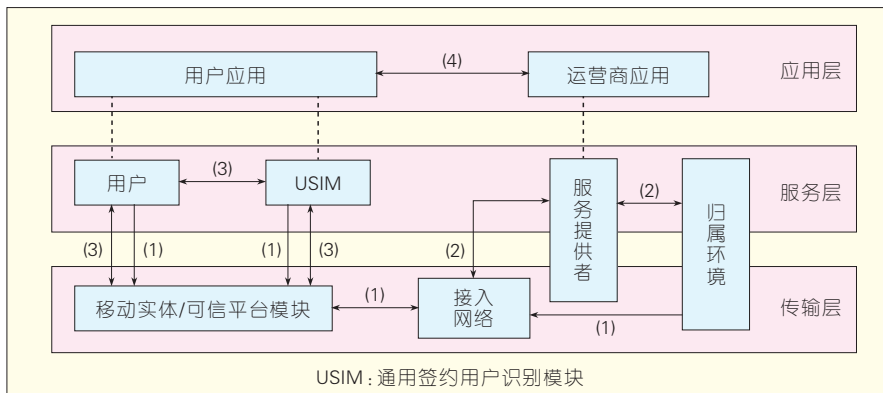
## 1.3 移动通信网络面临的安全威胁

3G移动通信网络正向全IP网络方向发展，移动通信网络已经和互联网一样，面临着威胁越来越多的威胁。病毒、木马、垃圾邮件和短信、窃听等安全事件，不断威胁着整个3G网络以及未来的4G网络的安全。

由于3G与传统移动通信的显著区别在于它是以网络应用服务为核心的，移动终端是用户的体验平台，也是互联网的一个终端。一方面，其自身的安全隐患会对整个3G网络带来极大的影响。3G手机对互联网的高速访问导致其经空中接口传输的敏感数据量大大增加。而且，手机病毒及有害信息也会通过手机终端向其他终端或节点传播。另一方面，互联网的开放性对移动终端的安全构成了重大威胁。移动用户对互联网资源的任意访问，导致手机中毒或被攻击的可能性大大增加。网络开放性带来的安全性问题必然会在3G网络中凸显。此外，3G系统采用的大量协议，也依然存在着一定的安全隐患<sup>[9]</sup>。

## 2 移动通信网络安全防护研究

面对3G移动通信网络以及未来的4G移动通信网络所面临的各种威



▲图2 4G网络安全结构图

胁,国内外的学者进行了大量的移动通信网络安全防护方面的研究。这些研究大致可以分为两个方面,一是对安全体系和机制的改进,重点保护空中接口的安全,防止空中窃听。这较多的集中于对3G安全机制中的核心协议——AKA的安全性分析和改进方案。另一个方面是,把安全防护的目标和手段锁定在终端,认为终端是安全问题发生的源头。通过在终端上引入安全的技术和手段,保护终端免受病毒侵害,以保护用户信息安全,进而保护整个网络的安全。而这又可分为两个主要研究热点,一是对终端进行病毒防杀,二是基于可信计算的安全终端理念。

### 2.1 基于体系安全的防护技术

文献[5]中,英国安格利亚鲁斯金大学提出了一种应用于3G网络的新型的对称/非对称认证协议的混合方法。文献[5]针对当前3G移动系统认证方案中存在的不足,如移动终端身份泄露和更新临时身份的高开销,提出了安全的认证机制。该方案将认证实体与网络之间初始认证时的信息交互从5次降为4次。随后的认证过程仅仅包含两次信息交互。该方案还可以用来对抗网络攻击,如重放攻击和猜测攻击等,并且满足3G通信系统的安全要求。

文献[6]中,美国伊利诺伊大学香槟分校提出了一种轻量级的、基于组件的、可重构的安全机制。该安全机制将Tiny SESAME结构应用于移动网络,增强了认证和基于IP应用的多媒体安全服务,从而增强了移动设备的安全功能。

文献[7]中,美国佛罗里达大学针对3GPP中AKA协议易受到伪基站攻击的问题,提出了增强型的AKA协议。伪基站攻击这一漏洞将会使得攻击者可以将用户的信令从一个网络重定向到另一个,还使得攻击者可以使用认证向量来假冒其他网络。他们提出的AP-AKA协议,有效地对

抗了以上攻击。

文献[8]提出了一种基于虚拟专用网IP安全协议(IPSec VPN)的3G网络安全多媒体业务的解决方案。这种基于IPSec的端到端VPN方案,提供了端到端的实时的安全的多媒体信息传输,并保证了服务的质量。

文献[9]分析了现有3G移动通信网络中AKA协议安全性的不足,如已经出现的认证向量攻击。文献[9]针对即将应用的4G通信系统,将已经被证实安全有效的安全套接层/传输层安全(SSL/TLS)协议引入到AKA机制中,提出了基于SSL/TLS协议的改进型AKA协议。

文献[10]研究了4G系统所受的安全威胁,用X.805标准对4G系统中的Y-Comm体系进行了分析。作为4G网络安全架构研发的组织之一,Y-Comm提出了集成安全模块和一个针对性的安全模型,较好的保护了数据、服务器和用户的安全。

文献[11]分析了3GPP系统架构演进(SAE)8号标准采用的AKA协议,指出了它已解决和未解决的安全问题,强调了其中存在的几个安全缺陷,如用户身份曝光、截取认证向量、共享K密钥泄露的潜在风险等,提出了一种新的3GPP SAE的认证和密钥协商协议。新协议中,采用公钥密码体制对网络域中的用户身份信息和认证向量进行了加密,用随机数产生本地认证的公共密钥。

文献[12]中,北京邮电大学对3GPP中AKA协议进行了安全性研究,分析了其容易遭受的4种攻击,提出在位置更新与位置不变两种情况下的基于公钥密码学的认证与密钥协商协议,采用形式化的分析方式证明了所提出算法的安全性,并将该协议与已有协议在安全性方面进行了比较,性能有一定的提升。

文献[13]中,同济大学提出了在移动网络环境下建立IPSec VPN连接的终端系统的实现方案,该系统利用NDIS中间驱动程序实现防火墙穿

越,以保证IPSec数据包的正常传输。同时利用安全智能卡存储X.509证书,用于身份验证,防止非法用户的入侵。

### 2.2 基于终端安全的防护技术

终端是创建和存放数据的源头,大多数的攻击事件都是由终端发起。如果移动系统中的每一个终端都是经过认证和授权的,并且其操作符合安全策略的规定,那么就可以保证整个网络系统的安全<sup>[4]</sup>。因此终端安全的思想正在逐渐被人们所重视,对其研究也备受关注。而这又分为两个主流的安全防护技术:一是从终端的防病毒和病毒查杀角度的安全防护,另一个是基于终端可信的安全防护。

文献[3]提出了一种用于4G移动终端的可信计算安全结构。该结构基于可信移动平台(TMP)和公钥基础设施(PKI),为用户在4G系统中接入敏感服务和敏感数据提供了一个鲁棒性的平台,并提出了混合型AKA认证方案。

文献[15]提出在终端安装反病毒软件,在网络侧添加旁路式检测和过滤器进行病毒查杀,以应对智能终端的病毒威胁。

文献[16]提出了从网络接入控制到应用服务控制的多层安全控制手段,在终端构造安全应用程序,在网络侧构造安全的网络访问控制和应用服务访问控制的策略,结合安全服务器,保障移动通信网络的安全。

文献[14]和文献[17],都倡导基于可信计算的终端安全体系结构,实现可信终端与可信网络的一致性,以实现系统的安全防护。文献[14]总结了可信计算的各种体系结构以及在终端安全防护上的进展,指出了下一步努力方向。该文献没有涉及系统效率等实际因素,也没有涉及如何构建全网统一安全防护问题。

综上所述,上述两种技术方向是移动网络信息安全不可或缺的两个



方面。前者着力保护空中接口的安全,后者旨在保护终端免受病毒入侵。在这两个方面中,前者发展相对完善;后者是这两年随着移动网络病毒的出现才受到重视。因此,本文重点讨论后者。

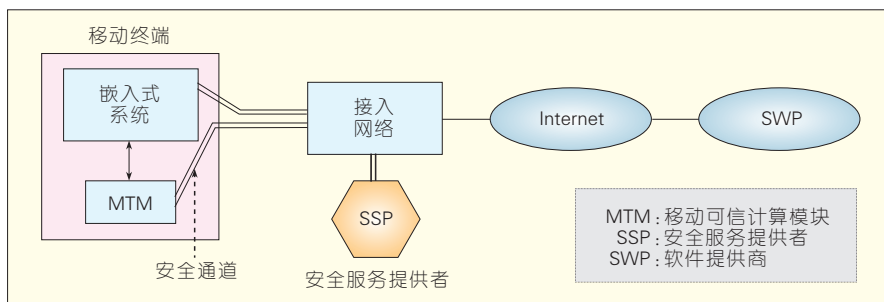
### 3 基于服务的移动网络安全体系

如前所述,在如何保护移动终端免受病毒入侵方面,主要有两种解决思路。其一是对终端进行扫描杀毒,另一种是为终端建立可信计算环境。无论是哪一种思路,都离不开安全服务体系。前者需要在移动网络中建立病毒库更新与杀毒服务中心,定期或在线为移动终端提供杀毒服务;后者需要为终端可信环境的建立和维护提供信任检查。不同于计算机用户,由于手机用户的非技术性,如果没有安全服务,很难保证移动网络的安全。

在保证手机终端与接入网络之间的身份认证、数据完整性和机密性的前提下,手机终端的安全威胁主要来自 Internet 网络,这和互联网上的计算机用户受到的安全威胁一样。人们希望可信终端能够防御来自网络的攻击。如果终端是可信的,终端的表现就要符合预期要求,那么终端上就不能存在未授权软件。也就是说,凡是在终端上安装和可以执行的软件一定要得到安全服务器的授权许可。只有这样,网上的病毒才不可能被植入到移动终端中。

#### 3.1 基于可信服务的安全体系结构

本文对现有的移动网络架构进行了改进。首先,移动终端中必须添加移动可信计算模块(MTM)<sup>[18]</sup>。该模块是独立的、安全的模块,具有计算能力,能够与安全服务提供者(SSP)进行安全通信。它可以计算出移动终端中的所有软件的完整性,并报告给 SSP;同时,它还能够对移动终端中需要安装和执行的软件检查其合法性,



▲ 图3 基于可信服务的移动网络安全体系

看其是否得到 SSP 的授权。如果没有授权,将禁止安装和执行。其次,移动网络中还需要添加 SSP 这个角色。它的主要工作是为移动终端提供软件合法性证明。在互联网中,软件提供商(SWP)向移动用户提供的软件必须持有 SSP 的合法证明,也就是必须有 SSP 签发的数字证书,才能在移动用户的手机中被安装和运行使用。图3给出了基于可信服务的移动网络安全体系结构图。

在图3中,SSP 服务器与 AN 服务器直接连接,这样对原有系统结构改动很小。通过接入认证后的移动终端被允许接入网络后,SSP 对该移动终端进行完整性检查。如果终端软件完整性受到破坏,则表明终端可能已经染毒,此时就可以不允许其进一步接入网络,以免将病毒扩散到其他网络终端;如果终端软件完整性未受破坏,则可通过 SSP 对使用中的移动终端的安装软件和运行软件过程进行安全监督,从而为移动终端提供动态安全服务。

#### 3.2 移动终端可信计算环境

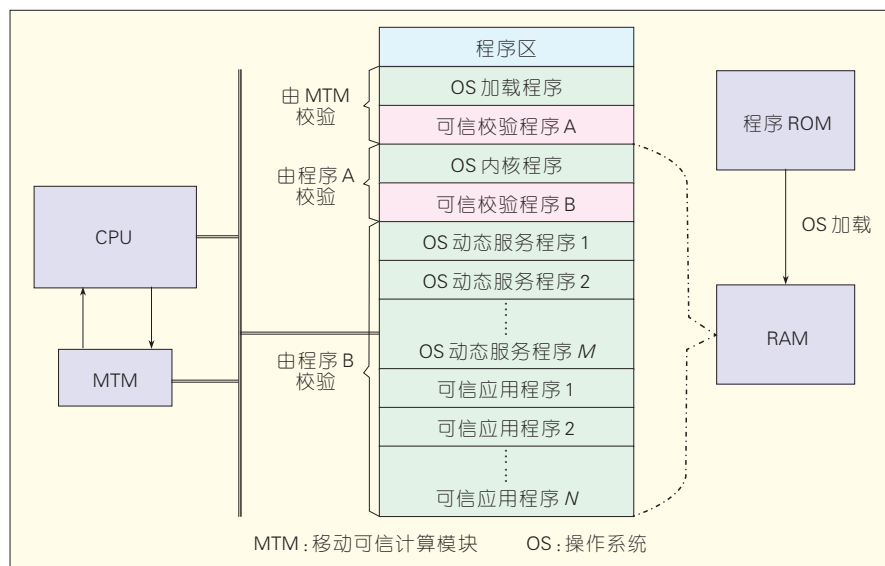
基于安全服务的防护体系能否有效运行的关键在于移动终端的可信计算环境的设计。本文将移动终端的状态分为启动时和启动后两个状态分别进行讨论。启动时建立的可信环境称为静态可信环境,启动后的可信计算环境称为动态可信环境。

关于静态可信的建立方法在很多文献中已有描述,这里再简要介绍一下。移动终端上电后,从可信模块

中固化的可信代码启动,硬件的特性保证了这段代码不可能被更改。可信代码首先校验系统装载代码是否完整,若完整就将控制权交给系统装载代码;接着,系统装载代码校验操作系统内核是否完整,若完整就装载操作系统内核;然后,操作系统内核接着对操作系统中的其他部分进行校验;操作系统校验完毕后就被启用;最后再对上层的各个应用程序进行完整性校验,直到所有程序被校验完毕,用户才能使用终端。如果某一个环节没有通过校验,那么就需要恢复之前的配置或重装系统。信任链通过这样的完整性校验从可信代码传递到操作系统,最后再传递给应用软件,就构成了整个系统的静态可信环境。图4为系统启动时的资源结构。可信校验程序附着在程序末尾,负责校验下一段程序的完整性。

从图4可见,为保证系统安全,在静态可信链建立以后,OS 内核程序和可信校验程序 B 不能被破坏,这两部分程序需要靠 MTM 来保护。因为,在系统启动之后,内核程序需要被运行,而可信检验程序 B 需要被用来动态检验新启动的应用程序,或者为 SSP 生成终端的完整性信息。

在系统运行之后,对系统的保护可依赖动态可信机制实现。由于在系统运行之后,随着用户开启的应用的不同,系统的完整性是动态变化的。比如,用户打开浏览器后,浏览器软件被运行,这时,系统中增加了与运行浏览器相关的程序,显然系统完整性发生了变化。如果不能及时



▲ 图4 可信系统启动时的系统资源结构

正确地更新系统的完整性信息,则可能被恶意软件钻了空子。但要计算动态完整性,必然要耗费系统的计算资源。因此,如何对运行中的系统进行安全保护,是可信计算的难点问题。可信计算要实现以下几个目标:

- (1)能够定期对指定程序或区域资源计算其完整性,并汇报给SSP。
- (2)能够检查即将安装的程序的合法性,如不合法则不能被安装。
- (3)能够检查即将运行的程序的合法性,如不合法则不能被运行。
- (4)上述安全机制本身必须是安全的。
- (5)上述安全机制应不明显影响系统运行效率。

在上述目标中,目标1是要检查运行中的系统软件或软件资源是否被修改,一旦被修改即能被发现。计算一段代码的完整性通常采用计算其摘要值并与已有摘要值(由SSP提供)相比的方法,也可以采用随机抽取代码位再取其摘要的方法。当代码较长时,后一种方法具有优势。

当移动终端需要安装或运行一个程序时候,不仅需要检查其完整性,还需要验证其合法性。目标2和目标3中程序合法性是通过检查程序是否有SSP授权来验证。该验证

过程同样由SSP提供。SSP通过与软件提供商SWP签订合同,并将合法软件的版本及其摘要信息保存在SSP服务器中供移动终端查询。该过程可以用图5所示的流程来描述。

对于目标4,关键是要保护好图4中的可信校验程序B不受破坏,这通常需要专门的硬件。一种有效的保护方法是通过硬件电路实现对可信校验程序B所在的地址空间不能被写入,除非得到MTM的授权许可。这种硬件保护电路可以一并设计在MTM中。

### 3.3 安全服务器

根据以上阐述,不难理解,安全服务器的两个主要安全服务功能为:

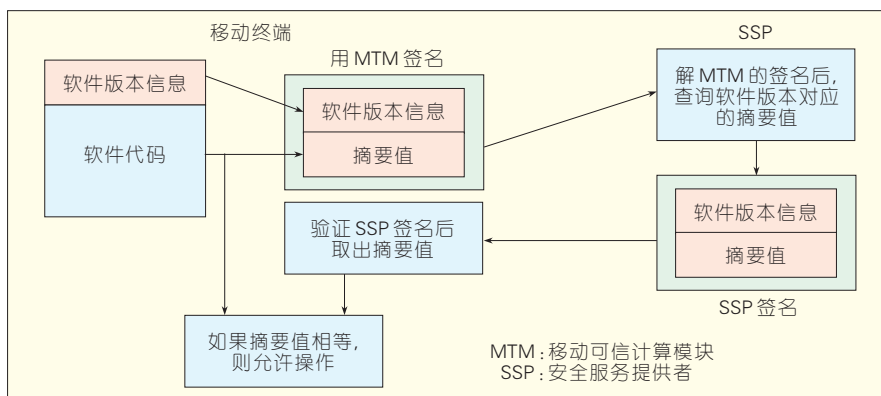
(1)检查移动终端的软件完整性,如不完整,则不允许其接入网络。如移动终端软件完整性受到破坏,表明终端可能已经遭受病毒入侵。如允许其接入网络,则可能会传染其他终端和网络设备。

(2)为移动终端提供软件合法性查询服务。当移动终端需要安装或者运行软件时,首先需要查询该软件是否合法。终端先在本地的MTM中查询,如无结果,则将查询申请递交给安全服务器,安全服务器验证终端的身份后将查询结果返回给该终端。

安全服务器的辅助功能还包括:与软件提供商的安全交互,以实现软件安全性审核及合法性信息生成功能;与移动网络运营商的AAA服务器安全交互,以实现身份认证及计费功能;与运营网络的接入网服务器交互功能,以实现基于移动终端完整性的接入控制功能等等。

## 4 未来的研究方向

随着网络构架和传输协议的日益成熟,未来移动通信安全的研究重点将转移到移动终端上。而由于目前移动终端上的嵌入式平台和嵌入式操作系统的设计初衷都不是专门为移动通信环境服务,因此这方面的安全问题尤为突出。嵌入式系统中程序空间和数据空间一体化的结构,为实现对关键程序的保护增加了难度。因此,有利于保护关键程序安全的嵌入式系统架构是需要进一步研



▲ 图5 移动终端对软件完整性和合法性的验证过程

究的问题之一。

类似于 TrustZone<sup>[19]</sup> 的域隔离技术,对内存空间的关键位置读写保护是一个很好的思路。操作系统和应用软件装载到内存后,可以通过对 CPU 访问的内存地址进行监控,控制对关键位置的读写操作。如果能从硬件上来控制读写操作,那么几乎不会影响到系统的运行效率。这种域隔离方案是解决系统实时防护的有效方法,但需要嵌入式操作系统的配合,并提供完整的内存管理的地址信息。因此,针对安全防护的需要,改进系统的结构也是必须研究的内容。

软件平台安全的关键在于操作系统,访问控制是有效的手段,但缺乏足够的理论支撑和安全性测量方法,这也是可信计算技术面临的问题之一。因此在操作系统的安全性研究上,通常侧重在理论指导下构建安全模型,从而增强系统的安全性。

系统软件与应用软件的完整性测量对构建安全体系至关重要。但完整性测量计算量很大,如何设计计算量小且有效的完整性测量算法有实际应用价值。如对软件代码随机抽取比特信息再做摘要,运算量会大幅度下降,但如何抽取和与验证端同步则是需要进一步研究的问题。

## 5 结束语

预计在不远的将来,手机终端将成为真正意义上的互联网终端。用户使用手机能实现个人电脑几乎所有的功能,如电子商务、收发邮件、手机钱包等。如果手机的安全问题得不到有效解决,将成为严重制约这些应用发展的瓶颈。

移动网络安全问题需要从整个网络出发整体考虑,将传统的由用户自行处理的终端杀毒方法转移到由网络运营商,为移动用户提供安全服务。由于运营商在技术、设施、管理等方面具有优势,能够为移动网络安全提供有力保障。

可以预见,随着移动网络安全事

件的不断出现,能否为用户提供优质的安全服务,将成为移动网络运营商商业竞争能否取胜的关键。基于安全服务的整体安全解决方案,将成为未来网络信息安全的主流发展方向。

## 6 参考文献

- [1] LEI Min, BI Hai, FENG Zhengjin. Security Architecture and Mechanism of Third Generation Mobile Communication [C]// Proceedings of the 2002 IEEE Region 10 Conference on Conference on Computers, Communications, Control and Power Engineering (TENCON'02): Vol 2, Oct 28-31, 2002, Beijing, China. Piscataway, NJ, USA: IEEE, 2002:813-816.
- [2] YANG Hao, RICCIATO F, LU Songwu, et al. Securing a Wireless World [J]. Proceedings of the IEEE, 2006,94(2): 442-454.
- [3] ZHENG Yu, HE Dake, YU Weichi, et al. Trusted Computing-Based Security Architecture for 4G Mobile Networks [C]// Proceedings of the 6th International Conference on Parallel and Distributed Computing, Applications and Technologies(PDCAT'05), Dec 5-8,2005, Dalian, China. Los Alamitos, CA,USA: IEEE Computer Society, 2005:251-255.
- [4] 戴沁芸,王允非. 网络安全迎来3G时代 [J]. 信息安全与通信保密, 2010(5):34-39.
- [5] AL-FAYOUMI M, NASHWAN S, YOUSEF S, et al. A New Hybrid Approach of Symmetric/Asymmetric Authentication Protocol for Future Mobile Networks [J]. Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB'07), Oct 8-10, 2007, White Plains, NY, USA. Piscataway, NJ, USA: IEEE, 2007:29.
- [6] AL-MUHTADI J, MICKUNAS D, ROY CAMPBELL R. A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices [J]. IEEE Wireless Communications, 2002,9(2):60-65.
- [7] ZHANG Muxiang, FANG Yuguang. Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol [J]. IEEE Transactions on Wireless Communications, 2005,4(2):734-743.
- [8] DIAB W B, PRISM S. VPN Solution for Securing Voice over Third Generation Networks [C]//Proceedings of the 2nd International Conference on Internet Multimedia Services Architecture and Applications (IMSAA'08), Dec 10-12,2008, Bangalore, India. Piscataway, NJ, USA: IEEE, 2008:6p.
- [9] KAMBOURAKIS G, ROUSKAS A, GRITZALIS S. Using SSL/TLS in Authentication and Key Agreement [C]//Proceedings of the 4th International Workshop on Mobile and Wireless Communications Network (MWCN'02), Sep 9-11,2002, Stockholm, Sweden. Piscataway, NJ, USA: IEEE, 2002: 152-156.
- [10] AIASH M, MAPP G, LASEBAE A, et al. Providing Security in 4G Systems: Unveiling the Challenges [C]//Proceedings of the 6th Advanced International Conference on Telecommunications (AICT'10), May 9-15, 2010, Barcelona, Spain. Los Alamitos, CA, USA: IEEE Computer Society, 2010: 439-445.
- [11] DENG Yaping, FU Hong, XIE Xianzhong, et al. A novel 3GPP SAE Authentication and Key Agreement Protocol [C]//Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content(IC-NIDC'09), Nov 6-8,2009, Beijing, China. Piscataway, NJ, USA: IEEE 2009:557-561.
- [12] 陆峰,郑康锋,钮心忻,等. 3GPP认证与密钥协商协议安全性分析 [J]. 软件学报, 2010,21(7): 1768-1782.
- [13] 汪欣荣. 基于IPSec VPN的手机安全系统研究 [J]. 计算机安全, 2009(1):52-54.
- [14] 刘威鹏,胡俊,方艳湘,等. 基于可信计算的终端安全体系结构研究与进展 [J]. 计算机科学, 2007, 34(10): 257-269.
- [15] 吕海军,陈前斌,吴小平. 智能手机病毒的发展及其对策研究 [J]. 信息安全与通信保密, 2008, 30(1):80-82.
- [16] 黄丹,桑梓勤. 移动通信网络病毒防治方案浅析 [J]. 光通信研究, 2008(2):39-43.
- [17] 吴振强,马建峰. 基于TPM的移动互联网络可信体系架构研究 [J]. 网络安全技术与应用, 2007(11):18-20.
- [18] NTT, DoCoMo, IBM, et al. Trusted Mobile Platform Hardware Architecture Description [EB/OL]. [2004-10-27]. [http://www.trusted-mobile.org/TMP\\_HWAD\\_rev1\\_00.pdf](http://www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf).
- [19] HALFHIL T R. ARM DonsArmor - TrustZone Security Extensions Strengthen ARMv6 Architecture [R]. Microprocessor Report, 2003.

收稿日期:2010-11-18

## 作者简介



**胡爱群**,东南大学信息安全研究中心主任、教授、博导;主要从事无线网络及其安全技术研究。



**李涛**,东南大学信息科学与工程学院在读博士研究生;主要研究方向为移动可信计算技术。



**薛明富**,东南大学信息科学与工程学院在读博士研究生;主要研究方向为移动可信计算技术。



# 物联网技术及其标准

## Internet of Things: Technologies and Standard

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0027-05

**摘要:** 物联网有3个层次, 从下到上依次是感知层、传送层和应用层。物联网涉及的关键技术非常多, 从传感器技术到通信网络技术, 从嵌入式微处理节点到计算机软件系统, 包含了自动控制、通信、计算机等不同领域, 是跨学科的综合应用。目前介入物联网领域主要的国际标准组织有IEEE、ISO、ETSI、ITU-T、3GPP、3GPP2等, 这些标准组织在物联网总体架构、感知技术、通信网络技术、应用技术等方面制订了一系列标准。

**关键词:** 物联网; 关键技术; 标准

**Abstract:** Internet of Things has 3 layers; from bottom to top they are perception layer, transport layer, and application layer. It also involves sensor technology, communication network technology, embedded microprocessing nodes, and computer software system. With applications such as automatic control, communications, and computing, Internet of Things is thoroughly interdisciplinary. Currently, major international standards organizations involved in the standardization of Internet of Things includes IEEE, ISO, ETSI, ITU-T, 3GPP, 3GPP2. These standards organizations have developed a series of standards in the structure of things, sensing technology, communication networks, technology and application technology.

**Key words:** Internet of things; key technologies; standard

诸瑾文/ZHU Jinwen

(中国电信股份有限公司上海研究院, 上海  
200122)  
(China Telecom Corporation Limited Shanghai  
Research Institute, Shanghai 200122, China)

入式微处理节点到计算机软件系统, 包含了自动控制、通信、计算机等不同领域, 是跨学科的综合应用。

### (1) 感知层

物联网的感知层主要完成信息的采集、转换和收集。感知层包含两个部分: 传感器(或控制器)、短距离传输网络。

传感器(或控制器)用来进行数据采集及实现控制, 短距离传输网络将传感器收集的数据发送到网关或将应用平台控制指令发送到控制器。

感知层的关键技术主要为传感器技术和短距离传输网络技术, 例如射频标识(RFID)标签与用来识别RFID信息的扫描仪、视频采集的摄像头和各种传感器中的传感与控制技术、短距离无线通信技术(包括由短距离传输技术组成的无线传感网技术)。在实现这些技术的过程中, 又涉及到芯片研发、通信协议研究、RFID材料研究、智能节点供电等细分领域。

### (2) 传送层

物联网的传送层主要完成信息传递和处理, 传送层包括两个部分: 接入单元、接入网络。

接入单元是连接感知层的网桥, 它汇聚从感知层获得的数据, 并将数据发送到接入网络。接入网络即现

物联网描绘了人类未来全新的信息活动场景: 让所有的物品都与网络实现任何时间和任何地点的无处不在的连接。人们可以通过对物体进行识别、定位、追踪、监控并触发相应事件, 形成信息化解决方案。目前很多全球主要国家都制订了开发物联网的长期发展计划。中国已经把物联网明确列入《国家中长期科学技术发展规划(2006—2020年)》和《2050年国家产业发展路线图》。物联网作为一个新的领域有些什么关键技术? 物联网领域标准化方面进展如何? 本文将对此进行初步探讨。

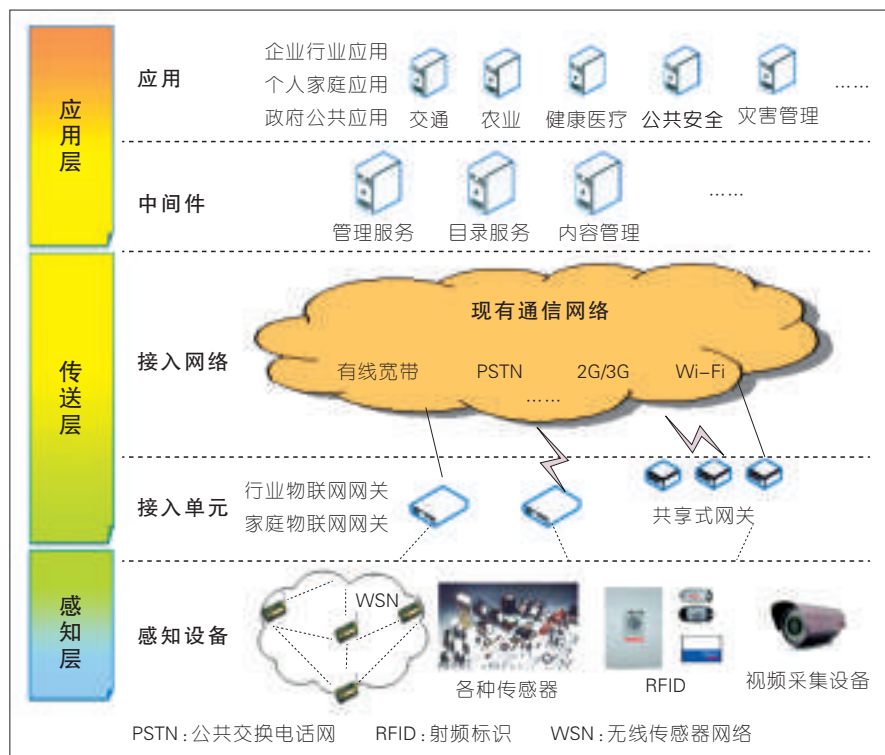
## 1 物联网关键技术

物联网技术不是对现有技术的

颠覆性革命, 而是通过对现有技术的综合运用。物联网技术融合现有技术实现全新的通信模式转变, 同时, 通过融合也必定会对现有技术提出改进和提升的要求, 催生出一一些新的技术。

在通信业界, 物联网通常被公认为有3个层次, 从下到上依次是感知层、传送层和应用层, 如图1所示。如果拿人来比喻的话, 感知层就像皮肤和五官, 用来识别物体, 采集信息; 传送层则是神经系统, 将信息传递到大脑进行处理; 应用层类似人们从事的各种复杂的事情, 完成各种不同的应用。

物联网涉及的关键技术非常多, 从传感器技术到通信网络技术, 从嵌



▲图1 物联网的3个层次

有的通信网络,包括移动通信网、有线电话网、有线宽带网等。通过接入网络,人们将数据最终传入互联网。

传送层是基于现有通信网和互联网建立起来的层。传送层的关键技术既包含了现有的通信技术,如移动通信技术、有线宽带技术、公共交换电话网(PSTN)技术、Wi-Fi 通信技术等,也包含了终端技术,如实现传感网与通信网结合的网桥设备、为各种行业终端提供通信能力的通信模块等。

### (3)应用层

物联网的应用层主要完成数据的管理和数据的处理,并将这些数据与各行业应用的结合。应用层包括两部分:物联网中间件、物联网应用。

物联网中间件是一种独立的系统软件或服务程序。中间件将许多可以公用的能力进行统一封装,提供给丰富多样的物联网应用。统一封装的能力包括通信的管理能力、设备的控制能力、定位能力等。

物联网应用是用户直接使用的

各种应用,种类非常多。物联网应用包括家庭物联网应用,如家电智能控制、家庭安防等,也包括很多企业和行业应用,如石油监控应用、电力抄表、车载应用、远程医疗等。

应用层主要基于软件技术和计算机技术实现。应用层的关键技术主要是基于软件的各种数据处理技术,此外云计算技术作为海量数据的存储、分析平台,也将是物联网应用层的重要组成部分。应用是物联网发展的目的。各种行业和家庭应用的开发是物联网普及的源动力,将给整个物联网产业链带来巨大利润。

## 2 物联网标准进展

在标准方面,与物联网相关的标准化组织较多。图2所示为全球主要物联网标准组织的徽标。

物联网覆盖的技术领域非常广泛,涉及总体架构、感知

技术、通信网络技术、应用技术等各个方面。物联网标准组织有的从机器对机器通信(M2M)的角度进行研究,有的从泛在网角度进行研究,有的从互联网的角度进行研究,有的专注传感网的技术研究,有的关注移动网络技术研究,有的关注总体架构研究。目前介入物联网领域主要的国际标准组织有 IEEE、ISO、ETSI、ITU-T、3GPP、3GPP2 等。

针对泛在网总体框架方面进行系统研究的国际标准组织比较有代表性的是国际电信联盟(ITU-T)及欧洲电信标准化协会(ETSI)M2M 技术委员会。ITU-T 从泛在网角度研究总体架构,ETSI 从 M2M 的角度研究总体架构。

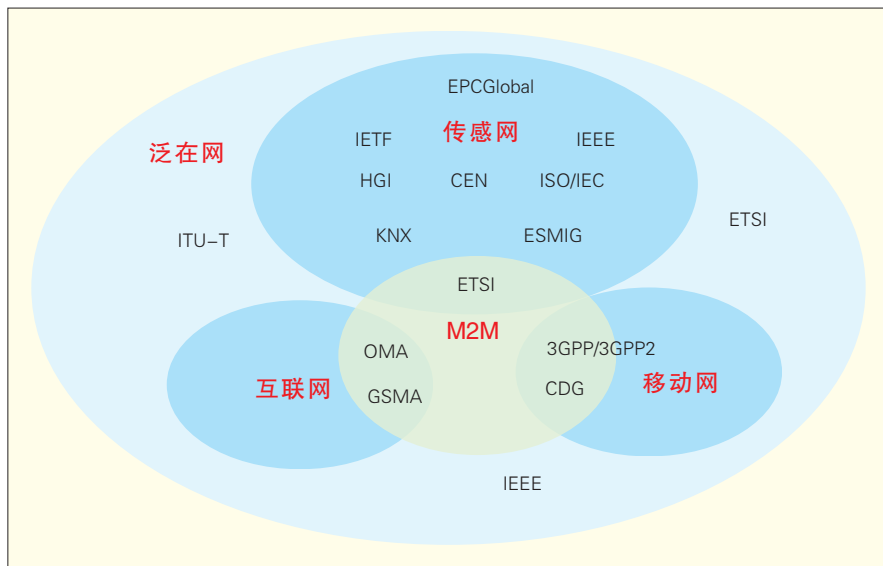
感知技术(主要是对无线传感网的研究)方面进行研究的国际标准组织比较有代表性的是国际标准化组织(ISO)、美国电气及电子工程师学会(IEEE)。

通信网络技术方面进行研究的国际标准组织主要有 3GPP 和 3GPP2。他们主要从 M2M 业务对移动网络的需求方面进行研究,只限定在移动网络层面。

在应用技术方面,各标准组织都有一些研究,主要是针对特定应用制订标准。



▲图2 全球主要物联网标准组织



▲图3 物联网在不同领域的主要标准组织分布情况

总的来说,国际上物联网标准工作还处于起步阶段,目前各标准组织自成体系,标准内容涉及架构、传感、编码、数据处理、应用等,不尽相同。

各标准组织都比较重视应用方面的标准制订。在智能测量、E-Health、城市自动化、汽车应用、消费电子应用等领域均有相当数量的标准正在制订中,这与传统的计算机和通信领域的标准体系有很大不同(传统的计算机和通信领域标准体系一般不涉及具体的应用标准),这也说明了“物联网是由应用主导的”观点在国际上已成为共识。

图3所示是物联网在不同领域的主要标准组织分布情况。本文选择一些在物联网领域重要的有一定影响力的标准组织进行简要介绍。

## 2.1 ITU-T 物联网标准进展

提到物联网标准,首先必须先提一下ITU-T。ITU-T早在2005就开始进行泛在网的研究,可以说是最早进行物联网研究的标准组织。

ITU-T的研究内容主要集中在泛在网总体框架、标识及应用3方面。ITU-T在泛在网研究方面已经从需求阶段逐渐进入到框架研究阶段,目前研究的框架模型还处在高层层面。

图4所示为ITU-T提出的物联网架构,曾经在各种场合被广泛引用。

ITU-T在标识研究方面和ISO通力合作,主推基于对象标识(OID)的解析体系;ITU-T在泛在网应用方面已经逐步展开了对健康和车载方面的研究。下面详细介绍ITU-T各个相关研究课题组的研究情况。

SG13主要从NGN角度展开泛在网相关研究,标准主导是韩国。目前

标准化工作集中在基于NGN的泛在网络/泛在传感器网络需求及架构研究、支持标签应用的需求和架构研究、身份管理(IDM)相关研究、NGN对车载通信的支持等方面。

SG16组成立了专门的问题组展开泛在网应用相关的研究,日、韩共同主导,内容集中在业务和应用、标识解析方面。SG16组研究的具体内容有:Q.25/16泛在感测网络(USN)应用和业务、Q.27/16通信/智能交通系统(ITS)业务/应用的车载网关平台、Q.28/16电子健康(E-Health)应用的多媒体架构、Q.21和Q.22标识研究(主要给出了针对标识应用的需求和高层架构)。

SG17组成立有专门的问题组展开泛在网安全、身份管理、解析的研究。SG17组研究的具体内容有:Q.6/17泛在通信业务安全、Q.10/17身份管理架构和机制、Q.12/17抽象语法规则(ASN.1)、OID及相关注册。

SG11组成立有专门的问题组“NID和USN测试规范”,主要研究节点标识(NID)和泛在感测网络(USN)的测试架构、H.IRP测试规范以及X.oid-res测试规范。



▲图4 ITU-T提出的物联网架构



ITU-T 还在智能家居、车辆管理等应用方面开展了一些研究工作。

## 2.2 ETSI 物联网标准进展

ETSI 采用 M2M 的概念进行总体架构方面的研究,相关工作的进展非常迅速,是在物联网总体架构方面研究得比较深入和系统的标准组织,也是目前在总体架构方面最有影响力的标准组织。

ETSI 专门成立了一个专项小组(M2M TC)从 M2M 的角度进行相关标准化研究。ETSI 成立 M2M TC 小组主要是考虑:目前虽然已经有一些 M2M 的标准存在,涉及各种无线接口、格状网络、路由和标识机制等方面,但这些标准主要是针对某种特定应用场景,彼此相互独立,如何将这些相对分散的技术和标准放到一起并找出不足,这方面所做的工作很少。在这样的研究背景下,ETSI M2M TC 小组的主要研究目标是从端到端的全景角度研究机器对机器通信,并与 ETSI 内 NGN 的研究及 3GPP 已有的研究展开协同工作。

M2M TC 小组的职责是:从利益相关方收集和制订 M2M 业务及运营需求,建立一个端到端的 M2M 高层体系架构(如果需要会制订详细的体系结构),找出现有标准不能满足需求的地方并制订相应的具体标准,将现有的组件或子系统映射到 M2M 体系结构中,M2M 解决方案间的互操作性(制订测试标准),硬件接口标准化方面的考虑,与其他标准化组织进行交流及合作。

## 2.3 3GPP/3GPP2 物联网标准进展

3GPP 和 3GPP2 也采用 M2M 的概念进行研究。作为移动网络技术的主要标准组织,3GPP 和 3GPP2 关注的重点在于物联网网络能力增强方面,是在网络层方面开展研究的主要标准组织。

3GPP 针对 M2M 的研究主要从移动网络出发,研究 M2M 应用对网络

的影响,包括网络优化技术等。3GPP 研究范围为:只讨论移动网的 M2M 通信;只定义 M2M 业务,不具体定义特殊的 M2M 应用。Verizon、Vodafone 等移动运营商在 M2M 的应用中发现了很多问题,例如大量 M2M 终端对网络的冲击,系统控制面容量的不足等。因此,在 Verizon、Vodafone、三星、高通等公司推动下,3GPP 对 M2M 的研究在 2009 年开始加速,目前基本完成了需求分析,转入网络架构和技术框架的研究,但核心的无线接入网络(RAN)研究工作还未展开。

相比较而言,3GPP2 相关研究的进展要慢一些,目前关于 M2M 方面的研究多处于研究报告的阶段。

## 2.4 IEEE 物联网标准进展

在物联网的感知层研究领域,IEEE 的重要地位显然是毫无争议的。目前无线传感网领域用得比较多的 Zigbee 技术就基于 IEEE 802.15.4 标准。

IEEE 802 系列标准是 IEEE 802 LAN/MAN 标准委员会制订的局域网、城域网技术标准。1998 年,IEEE 802.15 工作组成立,专门从事无线个人局域网(WPAN)标准化工作。在 IEEE 802.15 工作组内有 5 个任务组,分别制订适合不同应用的标准。这些标准在传输速率、功耗和支持的服务等方面存在差异。

TG1 组制订 IEEE 802.15.1 标准,即蓝牙无线通信标准。标准适用于手机、PDA 等设备的中等速率、短距离通信。

TG2 组制订 IEEE 802.15.2 标准,研究 IEEE 802.15.1 标准与 IEEE 802.11 标准的共存。

TG3 组制订 IEEE 802.15.3 标准,研究超宽带(UWB)标准。标准适用于个域网中多媒体方面高速率、近距离通信的应用。

TG4 组制订 IEEE 802.15.4 标准,研究低速无线个人局域网(WPAN)。

该标准把低能量消耗、低速率传输、低成本作为重点目标,旨在为个人或家庭范围内不同设备之间的低速互联提供统一标准。

TG5 组制订 IEEE 802.15.5 标准,研究无线个人局域网(WPAN)的无线网状网(MESH)组网。该标准旨在研究提供 MESH 组网的 WPAN 的物理层与 MAC 层的必要的机制。

传感器网络的特征与低速无线个人局域网(WPAN)有很多相似之处,因此传感器网络大多采用 IEEE 802.15.4 标准作为物理层和媒体存取控制层(MAC),其中最为著名的就是 ZigBee。因此,IEEE 的 802.15 工作组也是目前物联网领域在无线传感网层面的主要标准组织之一。中国也参与了 IEEE 802.15.4 系列标准的制订工作,其中 IEEE 802.15.4c 和 IEEE 802.15.4e 主要由中国起草。IEEE 802.15.4c 扩展了适合中国使用的频段,IEEE 802.15.4e 扩展了工业级控制部分。

## 2.5 中国物联网标准进展

总的来说,中国物联网标准的制订工作还处于起步阶段,但发展迅速。目前中国已有涉及物联网总体架构、无线传感网、物联网应用层面的众多标准正在制订中,并且有相当一部分的标准项目已在相关国际标准组织立项。中国研究物联网的标准组织主要有传感器网络标准工作组(WGSN)和中国通信标准化协会(CCSA)。

WGSN 是由中国国家标准化管理委员会批准筹建,中国信息技术标准化技术委员会批准成立并领导,从事传感器网络(简称传感网)标准化工作的全国性技术组织。WGSN 于 2009 年 9 月正式成立,由中国科学院上海微系统与信息技术研究所任组长单位,中国电子技术标准化研究所任秘书处单位,成员单位包括中国三大运营商、主要科研院校、主流设备厂商等。传感器网络标准工作组将

“适应中国社会主义市场经济建设的需要,促进中国传感器网络的技术研究和产业化的迅速发展,加快开展标准化工作,认真研究国际标准和国际上的先进标准,积极参与国际标准化工作,并把中国和国际标准化工作结合起来,加速传感网标准的制修订工作,建立和不断完善传感网标准化体系,进一步提高中国传感网技术水平。”作为其宗旨。目前 WGSN 已有一些标准正在制订中,并代表中国积极参加 ISO、IEEE 等国际标准化组织的工作。由于成立时间尚短,目前 WGSN 还没有形成可发布的标准文稿。

CCSA 于 2002 年 12 月 18 日在北京正式成立。CCSA 的主要任务是为了更好地开展通信标准研究工作,把通信运营企业、制造企业、研究单位、大学等关心标准的企事业单位组织起来,按照公平、公正、公开的原则制订标准,进行标准的协调、把关,把高技术、高水平、高质量的标准推荐给政府,把具有中国自主知识产权的标准推向世界,支撑中国的通信产业,为世界通信做出贡献。2009 年 11 月,CCSA 新成立了泛在网技术工作委员会(即 TC10),专门从事物联网相关的研究工作。虽然 TC10 刚刚成立不久,但在 TC10 成立以前,CCSA 的其他工作委员会对物联网相关的领域也进行过一些研究。目前 CCSA 有多个与物联网相关的标准正在制订中,但尚未有发布标准文稿。

与物联网相关的,还有 2009 年 4 月成立的 RFID 标准工作组。RFID 工作组在信息产业部科技司领导下开展工作,专门致力于中国 RFID 领域的技术研究和标准制订,目前已有一定的工作成果。

上述标准组织各自独立开展工作,各标准组的工作各有侧重。WGSN 偏重传感器网络层面,CCSA TC10 偏重通信网络和应用层面,RFID 标准工作组则关注 RFID 相关的领域。同时各标准组的工作中也有不少重复的部分,如 WGSN 也会涉及到传感器网络以上的通信部分和应用部分的内容,而 CCSA 也涉及到了一些传感网层面的工作内容。对于这些重复的部分,各标准组之间目前还没有很好的横向沟通和协调机制,因此,近期国家层面正在筹备成立“物联网标准联合工作组”。联合工作组旨在整合中国物联网相关标准化资源,联合产业各方共同开展物联网技术的研究,积极推进物联网标准化工作,加快制订符合中国发展需求的物联网技术标准,为政府部门的物联网产业发展决策提供全面的技术和标准化服务支撑。

### 3 结束语

物联网技术内容众多,所涉及到的标准组织也较多,不同的标准组织基本上都按照各自的体系进行研究,采用的概念也各不相同。

总体架构层面,目前分感知层、

网络层、应用层的 3 层架构已经得到业界的共识,但是对于 3 层之间的具体界限、研究内容尚未有统一的共识,总体性的概念和术语,也尚未统一。在感知层,传感器技术已经历数十年的发展,相对成熟,并已形成了专门的学科。目前传感器种类繁多,并已在各行各业被广泛应用,而无线传感网技术尚处于百家争鸣的阶段,是物联网研究重点之一。网络层的远程通信技术以现有的包括移动网、固网、宽带、窄带等通信网络技术为基础,在此基础上探讨通信网络如何更好地适应承载物联网应用,是保障物联网应用有序发展的前提。物联网应用种类繁多,涉及社会生活各个方面,是物联网研究的重点。<sup>[1-3]</sup>

### 4 参考文献

- [1] 祁庆中. 物联网与 M2M 业务的战略思考 [J]. 中兴通讯技术, 2010, 16(1): 3-6.
- [2] 史敏锐. 移动通信网承载物联网业务的研究 [J]. 电信科学, 2010, 26(7): 19-22.
- [3] 黄海昆, 邓佳佳. 物联网网关技术与应用 [J]. 电信科学, 2010, 26(4): 56-59.

收稿日期: 2010-11-22

### 作者简介



诸瑾文, 中国电信股份有限公司上海研究院高级产品经理, CCSA TC10 WG3 组组长; 研究方向为物联网领域技术研究、产品开发、行业标准制订; 已发表相关论文 4 篇, 出版专著 1 本, 申请专利 2 项。

## 综合信息

### 中兴通讯荣膺《亚洲电信》“最佳年度宽带网络供应商”

【本刊讯】在《亚洲电信》杂志举办的 2010 年度读者评选的最佳年度供应商活动中, 中兴通讯凭借其宽带产品领域持续的技术创新和市场份额的快速增长, 荣获了“2010 年度最佳宽带网络供应商”奖。这是继 2009 年 IPTV 产品获奖后, 中兴通讯再度获得年度最佳供应商奖。

近年来, 中兴通讯的宽带接入产品在国际著名论坛上屡次获奖。2007 年, 中兴通讯固网宽带产品以“xPON+VDSL2”组合技术方案获国际工程协会(IEC)颁发 InfoVision 技术创新奖; 2008 年, 中兴通讯以 DSL 9806H 产品在伦敦 SOFNET 论坛上获得“最佳绿色创新奖”; 2010 年, 中兴通讯以“ZX10 C300 下一代光接入平台”设备再次荣获 InfoVision 技术创新奖。

# 车载物联网技术探讨

## Vehicular Networks: A Case for the Internet of Things

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0032-06

**摘要:** 基于车载无线通信技术的新进展, 文章讨论了未来车载网络中不同网络协议层面临的挑战; 信息传播是车载网络研究中最重要研究课题之一, 文章围绕信息这一中心元素, 讨论了宏观和微观信息传播过程中面临的挑战; 文章还介绍了美国和欧洲几个典型的车载网络应用案例。

**关键词:** 物联网; 车载网络; 信息传播

**Abstract:** This paper presents recent advances in wireless communication technologies in vehicular environments. It discusses research challenges in different protocol layers with a focus on information dissemination from an information-centric perspective. Some vehicular network projects that are currently underway around the world are also reviewed.

**Key words:** Internet of things; vehicular networks; information dissemination

俞波/YU Bo<sup>1</sup>

须成忠/XU Chengzhong<sup>1</sup>

过敏意/GUO Minyi<sup>2</sup>

(1. 美国韦恩州立大学, 密歇根州 底特律市, 48202;

2. 上海交通大学, 上海 200030)

(1. Wayne State University, Detroit 48202, USA;

2. Shanghai Jiao Tong University, Shanghai 200030, China)

### 1 车载物联网概念

车载物联网是一项新兴技术, 可以大幅提高未来交通系统的安全和效率, 并将车辆连接到计算机网络。车载物联网能够在行驶中的车辆之间建立无线通信, 也能够通过在过路车辆和路边基站之间建立无线通信。利用多跳转发的方式, 车载网络能够让两个在信号范围之外的车辆也建立通信连接。车载网络将成为未来智能交通系统的重要组成部分。

当前的智能交通系统严重依赖于预先部署的基础设施。例如, 嵌入路面的电磁感应器, 部署在主要道路交叉口的交通摄像头, 高速公路收费口安装的射频标签(RFID)读取器。通常, 一个收集和发布交通信息的典型过程如下: 首先, 路面传感器对车流

的速度、密度进行检测, 然后上传到城市交通中心。经过数据处理之后, 流量报告可以通过蜂窝网络传递到用户的手机。这样来传播与位置相关的信息是一个昂贵和低效的方式, 因为通常信息源和信息消费者的实际距离只有几百米远。

车载网络的短距离通信能力将会改变这种传统的智能交通系统的通信模式, 以更直接的方式帮助信息的产生、传播和消费。

本质上车载物联网是一个巨大的无线传感器网络。每一辆汽车都可以被视为一个超级传感器节点。通常一辆汽车装备有内部和外部温度计、亮度传感器、一个或多个摄像头、麦克风、超声波雷达, 以及许多其他装备。此外, 未来的汽车将配备一个车载计算机、GPS定位仪和无线收发装置。这使得汽车之间, 以及汽车和路边基站之间能够无线通信。这种前所未有的无线传感器网络扩展

了计算机系统对整个世界的感知与控制能力, 并可以让信息在本地产生和共享, 不必涉及庞大的基础设施。

未来的汽车和车载网络为人们提供了一系列应用。车载网络的应用可分为4个类别。

#### (1) 安全应用

安全应用包括碰撞预警、电子路牌、红绿灯警告、网上车辆诊断、道路湿滑检测等。通常这类应用利用短距离通信实时性的特点来为司机提供即时警告。

#### (2) 效率应用

效率应用包括城市交通管理、交通拥塞检测、路径规划、公路收费、公共交通管理等。这类应用致力于改善公众和个人的出行效率。

#### (3) 商业应用

商业应用包括基于位置的服务, 将带给人们巨大的商机。这些商业应用的种类繁多, 如, 最近的餐馆、最便宜的加油站、商场促销信息等。这些可能的商业应用将为服务业带来新的竞争手段。

#### (4) 信息娱乐应用

信息娱乐应用包括视频和音乐共享、基于位置的餐厅评论、拼车、社

**基金项目:** 美国自然科学基金项目 (CCF-0914330、CNS1016969); 中国自然科学基金海外合作项目(61028005)

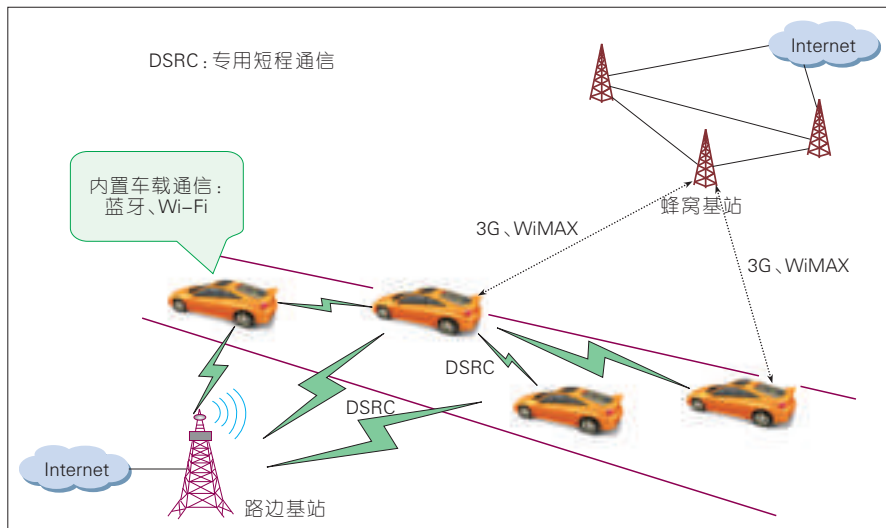


交网络等。实际上,信息娱乐的一些应用,如福特 SYNC<sup>[1]</sup>和起亚 UVO,已成为当前汽车市场的一个引人注目的亮点。信息娱乐系统的网络化将是必然趋势。

在车载网络的发展过程中,有4类参与者将起到积极的作用。4类参与者为政府、汽车制造商、本地零售商和消费者。传统智能交通系统由各国政府主导进行投资和实施,其他少数几个地理信息系统(GIS)公司,如谷歌、Garmin、TomTom 等公司也参与了交通信息的采集和发布。然而,未来的车载网络将吸引更多的参与者,并使他们从车载网络中获取巨大的商业利润。首先,汽车制造商将很乐于开发装备车载网络的汽车,这将增强汽车的安全性,并提供更丰富的车内娱乐系统,从而进一步提高其汽车的竞争力。汽车电子化是一种必然趋势,安全系统和信息娱乐系统的电子化是进程的两个主要方面。福特 SYNC 车载信息娱乐系统是一个非常成功的例子。其次,本地零售商及服务商家也将非常感兴趣,车载网络将十分方便地传播他们的促销信息以及推广他们的服务。车载网络会带来激烈的商业竞争。最后,毫无疑问,这些增强的安全性、提高效率、价廉物美的商品、丰富的娱乐应用等将吸引更多的消费者,并使他们成为最终受益者。

## 2 车载物联网无线通信技术

无线个人局域网(WPAN)在消费电子产品(包括汽车电子产品)领域取得了巨大成功。福特的 SYNC 是一个很好的例子。它通过蓝牙技术将司机的手机连接到汽车的音响系统,因而司机可以在行驶中通过语音命令播放音乐或拨打电话。由于大规模生产降低了成本,802.11a/b/g 无线局域网技术已经被广泛使用。虽然 802.11a/b/g 最初不是针对车载环境而设计的,但由于其被广泛使用带来的优势,许多研究人员在车载环境中进



▲图1 未来车载无线通信混合架构

行了实验,如文献[2-4]对 802.11a/b/g 在车载环境中的应用进行了一系列实验。802.11p 和专用短程通信(DSRC)标准对 802.11 标准进行了扩充,以使其能够适应车载环境的无线通信<sup>[5-6]</sup>。802.11p 技术使用 5.9 GHz 频段,能够在移动的车辆之间,以及移动车辆和路边基站之间建立短距离无线通信。无线城域网(WMAN),也称为 WiMAX(即 IEEE 802.16),是另一项新兴技术。无线城域网能够以不同的方式提供长距离传输,例如,两个固定位置的节点之间的通信,以及类似于蜂窝系统的移动节点通信。然而,目前为止,最常见的车载通信技术还基于蜂窝网络,通常称之为汽车远程信息处理。通用汽车的 OnStar 系统<sup>[7]</sup>和福特的 RESCU 系统都基于这一类技术。一些地理信息系统公司,如 TomTom 和 Garmin 等,也使用蜂窝网络来传输实时交通信息。通常情况下,基于蜂窝的远程信息处理是一种基于用户订阅的有偿服务。

本文认为在不久的将来车载通信将建立于一种混合式的架构,如图1所示。在这种混合架构中,长距离通信技术,如蜂窝网络和 WiMAX,能够为人们提供即时的互联网接入;而短距离通信技术,如 DSRC、Wi-Fi(即 802.11a/b/g),则能够为安全系统提供

实时响应的保障以及为基于位置的信息提供有效支持。

本文认为车载自组织网络(VANET)将在未来智能交通系统中发挥重要作用。车载自组织网络依靠短距离通信技术实现车与车以及车与路边基站之间的通信。与传统的基础设施网络相比,车载自组织网络有两个主要优势:首先,车载自组织网络具有成本低、容易部署和操作的优点。消费者无需订阅即可享受服务。其次,从技术角度来看,智能交通系统中传播的很多信息有很强的位置相关性,车载自组织网络能够很方便地为临近车辆建立实时或者非实时的短距离通信。

## 3 车载物联网面临的挑战

车载网络所独有的特性给人们带来了前所未有的挑战,然而,与此同时,这些特性也使人们能够从以往不同的角度去思考和解决问题。

车载网络分3层:链路层、网络层和应用层。各网络协议层面临不同的挑战。

### 3.1 链路层面临的挑战

在链路层,面临的主要挑战是如何使链路层协议适应独特的车辆运行环境,使链路层获得最佳性能。链

路层协议包括3个主要设计目标:响应能力、可靠性和可扩展性。首先,链路层协议需要能够对信道条件和车辆的移动性快速响应,同时协议的可靠性和可扩展性对与安全相关的应用也起着重要的作用。一些传统的链路层协议的设计方法,如无线接入点(AP)握手、媒体访问控制(MAC)层超时管理、地址解析协议(ARP)超时等,在高速移动的车载环境中已显示出低下的性能。这些传统的设计方法通常会导致增加的启动延时、未充分利用的带宽,以及带宽的不公平分配。

实际上,可扩展性和可靠性在一定程度上互相影响,互相作用。可靠广播技术也是重要的研究问题之一。目前的可靠广播技术一般包括重复广播、合作式传递、发射功率自适应等。可靠性和可扩展性仍然值得进一步深入研究,特别是针对车辆安全系统的应用,因为最终用户对车辆安全系统要求很高。

### 3.2 网络层面临的挑战

在网络层,面临的主要挑战是建立一个新的路由模式,以促进车载网络的信息传播。在过去10年中,无线自组织网络方面得到广泛研究。特别是,研究人员为车载网络提出了许多具有环境自适应能力的路由协议,如MDDV<sup>[8]</sup>和VADD<sup>[9]</sup>。这些协议利用车辆的移动性,通过GPS定位技术、数字地图技术,在车载网络环境中提高数据包的转发性能。从本质上讲,这些协议都是针对以数据包为基本单位而设计。数据包在从源到目的地的整个转发过程中都保持不变。然而,这种基于分组转发的模式已不能适应以信息为中心的应用需求。首先,对于某些应用转发路由没有明确的数据源和目的地。信息由某些节点共同产生,然后传递给另一些节点。其次,信息在传递的过程中会被修改。如在交通阻塞的检测中,每部车都能产生交通拥塞报告,而这

个报告可以和其他临近的车辆产生的报告相融合。所有向拥塞地点行驶的车辆是这些报告的接收者。在这类应用中,人们事先并不知道什么时间、什么地点、哪些车辆会产生报告,人们也不知道谁会成为接收者。有一些基于分组转发的路由协议,例如多播技术和基于位置的广播技术,能够部分解决这类应用的需求。然而,从本质上讲,人们需要一个新的路由模式,能够为以信息为中心的数据传输提供支持,这个模式将能够有助于信息的产生,融合,传播和删除。

### 3.3 应用层面临的挑战

在应用层,人们所面临的主要挑战是如何有效地表示、发现、存储和更新整个网络的信息。

命名和寻址是车载网络的核心问题。如何有效地将真实世界的信息建立索引,以方便信息存储和传播,是一个有待研究的问题。本文认为寻址将采用混合型、多层次的方案,真实世界的环境信息将起重要作用。命名和寻址政策对系统中的其他协议,如路由和信息发现有重大影响。由于车辆的高移动性,另一个挑战是如何动态地将车辆的标签(ID)映射到基于位置的地址,如在基于位置的广播中,人们需要知道在某一区域内的所有车辆列表。这个问题对于整个混合网络体系都有非常重要的影响。本文认为可以在车辆以及路边基站上实现类似地址解析协议/反向地址解析协议(ARP/RARP)来帮助解决这个问题。

分布式数据管理是另一个车载

网络中具有挑战性的问题。它包括数据复制、数据删除、缓存管理等一系列问题。传统的分布式数据管理假定在地理上分散的多台服务器连接在同一网络,这在车载自组织网络中不再成立。从本质上讲,人们可以把车载网络看作一个巨大的分布式数据库系统,其中每个车辆维护一个本地的数据库。车和车间不定期交换数据,从而逐步更新全局数据库系统。从全局的角度来说,不一致性不可避免。为此,一个研究问题是如何以最小的开销来维护一个相对一致的分布式数据库。

## 4 车载物联网中的信息传播

本文认为车载网络是一个以信息为中心的分布式系统,信息在网络的不同位置生成、收集和发布。人们可以把信息传播分为两个不同的层次:宏观信息传播和微观信息传播。以信息为中心来发现系统需求十分重要。表1列出了宏观和微观层次上主要的研究课题和及其代表性的工作。

### 4.1 宏观信息传播

宏观信息传播指在一个特定的地理区域里将信息传递给一个或一组节点。信息传播的目的地是网络中的特定的单个节点或者一组指定的节点组,甚至可能是一组未知节点。宏观信息传播的目的是减少信息传递延时,减少传递开销(包括存储开销和通信开销),并提高未来查询的成功率(如果接收节点是事先未知的)。宏观信息传播的研究课题通

表1 车载网络中信息传播的代表性工作

信息传播的分类		代表性工作
宏观	基于基础设施	见文献[10]
	容迟网络路由	见文献[11]、文献[12]、文献[13]、文献[14]
	数据融合、数据缓存	见文献[15]、文献[16]、文献[17]
微观	单跳	见文献[2]、文献[3]、文献[4]
	多跳转发	见文献[8]、文献[9]、文献[18]
	资源管理	见文献[17]、文献[19]、文献[20]

常包括信息路由、数据缓存、数据融合等。

信息传播可以建立在基础设施之上,也可以不依赖基础设施。Jedrzej等<sup>[10]</sup>提出建立于蜂窝网络基础设施上的P2P叠加网络。车辆通过蜂窝网络的基础设施建立到互联网的可靠链接,然后这些车辆之间可以以P2P叠加网络的方式来实现非安全应用的信息共享、发现和交换。然而,由于基础设施提供的服务通常是付费订阅的方式,这实际上限制了消费者的数量。与基于基础的网络服务相比,相对廉价的自组织网络方案显得更有吸引力。另一方面,大多数的非安全应用没有严格的实时性要求,因而,当前的一项研究热点是以容迟的方式来实现车载自组织网络的信息传播。研究者提出了一些通用的容迟网络路由协议,如流行性路由<sup>[12]</sup>。还有一些前摄的办法,如文献[13]、文献[14]利用预知的地理位置、连接模式和可能的运动方向来帮助信息传播。一些现有的容迟网络(DTN)路由协议假定一个预定义源和目的地。如Small和Hass的研究<sup>[11]</sup>建立了监控野生鲸鱼的DTN网络。他们在鲸鱼的背上安装一个传感器节点,鲸鱼的运动信息就以容迟的方式一跳一跳地传递到接收站。

数据缓存和数据融合也是车载自组织网络中热门的研究方向。Zhao等人<sup>[15]</sup>使用了定期广播和缓冲的方法从数据中心分发信息到车载自组织网络。根本上来说,它是一个从数据中心到车辆的单向信息传播。Lochert等人<sup>[21]</sup>提出了一个层次性的数据融合方案。该方案定义了一组地标来帮助计算旅行时间。他们还提出了一个路边基站的部署算法来优化信息融合。

在车载自组织网络中,信息的传播、缓存和融合都有过相应的研究。然而,在车载自组织网络中,大多数类型的信息中并不包括任何目标车辆的先验知识,因而容迟的数据传

播、数据查询、数据缓存以及数据融合密切地联系在了一起。任何车辆可能会产生并发出一个查询,且希望其临近车辆能尽快响应。

传统的包路由已不能适应以信息为中心的应用,人们需要建立一个全新信息路由模式。首先,需要定义信息路由的目的地。对大多数人而言,传播的目的地是一个虚拟的概念。它受时间、空间和车辆的限制。换句话说,目的地包括的是所有满足当时时空条件的车辆。有两个基本的信息传播模式:拉(Pull)模式和推(Push)模式。拉是指一辆车定期广播它感兴趣的查询,并从邻居车辆中获取数据。推模式是指车辆有目的地把信息推入周边的车辆,使得对此信息感兴趣的用户可以更方便地得到这些信息。在车载网络技术市场化的初级阶段,只有较少比例的车辆具备车载通信能力,通信仅限于一跳,因此推模式更为重要。当制订推模式的策略时,人们必须考虑到数据缓存和融合的潜在影响。人们可以利用启发式的周边信息(如行驶方向、速度、经常光顾的地方等)或社交网络信息来预测和控制传播。

#### 4.2 微观信息传播

微观信息传播指涉及一跳或者几跳的局部信息传递。在车载网络技术市场化的初级阶段,车辆很少有机会遇到其他车辆或路边基站。所以,提高两车相遇时信息传播的效率十分重要。

最近的一些研究关注于车载环境中的单跳通信性能。Bychkovsky等人<sup>[2]</sup>研究了在公共Wi-Fi无线网络中提高单跳通信的数据吞吐量的技术。他们进行了一系列的实地测试来调查在MAC握手、获取IP地址、建立IP路由等时候可能的性能损失。Hadaller等人<sup>[4]</sup>进行了以802.11协议为基础的单跳通信的实验,并提供了详细的实验分析。通过实验,他们发现了一些现有无线访问机制在数据

吞吐量方面低效的根本原因。以上这些工作从底层协议(物理层、MAC地址、路由)的角度来分析和改进链路吞吐量。

微观信息传播也涉及局部多跳通信。一般来说,本地多跳通信的主要任务是协调本地车辆并帮助信息沿预定方向传播。VADD<sup>[9]</sup>是一种利用车流模式和道路拓扑来找到传递数据包的最优道路的转发协议。MDDV<sup>[8]</sup>利用车辆的流动性来帮助信息传播。MDDV使周边的车辆协作转发数据包,以此来提高数据包转发的可靠性。Zhao等人<sup>[18]</sup>研究了如何以路边基站作为中继的方式来提高吞吐量。

由于两车相遇时有效通信时间短暂,有效的信道资源管理是一个是十分重要的问题。Chang等人<sup>[19]</sup>提出了一种从路边基站到过往车辆的下行调度算法。Zhang等人<sup>[20]</sup>提出了另一种同时考虑上行和下行请求的调度算法。Yu等人<sup>[17]</sup>研究了在路边基站负载接近超负荷的情况下的请求许可控制问题。这些研究从不同的资源分配角度提高了路边基站的访问效率。

通常,微观信息传播的主要挑战在于如何把下层条件(车辆移动性、无线信道、相对位置)和上层应用的需求联系在一起。从上层的角度来看,容迟网络的应用可以容忍一定的信息延迟和误差。从底层的角度来看,移动性、信道和车辆位置却可能在很短的时间内大幅变化。现有的工作研究了不同的网络通信协议下的单跳问题,然而,仍然缺少一个上层和下层之间的有效联系。这种联系可以使人们能够利用底层的苛刻条件,而不是受其限制。

当人们设计微观信息传播协议时,可以重点关注3方面的问题:

##### (1) 应用需求

容迟网络的应用不一定需要一个可靠的链接,但是他们却需要根据数据传输的重要性来安排数据的优



先性。人们还希望能够设定一个在传播的过程中允许的信息丢失程度阈值。

### (2) 资源管理

主要问题包括如何调度低层资源(例如传输信道、传输速率等),如何调度上层任务,如何分配资源以确保公平等。

### (3) 协作

人们可以利用多任务调度、转发、中继、多方网络编码等不同的技术来帮助在信号范围内各车辆的互相协作,提高整体性能。

## 5 车载物联网应用案例

FleetNet<sup>[23]</sup>是一个由欧洲多个汽车公司、电子公司和大学的合作项目,合作者包括 NEC 公司、DaimlerChrysler 公司、Siemens 公司和 Mannheim 大学。该项目利用无线多跳自组织网络技术实现无线车载通信,能够有效提高司机和乘客的安全性和舒适性。FleetNet 的设计目标包括实现近距离多跳信息传播以及为司机和乘客提供位置相关的信息服务。在该项目中,位置信息起着重要的作用,一方面它本身是 FleetNet 一些应用的基本需求,另一方面它也能使得通信协议更有效地运作。NEC 欧洲实验室和 Mannheim 大学为车载网络设计了基于位置的路由和转发算法,然后基于该算法实现了一个基于位置的车-车通信路由器。研究人员建立了一个由 6 辆车组成的实验网络,其中每辆车装备了一个 GPS 接收器、一个 802.11 无线网卡,以及一个车-车通信路由器。另外,每辆车还装备了一个 GPRS 接口,这样可以实现对自组织网络中的每辆车进行实时监控。

CarTalk<sup>[23]</sup>是一个欧洲的司机辅助系统研究项目。该项目利用车-车通信技术为移动中的车辆建立一个移动自组织网络,来帮助增强道路系统的安全性。例如,当一个车辆刹车的时候或者检测到危险的道路状况的

时候,它会给后方车辆发送一个警告消息。即使在前方有其他车辆遮挡的情况下,后方车辆也能够尽早得到警告。这个系统同时也能够帮助车辆更安全地驶入高速公路和驶离高速公路。

California Path<sup>[24]</sup>是加州大学伯克利分校的一个关于智能交通系统的综合性研究项目。该项目始建于 1986 年,主要由伯克利分校的交通研究院负责管理,同时也和加州交通部有密切合作。California Path 致力于运用前沿技术解决和优化加州道路系统存在的问题,其主要关注于 3 个方面的研究:

#### (1) 交通系统运筹学研究

其研究方向包括车流管理、旅行者信息管理、监控系统、数据处理算法、数据融合和分析等。

#### (2) 交通安全研究

研究内容包括十字路口协同安全系统研究、司机行为建模、工人与行人相关的安全研究等。

#### (3) 新概念应用研究

该研究致力于发现、验证在公共交通系统中的新概念和方法,帮助减少交通系统的阻塞,提高公共交通的出行效率。

MIT CarTel<sup>[25]</sup>是麻省理工学院的一个分布式移动传感器网络和远程通信系统。CarTel 的应用能够收集、处理、传递、分析和可视化来自手机或者车辆的传感器数据。在该项目中,一个小型嵌入式计算机能读取一系列不同的传感器数据,对数据进行处理,然后将处理后的数据发送到一个 Internet 服务器。服务器进一步对数据进行分析,然后提供给最终用户多种不同的服务。整个系统的框架包括进行传感器数据采集的硬件和软件、在车辆之间数据传递的网络、能够容忍网络连接中断的数据库查询系统、为基于位置的服务设计的隐私协议、车流预测模型系统以及道路表面状况监测系统。

美国政府与工业界也积极参加

到车载物联网的研发中。车辆基础设施集成计划 (Vehicle Infrastructure Integration) 致力于利用无线通信技术使行驶中的车辆更紧密地与周围的环境相联系,从而提高交通系统的安全性。该计划的主要参与者包括美国交通部、加州交通部以及戴姆勒、福特、通用等汽车公司。该计划的参与者在加州 101 公路和密歇根 Novi 市部署了数十个路边基站,用于测试汽车与路边基站的通信能力。在通用公司展示的车载安全系统中,车辆通过 DSRC 无线技术实时监控周围车辆的位置、速度与方向,一旦发生紧急情况,车辆通过声、光信号警告司机。最近,由美国交通部主导的 IntelliDrive 项目<sup>[26]</sup>致力于在个人移动设备(如手机和 PDA)、车辆以及路边基站之间建立安全、灵活的无线通信,使道路交通系统更安全、更智能和更环保。美国交通部目标在 2013 年前对现有的无线通信技术进行测试和评估,以帮助落实未来交通系统的决策与实施。

## 6 结束语

车载物联网是一个具有巨大发展潜力的新兴领域。它能够使人们的日常生活更紧密地与计算机技术和互联网技术相结合,增强交通安全,提高城市交通效率,以及提供各种与位置相关的信息服务。近些年,车载物联网已经得到了学术界、工业界以及政府部门的高度重视,相关的工业、技术标准已提上制订日程。然而,针对不同的应用和不同的环境,仍然有很多尚未妥善解决的问题。人们相信,在车载物联网领域,会看到更多更深入的研究,同时车载物联网技术将能够很快走出实验室,投入实际应用。

## 7 参考文献

- [1] Ford Sync [EB/OL]. [2004-10-27]. <http://www.fordvehicles.com/innovation/sync/>.
- [2] OTT J, KUTSCHER D. Drive-Thru Internet: IEEE 802.11b for "Automobile" Users [C]// Proceedings of the 23rd Annual Joint

- Conference of the IEEE Computer and Communications Societies (INFOCOM '04): Vol 1, Mar 7-11, 2004, Hong Kong, China. Piscataway, NJ, USA: IEEE, 2004: 362-373.
- [3] BYCHKOVSKY V, HULL B, MIU A K, et al. A Measurement Study of Vehicular Internet Access Using in Situ Wi-Fi Networks [C]// Proceedings of the 12th Annual International Conference on Mobile Computing and Communications (MOBICOM '06), Sep 24-29, 2006, Los Alamitos, CA, USA. New York, NY, USA: ACM, 2006: 50-61.
- [4] HADALLER D, KESHAV S, BRECHT T, et al. Vehicular Opportunistic Communication Under the Microscope [C]// Proceedings of the 5th International Conference on Mobile Systems, Applications and Services (MobiSys '07), Jun 11-13, 2007, San Juan, Puerto Rico, USA. New York, NY, USA: ACM, 2007: 206-219.
- [5] ARMSTRONG L. Dedicated Short Range Communications Project [EB/OL]. [2004-10-27]. <http://www.leearmstrong.com/DSRC/DSRCHomeset.htm>.
- [6] IEEE 802.11p. WAVE—Wireless access for the vehicular environment [S]. 2008.
- [7] GM OnStar [EB/OL]. [2004-10-27]. <http://www.onstar.com>.
- [8] WU H, FUJIMOTO R, GUENSLER R, et al. MDDV: A mobility-Centric Data Dissemination Algorithm for Vehicular Networks [C]// Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04), Oct 1, 2004, Philadelphia, PA, USA. New York, NY, USA: ACM, 2004: 47-56.
- [9] ZHAO Jing, CAO Guohong. VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks [C]// Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM '06): Vol 1, Apr 23-29, 2006, Barcelona, Spain. Piscataway, NJ, USA: IEEE, 2006: 289-294.
- [10] RYBICKI J, SCHEUERMANN B, KIESS W, et al. Challenge: Peers on Wheels - A Road to New Traffic Information Systems [C]// Proceedings of the 13th Annual International Conference on Mobile Computing and Networking (MobiCom '07), Sep 9-14, 2007, Montr é al, Canada. New York, NY, USA: ACM, 2007: 215-221.
- [11] SMALL T, HAAS Z J. The Shared Wireless Infostation Model: A New Ad Hoc Networking Paradigm (or Where There is a Whale, There is a Way) [C]// Proceedings of 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '2003), Jun 1-3, 2003, Annapolis, MD, USA. New York, NY, USA: ACM, 2003: 233-244.
- [12] VAHDAT A, BECKER D. Epidemic Routing for Partially-Connected Ad Hoc Networks [R]. Technical Report CS-200006. Durham, NC, USA: Duke University, 2000.
- [13] YUAN Q, CARDEI I, WU J. Predict and Relay: An Efficient Routing in Disruption-Tolerant Networks [C]// Proceedings of the 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '09), May 18-21, 2009, New Orleans, LA, USA. New York, NY, USA: ACM, 2009: 95-104.
- [14] GAO Wei, LI Qinghua, ZHAO Bo, et al. Multicasting in Delay Tolerant Networks: A Social Network Perspective [C]// Proceedings of 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '09), May 18-21, 2009, New Orleans, LA, USA. New York, NY, USA: ACM, 2009: 299-308.
- [15] ZHAO J, ZHANG P, CAO G. On Cooperative Caching in Wireless P2P Networks [C]// Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08), Jun 17-20, 2008, Beijing, China. Piscataway, NJ, USA: IEEE, 2008: 731-739.
- [16] YU Bo, GONG Jiayu, XU Chengzhong. Catch-up: A Data Aggregation Scheme for VANETs [C]// Proceedings of the 5th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '08), Sep 15, 2008, San Francisco, CA, USA. New York, NY, USA: ACM, 2008: 49-57.
- [17] YU Bo, XU Chengzhong. Admission Control for Roadside Unit Access in Intelligent Transportation Systems [C]// Proceedings of 17th IEEE International Workshop on Quality of Service (IWQoS '06), Jul 13-15, 2009, Charleston, SC, USA. Piscataway, NJ, USA: IEEE, 2009: 9p.
- [18] ZHAO J, ARNOLD T, ZHANG Y, et al. Extending Drive-Thru Data Access by Vehicle-to-Vehicle Relay [C]// Proceedings of the 5th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '08), Sep 15, 2008, San Francisco, CA, USA. New York, NY, USA: ACM, 2008: 66-75.
- [19] CHANG Chungju, CHENG Rayguang, SHIH Haotang, et al. Maximum Freedom Last Scheduling Algorithm for Downlinks of DSRC Networks [J]. IEEE Transactions on Intelligent Transportation Systems, 2007, 8 (2): 223-232.
- [20] ZHANG Yang, ZHAO Jing, CAO Guohong. On Scheduling Vehicle-Roadside Data Access [C]// Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc

Networks (VANET '07), Sep 10, 2007, Montreal, Canada. New York, NY, USA: ACM, 2007: 9-18.

- [21] LOCHERT C, SCHEUERMANN B, WEWETZER C, et al. Data Aggregation and Roadside Unit Placement for a VANET Traffic Information System [C]// Proceedings of the 5th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '08), Sep 15, 2008, San Francisco, CA, USA. New York, NY, USA: ACM, 2008: 58-65.
- [22] FleetNet [EB/OL]. [2004-10-27]. <http://www.nw.neclab.eu/Projects/fleetnet.htm>.
- [23] CarTalk [EB/OL]. [2004-10-27]. <http://www.cartalk2000.net/>.
- [24] California Path [EB/OL]. [2004-10-27]. <http://www.path.berkeley.edu/>.
- [25] MIT CarTel [EB/OL]. [2004-10-27]. <http://cartel.csail.mit.edu/doku.php>.
- [26] IntelliDrive [EB/OL]. [2004-10-27]. <http://www.intelldrivewayusa.org>.

收稿日期: 2010-11-09

## 作者简介



俞波, 美国韦恩州立大学博士后; 研究方向为车载物联网、无线传感器网络、移动自组织网络; 已发表论文 12 篇。



须成忠, 美国韦恩州立大学电子与计算机工程系教授、互联网与云计算实验室主任、SUN 公司韦恩州立大学开源计算与应用中心主任、上海交通大学和北京邮电大学的客座教授; 研究领域为并行分布计算、无线嵌入式系统; 已出版专著 2 部, 发表论文 160 篇。



过敬意, 日本筑波大学计算机科学博士毕业; 曾任日本会津大学教授和系主任, 现任上海交通大学计算机科学与工程系主任, 上海交通大学特聘教授, 华中科技大学、中南大学、南京大学、四川大学客座教授。

## 广告索引

A1-A5、封四: 中兴通讯股份有限公司



# IoT 的数据管理与智能处理

## Data Management and Intelligent Processing in IoT

中图分类号: TN91 文献标志码: A 文章编号: 1009-6868 (2011) 01-0038-04

**摘要:** 在物联网(IoT)中物与物、人与物的智能交互的实现要依赖于数据的智能处理,而数据管理则是数据智能处理的基础。由于物联网中的数据具有异构、海量和不确定等特点,因此要实现对其数据管理与智能处理,必须在运用已有技术的基础上进一步采用新的技术和方法。文章基于物联网中数据的特点、物联网新的数据管理与智能处理技术,提出了数据空间技术、不确定数据推理技术以及云计算在物联网中的应用思路,揭示了需要研究的关键内容。

**关键词:** 物联网; 数据管理; 智能处理; 数据空间; 云计算

**Abstract:** Thing-thing and human-thing interaction in IoT should be dependent on intelligent data processing based on data management. Since IoT data is heterogeneous, mass-scale, and somewhat unpredictable, using new methods and technologies in conjunction with existing technologies is necessary for data management and processing. In this paper, the characteristics of IoT are analyzed, and several new data management and intelligent processing technologies are introduced. Dataspace technology, uncertain data reasoning technology, and cloud computing technology in IoT are proposed and areas of further research are outlined.

**Key words:** Internet of things; data management; intelligent processing; data space; cloud computing

李玲娟/LI Lingjuan

(南京邮电大学 计算机学院, 江苏 南京 210003)  
(College of Computers, Nanjing University of  
Posts and Telecommunications, Nanjing,  
210003, China)

数据分布、数据路由策略的研究,数据库中的数据管理技术侧重于数据模型、存储方式、索引策略和查询实现的研究,智能控制中的数据处理侧重于数据融合、特征提取和实时响应等。物联网中的数据智能处理技术不仅涵盖了这些数据处理方式,同时具有自己的特点。因此,要实现物联网的数据管理与智能处理,必须在合理运用已有技术的基础上引入新的技术和方法。

### 1 物联网中数据的特点

物联网中数据的特点主要表现在以下几个方面:

#### (1) 异构性

在物联网中,不仅不同的对象会有不同类型的表征数据,同一个对象也会有各种不同格式的表征数据。比如在物联网中为了实现对一栋写字楼的智能感知,需要处理各种不同类型的数据,如探测器传来的各种高维观测数据,专业管理机构提供的关系数据库中的关系记录,互联网上提供的相关超文本链接标记语言(HTML)、可扩展标记语言(XML)、文本数据等。为了实现完整准确的感知,必须综合利用这些不同类型的数据来全面地获得信息,这也是提供有效的信息服务的基础。

物联网(IoT)是通过射频标签(RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络。它是继计算机、互联网与移动通信网之后的又一次信息产业浪潮。

物联网通过标识、感知、处理和信息传送4个关键环节,将整个世界无缝地连接在一起,智能地感知、推理和分析。

物联网具备3个特征,一是全面

感知,即利用RFID、传感器、二维码等随时随地获取物体的信息;二是可靠传递,通过各种电信网络与互联网的融合,将物体的信息实时准确地传递出去;三是智能处理,利用云计算、模糊识别等各种智能计算技术,对海量数据和信息进行分析 and 处理,对物体实施智能化的控制。

物联网要实现人与物、物与物的智慧对话,必须对数据进行管理和智能处理,主要包括数据的采集、存储、查询、分析(融合与挖掘)等关键环节。这些数据智能处理技术已渗透在信号处理、传感网、数据库、信息检索技术、智能控制等领域。这些不同的领域都侧重于数据处理的不同方面:传感网研究中侧重于网络节点上

基金项目:国家重点基础研究发展(“973”)规划(2011CB302903)



### (2)海量性

物联网是一个网络的海洋,更是一个数据的海洋。在物联网中,世界中的各个对象都连接在一起,每个对象都可能在变化,表达其特征的数据在不断地积累。如何有效地改进已有的技术和方法或提出新的技术和方法来高效地管理和处理这些海量数据将是从事数据中提取信息并进一步融合、推理和决策的关键。

### (3)不确定性

物联网中的数据具有明显的不确定性特征,主要包括数据本身的不确定性、语义匹配的不确定性和查询分析的不确定性等。为了获得客观对象的准确信息,需要去粗取精、去伪存真,以便人们更全面地进行表达和推理。

## 2 物联网涉及的技术

由于物联网是一个综合了已有技术并具有自己特色的新兴的产业,因此到目前为止,尚无能适应上述物联网数据特点的系统化研究结果面世,但是一些思想和已有的技术是可以借鉴的。

除了传统的数据库技术之外,近年来兴起的数据空间技术、云计算数据管理技术、数据挖掘与融合技术、不确定性数据管理技术、语义Web技术等都可物联网所用。

### 2.1 数据空间技术

数据空间是近几年提出的数据管理新技术。按照文献[1]和文献[2]的描述,数据空间是与主体相关的数据及其联系的集合,其中的所有数据对主体来说都是可控的。主体相关性和可控性是数据空间数据项的基本属性。文献[3]指出数据空间有3个基本要素:主体、数据集和服务,其中主体是指数据空间的所有者;数据集是与主体相关的所有可控数据的集合,包括对象和对象之间的关系;主体通过服务对数据空间进行管理和使用,服务包括分类、查询、更新、

索引等。可以说一个数据空间应该包含与某个组织或个体相关的一切信息,无论这些信息是以何种形式存储、存放于何处。数据空间技术包括信息抽取、分类、模式匹配、数据模型、数据集成与更新、数据查询、存储索引、数据演化等多个方面。

提出数据空间的初始目标是解决Web应用中多源、异构、海量数据的管理和使用问题。典型的例子是通过构造个人数据空间,用户可以实现复杂的语义查询,实现随时随地对个人数据的快速访问,可以方便地备份个人重要数据,保持异地数据同步。通过构造群组数据空间,群组成员之间可以方便地进行信息的共享与交流。

### 2.2 云计算技术

云计算是并行计算、分布式计算和网格计算的发展,或者说是这些计算机科学概念的商业实现<sup>[4]</sup>。

作为一种以数据为中心的密集型的超级计算技术,云计算的技术特点如下:

#### (1)海量分布式存储

云计算采用分布式存储的方式来存储数据,采用冗余存储的方式来保证存储数据的可靠性以高可靠软件来弥补硬件的不可靠,从而提供廉价可靠的系统。

#### (2)并行编程模式

为了高效地利用云计算的资源,云计算采用MapReduce编程模式,将任务自动分成多个子任务,通过映射(Map)和化简(Reduce)两步实现任务在大规模计算节点中的调度与分配。后台复杂的并行执行和任务调度对用户和编程人员透明。

#### (3)数据管理

云计算系统对大数据集进行处理、分析,向用户提供高效的服务,数据管理技术必须能够高效地管理大数据集。

基于以上技术,云计算使得云用户不需要了解“云”的技术构架和专

业知识就可以轻松便捷地完成应用的部署或迁移,只需要联网便可以在网络上实现各种应用,甚至包括完成超级计算任务。与传统应用模式相比,云计算具有超大规模、虚拟化、可靠性强、通用、高度可扩展、按需服务等特点<sup>[5]</sup>。

目前提供的云计算服务形式有:软件即服务(SAAS)、实用计算、网络服务、管理服务提供商(MSP)、商业服务平台、互联网整合等。

### 2.3 数据挖掘与融合技术

数据挖掘是从大量的数据中提取潜在的、事先未知的、有用的、能被理解的模式的高级处理过程。被挖掘的数据可以是结构化的关系数据库中的数据,半结构化的文本、图形和图像数据,或者是分布式的异构数据。数据挖掘是决策支持和过程控制的重要技术支撑手段。

数据融合<sup>[6-7]</sup>是一个多级,多层次的数据处理过程,主要完成对来自多个信息源的数据的自动检测、关联、估计及组合等的处理,是基于多信息源数据的综合、分析、判断和决策的新技术。数据融合有数据级融合、特征级融合、决策级融合,其中:

(1)数据级融合直接在采集到的原始数据上进行融合,是最低层次的融合,它直接融合现场数据,失真度小,提供的信息比较全面。

(2)特征级融合先对来自传感器的原始信息进行特征提取,然后对特征信息进行综合分析和处理,这一级的融合可实现信息压缩,有利于实时处理,它属于中间层次的融合。

(3)决策级融合在高层次上进行,根据一定的准则和决策的可信度做最优决策,以达到良好的实时性和容错性。

数据挖掘与数据融合是两种功能不同的数据处理过程,前者发现模式,后者使用模式。两者的目标、原理和所用的技术各不相同,但功能上相互补充,将两者集成可以达到更好

的多源异构信息处理效果。

#### 2.4 不确定性数据管理技术

在经济、军事、物流、金融、电信等领域,数据的不确定性普遍存在。不确定性数据的产生原因比较复杂。文献[8]将之概括为5个方面:

(1)原始数据不准确。这是产生不确定性数据最直接的因素。比如:数据的准确度会受仪器的精度、传输过程中网络的带宽、传输延时、能量等因素影响;在传感器网络与RFID等应用中,原始数据的准确度会受周围环境的影响。

(2)从粗粒度数据集合转换到细粒度数据集合的过程可能会引入不确定性。

(3)出于隐私保护等特殊目的,某些应用无法获取原始的精确数据,而仅能得到变换之后的不精确数据。

(4)装备故障、无法获取信息、与其他字段不一致、历史原因等都可能产生缺失值。

(5)不同数据源的数据信息可能存在不一致,在数据集成过程中就会引入不确定性。

不确定性数据的表现形式多种多样,它们可以以关系型数据、半结构化数据、流数据或移动对象数据等形式出现。

目前国际上的一些大学和科研机构已在不确定数据的数据模型、数据预处理与集成、存储与索引、查询处理、管理系统等方面做了有益的研究工作<sup>[9-11]</sup>。

### 3 物联网数据管理与智能处理思路

为了实现物联网中海量数据的高效处理,无缝地融合各种异构数据,最终为物联网中的决策与控制服务提供支撑,本文提出一种综合运用以上技术来解决物联网的数据管理与智能处理问题的思路:以云计算平台为数据管理平台;以数据空间来逻辑组织主体的数据和服务;在此基础

上以数据挖掘和数据融合相集成的方式实现多层次、多粒度、跨领域的数据处理;同时,以不确定的方式对数据及其上的服务进行表达和推理,从而实现对多元世界的准确刻画。

由于物联网中的数据具有多源、异构、海量的特点,做出一个决策可能要使用原始感知数据、融合过的数据、领域数据。这些数据经常具有不同类型,比如字符型等常规数据、时间数据、空间数据、知识等,而且这些数据所表征的事物可能是同领域的,也可能是跨领域的,但他们之间通常具有内在的联系。数据空间的初始目标就是解决Web应用中多源、异构、海量数据的管理和使用问题。因此,在数据空间的概念下组织、管理和使用物联网数据是可行而有效的途径,也符合物联网自身的可扩展性特点。

基于云计算平台来实施物联网数据的管理可以充分利用云计算平台的可靠、安全的数据存储中心和严格的权限管理策略,以及云计算中心对接入网络的终端的普适性,有利于解决物联网的机器对机器通信(M2M)应用的广泛性,并可与运营商合作,避免重复投资。同时借鉴云计算数据管理技术,设计海量数据处理的体系结构,能突破吞吐量“瓶颈”,实现实时或准实时的数据查询和深层次的数据分析。

在物联网中通常要综合利用各种异构的数据源来实现智慧感知。数据源本身的不确定性不可避免地带来物联网数据空间的不确定性,主要包括数据本身的不确定性、语义映射的不确定性和查询分析的不确定性等,有必要利用不确定性技术来对物联网的数据进行管理。采用不确定性理论对数据本身、语义映射和查询服务进行表达,并据此推理,能够更好地描述可能的物联网世界,符合物联网数据不确定和动态演化的特点,能帮助人们实现不确定条件下的情景感知和决策。

解决物联网数据管理与智能处理的关键研究内容包括:

#### 3.1 物联网数据的管理

针对物联网的数据管理需要研究以下内容:

##### (1)数据空间中采用的数据模型

需要合理地定义物联网数据空间的要素,研究出更为灵活的模型来表达数据空间数据及其关联关系的方法,研究由数据获取模式的方法、模式演化的维护等。

##### (2)不同粒度主体对数据的提取

需要针对物联网数据空间的3个不同的数据融合层次,研究融合感知数据提取实体数据、融合实体数据提取决策数据、3个层次间的相互融合关系。

##### (3)数据的存储方式

由于物联网数据空间中数据模式频繁变化,主体对应的数据多样,需要研究合理的存储策略及其在云计算平台的分布策略。

##### (4)数据的索引策略

数据空间是介于模式固定的数据管理方式和松散的搜索引擎间的一种更为灵活的数据管理方式,其索引不仅要充分利用结构特征也要利用内容特征,比如关键字等。需要全面研究物联网数据的结构索引策略、内容索引策略、结构和内容相结合的索引策略。

#### 3.2 物联网数据的智能处理

数据处理是受服务驱动的,物联网的服务包括:分析、决策与控制。为了实现这些服务,在数据层面,需要进行一系列的数据处理工作。针对物联网数据的智能处理,需要研究以下内容:

##### (1)以融合和决策为目的海量数据的实时挖掘

基于物联网服务的需求,物联网中的数据挖掘应分为两个方面:辅助常规决策的数据挖掘和辅助数据融合的数据挖掘。

鉴于物联网数据的异构、海量、分布性和决策控制的实时性,需要研究数据挖掘引擎的布局及多引擎的调度策略;需要研究时空数据的实时挖掘方案,海量数据的实时挖掘方法,不确定知识条件下的实时挖掘算法,数据挖掘算法的综合运用、改进和新算法,低时空复杂度算法;需要考虑物联网隐私的重要性,需要研究隐私保护的数据挖掘方法。

(2)以情境感知为目的的不确定性建模和推理

针对数据本身的不确定性,需要研究感知数据本身的不确定性表达和推理、实体数据的不确定性表达和推理以及决策数据的不确定性表达和推理。

针对语义映射的不确定性,需要研究融合感知数据获取实体数据过程中的不确定性表达和推理、融合实体数据获得决策数据过程中不确定性表达和推理。

针对查询分析的不确定性,需要研究物联网高维数据在松散模式下查询的不确定性表达、查询结果的不确定性表达和推理、联机分析处理(OLAP)和数据挖掘如何从不确定性数据中获得合理结果等内容。

### (3)物联网与云计算的结合

本文希望实现数据空间概念下的基于云计算平台的物联网数据管理和智能处理。针对物联网与云计

算的结合,需要研究符合物联网数据海量和负载动态变化特点的云计算平台构建方法。除了设计数据的存储之外,需要研究每个主体的分析与挖掘服务如何通过云计算的批处理任务实现,如何实现任务调度引擎,如何实现在线的监测和查询服务。各项研究应以达到物联网实时或准实时的处理要求为目标。

## 4 结束语

数据管理与智能处理是物联网必须解决的关键问题,鉴于物联网数据的多源、异构、海量、动态等特点以及物联网的可扩展性,本文提出了一种综合运用先进的数据空间技术、不确定数据管理技术、云计算技术解决这一问题的思路,也给出了在此思路下需要研究的关键内容。

随着物联网产业发展步伐的加快,以上内容有很大的研究空间,有效的研究成果将对物联网的实用化起到很好的技术支撑作用。

## 5 参考文献

- [1] FRANKLIN M, HALEVY A, MAIER D. From Databases to Dataspace: A New Abstraction for Information Management [J]. SIGMOD Record, 2005,34(4):27-33.
- [2] JONES W, BRUCE H. A Report on the NSF-Sponsored Workshop on Personal Information Management [C]//An NSF Sponsored Invitational Workshop of Personal Information Management (NSF PIM Workshop), Jan 27-29, 2005, Seattle WA, USA.2005.

- [3] 李玉坤, 孟小峰, 张相於. 数据空间技术研究 [J]. 软件学报, 2008,19(8):2018-2031.
- [4] 邓倩妮, 陈全. 云计算及其关键技术 [J]. 高性能计算发展与应用, 2009,26(1):2-6.
- [5] LIU Peng, SHI Yao, LI Sanli. Computing Pool—A Simplified and Practical Computational Grid Model [C]//Proceedings of the 2nd International Workshop on Grid and Cooperative (GCC'03), Dec 7-10, 2003, Shanghai, China. LNCS 3032. Berlin, Germany: Springer-Verlag, 2004: 661-668.
- [6] LI Tongying, FEI Minrui. Information Fusion in Wireless Sensor Network based on Rough Set [C]//Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC'09), Nov 6-8, 2009, Beijing, China. Piscataway, NJ, USA: IEEE, 2009:129-134.
- [7] 张西川, 张平定, 杨丽娜. 数据挖掘与数据融合相结合的异类信息融合 [J]. 指挥控制与仿真, 2008,30(3): 42-44.
- [8] 周傲英, 金澈清, 王国仁, 等. 不确定性数据管理技术研究综述 [J]. 计算机学报, 2009,32(1): 1-16.
- [9] ORION DBMS: Handling Nebulous Data [EB/OL]. [2010-03-15]. <http://orion.cs.purdue.edu/>.
- [10] Trio: A system for Integrated Management of Data, Uncertainty, and Lineage[EB/OL]. [2010-03-15]. <http://infolab.stanford.edu/trio/>.
- [11] 康奈尔大学 MayBMS 项目 [EB/OL]. [2010-03-15]. <http://www.cs.cornell.edu/database/maybms/>.

收稿日期: 2010-11-08

### 作者简介



李玲娟, 南京邮电大学计算机学院教授、博士; 主要研究领域为数据库技术、数据挖掘、分布式计算、信息安全等; 主持和参与基金项目 10 项; 已发表论文 30 篇, 其中被 SCI/EI 核心检索 4 篇。

## 综合信息

### 中兴通讯已拥有 235 项 LTE 基本专利

【本刊讯】2011 年 1 月 12 日, 中兴通讯宣布, 中兴通讯已经拥有 235 件 LTE 标准必须使用的基本专利(简称 EP), 这些专利已经在欧洲电信标准组织(ETSI)进行申请。截至 2010 年 11 月 30 日, 已有包括所有全球主要通信设备商在内的 34 家公司发布了约 3 413 件 LTE 标准必须使用的基本专利, 其中, 中兴通讯拥有 EP 的占比约 7%, 在所有设备商中排名第 5, 且与前几名设备商差距微小。

LTE 及其演进技术已被业界公认为无线宽带主流技术, 从 2004 年开始, 中兴通讯开始着力于 LTE 标准关键技术及其基本专利的研发工作。截至 2010 年底, 中兴通讯已经投入超过 4 000 人进行 LTE 研发, 向 3GPP 提交了 6 800 篇提案, 其中 LTE/SAE 相关提案超过 3 900 篇, 申请 LTE 相关专利 2 900 件。

中兴通讯表示未来将投入更大资源致力于 4G 标准技术研究 with 标准起草工作, 目标是在 2012 年拥有 LTE 的 EP 至少达到 10%。



# 向未来互联网演进

## Evolving Towards the Future Internet

中图分类号: TP393 文献标志码: A 文章编号: 1009-6868 (2011) 01-0042-03

**摘要:** 随着互联网用户的不断增长、网络应用的日趋丰富、技术水平的持续提高,未来互联网发展的焦点已经不再单纯是简单的接入,而是在此之上的多层次的、具有高可扩展性的增值服务。文章在分析了向未来互联网演进4个不同阶段所面临的重大挑战后,提出目前下一代互联网中重要的IPv6技术已经难以胜任向未来互联网演进的需要。文章强调未来互联网虽然存在着多个研究方向和热点,但在一些基本问题上缺乏共识,因此对于未来互联网的研究需要从更基础的起点出发。

**关键词:** 未来互联网; 网络体系结构; 下一代互联网(NGI); IPv6

**Abstract:** With an abundance of network applications and sustained improvements in technology, Internet development must be focused not only on simple access but also on multilevel and highly scalable value added services. This paper analyzes challenges in the four different stages of evolution to future Internet and suggests IPv6 is not satisfactory for the future Internet. Many avenues of research are being explored for future Internet, but there is still a lack of consensus on basic issues. More research is required into the fundamentals of the future Internet.

**Key words:** future Internet; network architecture; Next Generation Internet (NGI); IPv6

何宝宏/HE Baohong

(工业和信息化部电信研究院 互联网中心,  
北京 100191)  
(The Internet Center, China Academy of  
Telecommunication Research of MIIT, Beijing  
100191, China)

- 互联网自身多个方面都面临着诸多相互关联的关键问题需要研究和解决
- IPv6沿用了IPv4的体系架构,是改良型技术路线的代表
- 未来互联网能否成功依然面临诸多挑战

### 1 “未来”互联网的演变

互联网自诞生以来,其终端、承载网络和应用等都已发生了翻天覆地的变化,但仍然有一个几乎不变的话题:互联网的“未来”在哪里?在互联网的历史发展阶段中,“未来”不断成为“历史”,同时又产生新“未来”和新问题。互联网不同的发展阶段,面临的问题和解决手段也有所不同,大致可以划分为4个阶段<sup>[1-3]</sup>。

(1) 理论准备阶段(20世纪60年代)。互联网采用的核心技术是包交换技术,这一时期业界讨论的焦点是包交换技术是否具有“未来”。20世纪60年代初,Paul Baran等人发表论文<sup>[4]</sup>,提出组建基于包交换技术的网络,在技术上是完全可行的。但由于

当时占主流的电路交换技术所带来的强大商业利益和政治影响力,以及计算机技术和数字化技术仍处于发展初期等原因,直接导致当时一些大牌计算机公司和电信公司,总体上都质疑甚至反对包交换技术,认为它没有“未来”。这一时期的典型特征是学术界奠定了互联网技术的理论基础,但产业界主流观点尚未接受,互联网的“未来”还只停留在纸面上。

(2) 实验阶段(1969—1993年)。仅有建立互联网的理论是远远不够的,还需要通过试验来验证组建的可行性,证明在现实中互联网是有“未来”的。1969年阿帕网的诞生表明从工程技术上讲,组建包交换的网络用于连接计算机是完全可行的。1983年传输控制协议/网际互联协议(TCP/IP)

IP)在互联网上的成功应用表明,业界已经找到了这样一种异构网络、大规模互联的技术。这一时期的典型特征有两个:包括IP在内的各种包交换技术,工程上已经证明是完全可行的;以电信业为主体支持的X.25和异步转移模式(ATM)等包交换技术,与以计算机业为主体支持的TCP/IP和以太网技术,展开了激烈的竞赛。

(3) 应用阶段(1994—2001年)。这一时期随着Tim Berners-Lee<sup>[4]</sup>在互联网上发明了万维网这样的“杀手级”应用,TCP/IP技术战胜ATM等技术成为最大的赢家,IP化成为潮流。互联网这一时期面临的最重要挑战已不再是证明自身技术的可行性和稳定性,而是考虑统一后如何建设一个新世界。因此互联网“未来”的主

要矛盾开始从“外部”转向“内部”，即自身的发展问题。IPv4 地址(尤其是 B 类地址)即将耗尽和路由表的不断膨胀，是自 90 年代以来互联网面向“未来”的核心问题。互联网工程任务组(IETF)提出发展下一代互联网(NGI)的建议，并且给出权威答案——IPv6。从这时起业界普遍认为，互联网的“未来”在于用 IPv6 替代 IPv4。

(4) 发展阶段(2001 年至今)。随着互联网社会化应用的不断发展，尤其是应用目的从教育科研的“公益”转向以盈利为目的的“商用”，用户群体从“自律”的科研人员转向普通大众，应用环境从数据为主转向话音和视频，接入方式从固定转向移动，终端从计算机转向手机。互联网自身从资源、网络到应用，从管理、安全到政策等，都面临着诸多相互关联的关键问题需要研究和解决。越来越多的人认为 IPv6 难以满足这些未来发展的需要，业界呼唤更先进、更强大的“未来”互联网。为了区别于 IPv6 为代表的“下一代互联网”，“未来互联网”在 2005 年前后开始出现<sup>[5-7]</sup>。

## 2 IPv6 的局限性

关于 IPv6 和下一代互联网的关系，目前的主流观点认为“IPv6 是下一代互联网技术的核心”，或者“基于 IPv6 的下一代互联网”，但总体来看，IPv6 在下一代互联网中的地位随着时间的推移被不断弱化。

IPv6 的设计始于大约 20 年前。上世纪 90 年代初，IETF 提出做下一代 IP(IPng)的直接原因：IPv4 地址即将耗尽(尤其是 B 类地址)及路由表的快速膨胀。这两者的出现将直接导致互联网无法持续发展。为此，1993 年在 RFC1550<sup>[8]</sup>中提出了征求新 IP 协议的呼吁，以替代当时已经使用了 10 年的 IPv4 协议，并公布了新协议需实现的主要目标。

在 RFC1550 中提出的下一代互联网协议的主要目标包括：“支持几乎无限大的地址空间”、“减小路由表的

大小”、“简化协议提高使路由器的性能”、“实现 IP 级的安全”、“支持实时业务”、“支持组播”、“Mobile IP 的支持”、“允许新旧协议共存一段时间”等。这些目标中潜在的矛盾是不可避免的，因此具有不同的实现优先级。编址相关问题(含路由)最为突出，因此它自然而然地成为最高优先级的问题。

后来 IETF 得到了多个 IPng 提案，并取长补短，于 1998 年融合成了现在的 IPv6 协议。很明显，最后正式批准通过的 IPv6 技术<sup>[9]</sup>，以地址空间的加长为 128 bit 为核心思想，部分满足了 RFC1550 提出的主要需求。直至今日虽然基本的 IPv6 地址长度、包头、路由和安全等机制已经确定和稳定，但一些所谓的“高级”特点仍在不断地发展完善中。

IPv6 所针对的需求是在 20 年前提出的，当时的互联网还没有商用，安全问题不突出，移动互联网、三网融合甚至物联网的概念也还没出现。因此 IPv6 沿用了当时看来非常完美的 IPv4 互联网体系架构(端到端透明)，而且主要针对的是地址短缺和路由扩展性等编址问题。现在看来，不仅是 IPv6 技术需要不断前进，当时 RFC1550 提出的对下一代互联网的需求也应该与时俱进。时代呼唤“未来互联网”。

## 3 未来互联网的研究

未来互联网/网络存在着多个研究方向和热点，如虚拟化网络、自动网络、层次交换网络、高性能网络、安全可信网络、长距低功耗网络及高带宽长延时网络等。针对这些重要方向，目前各国都在积极制订政策，并投入大量的资金开展研究，力求在下一代互联网的研究方面取得先机。其中比较典型的研究项目有美国的 PlantLab<sup>[9]</sup>、欧盟的 FP7/4WARD<sup>[6]</sup>、日本的 AKARI<sup>[7]</sup>以及中国自主研究的公共电信数据网络(PTDN)<sup>[10]</sup>等。

除了以上一些国家层面的研究

活动，ITU、IETF、国际标准化组织(ISO)和万维网联盟(W3C)等多个标准化组织，也都在进行未来互联网/网络的标准化制订工作。ITU 的工作方向侧重于“革命”思路，第十三研究组(SG 13)一直是未来网络的领导研究小组。该小组专门成立了未来网络焦点组，对未来网络的愿景、需求、新技术、时间表以及标准化等问题进行探讨。目前该小组的主要工作还停留在对未来网络的设计原则、概念、需求以及技术特征等的收集上，距离达成共识尚很遥远。IETF 一直在做“改良”互联网的标准化工作：推出了下一代地址协议 IPv6，以解决地址扩展性问题；研究下一代路由寻址架构以解决路由扩展性问题，目前已经出现了 ID/Locator(身份地址分离)和 Map/Encaps(映射封装)两种主要思路；研究能提供点对点(P2P)分布式域名服务的下一代域名系统(DNS)，以解决其过载及安全问题；研究基于多路径的下一代 TCP 协议以获得更高的网络吞吐量等等。W3C 则对语义网的原则和协议的制订担负着领导角色。基于语义的体系结构从底往上共有 7 层：编码定位层、XML 结构层、资源描述层、本体层、逻辑层、证明层和信任层。基于下面 4 层的主要标准规范已经发布，目前 W3C 的主要工作是继续研究建立在资源描述框架(RDF)之上的新工具和新语言，开发新的应用。此外，ISO 也刚启动了未来网络体系架构的研究和标准化工作。

## 4 向未来互联网的演进路线

向未来互联网的演进，已经成为全球的共识。但对于如何向下一代互联网(包括下一代 IP 技术)演进，目前出现了大致两种技术路线：“改良型”和“革命型”。

(1) 改良型演进的技术路线主张在现有互联网网络体系下进行修补，对网络设备或拓扑进行改造，使其适应新的需求。典型的改良型技术有：

针对互联网的地址扩展性的 IPv6、路由扩展性的标识/位置分离、服务质量的差分服务、网络安全性的 IPSec、名字服务的 DNSSec 以及移动性的移动 IP 等。

(2) 革命型演进的技术路线主张抛弃现有互联网网络体系,建立全新的网络架构,从根本上解决原有体系结构存在的问题。近年来,互联网发达国家以及国际标准组织都加强了对未来网络体系结构的研究,主要包括:美国的 PlanetLab、GENI、FIND 和 FARA,欧盟 FP7 的 4WARD,日本的 AKARI,ITU 的 Future Network 等计划。

改良型路线的支持者认为:对一个存量巨大的互联网进行颠覆性改造,重新建设新网络、应用和内容,甚至培养用户新的使用习惯,无论是时间成本还是经济成本都是巨大的;而革命型路线的支持者认为:采用渐进修补策略,如使用网络地址翻译(NAT)、多协议标记交换(MPLS)、IPv4 和 IPv6 互通等技术,会使得原本简洁的网络结构变得日益复杂(截至 2010 年 10 月 IETF 发布的 RFC 已超过 6 000 个)。另外,有些“补丁”的实施又相互钳制,使得增加新的修补措施变得越来越困难。

改良型与革命型技术路线的主要区别在于是否沿用现有的互联网体系结构。可以认为:IPv6 沿用了 IPv4 的体系架构,是改良型技术路线的代表。但令人遗憾的是,革命性技术路线的互联网体系架构,至今也没有出现业界普遍认可的基本思路。

## 5 未来互联网面临的挑战

虽然关于未来互联网的研究和标准化工作,多个国家和标准化组织已经展开,然而未来互联网能否成功依然面临着诸多挑战和问题。

首先,标准化工作难以协调和统一。各个标准化组织工作各自为政,彼此之间缺乏共识。譬如,ITU 热衷于“革命”思路,致力于推出一个全新的网络体系架构标准;而 IETF 更加

“现实”,倾向于在互联网现有体系架构下进行改良,针对已出现的问题推出新的 RFC,不考虑太长远的事情,不考虑互联网的新型架构。

其次,对体系架构的理解不同。体系架构是描述网络中不同的组成部分,以及这些部分如何关联起来,它是所有新网络设计的基础性工作。对未来互联网体系架构的理解不同,直接导致了“鸡和鸭讲”的问题。例如,W3C 认为语义网就是下一代互联网,更多地从应用层来理解网络体系架构;而 ITU 等其他组织和机构则更多地从承载网层面来理解;IETF 试图不对现有互联网的体系架构做任何改动,因此仍围绕 IPv6 做文章。随着云计算的兴起,一些人认为云计算就代表着未来互联网的发展趋势和架构。

第三,对于未来互联网如何继承现有技术的问题,各方态度不一。IETF 已经承认,他们在 IPv6 标准上犯下了一个致命错误,就是没有提供对现有互联网协议 IPv4 的向下兼容性;而 ITU 则认为,在以开发性的思路设计未来网络体系架构时,也许不需要考虑和现有网络的兼容性。未来的网络体系架构要不要汲取 IPv6 的教训,兼容现有的 IPv4 和 IPv6 网络,该问题到目前为止依然没有达成共识。

最后,没有考虑外部环境的巨大变化<sup>[11]</sup>。互联网向“未来”的发展演进,其实也是互联网不断“复杂化”的一个过程。维持互联网这样一个复杂系统正常运转,最需要的是外部的“能源供给”:廉价的电力资源和取之不竭的计算资源。

## 6 结束语

从理论准备阶段开始,在互联网近 50 年的发展历史中,对向未来互联网演进的问题上,一直以来争议不断。当 IP 一统天下后,业界焦点开始转移到 IP 自身问题上来。IPv6 是在大约 20 年前提出的,因此设计中存在重大缺陷、在下一代互联网中的

地位随着时间的推移被不断弱化在所难免。

5 年多来,虽然对未来互联网的研究有多个方向和热点<sup>[12]</sup>,但即使是在最基本问题(如网络架构、层次模型等)上都还缺乏共识(当然也有利益之争)。对于未来互联网的研究,目前还过多地拘泥于现有互联网的一些基本思路,缺乏大视野导致缺乏大创新、大突破。对于未来互联网的研究,需要走出现有互联网巨大成功带来的路径依赖“阴影”,从更基础的起点出发。

## 7 参考文献

- [1] 何宝宏,于群. 40 年网络技术发展历程[J]. 中兴通讯技术,2010,16(Z1):17-20.
- [2] 信息产业部电信研究院. 互联网技术发展白皮书 第一卷 发展脉络与体系架构[J]. 世界电信,2007,20(7):8-13.
- [3] BARAN P. On Distributed Communications Series[EB/OL]. <http://www.rand.org/about/history/baran.list.html>.
- [4] Tim\_Berners-Lee[EB/OL]. [http://en.wikipedia.org/wiki/Tim\\_Berners-Lee](http://en.wikipedia.org/wiki/Tim_Berners-Lee).
- [5] PlanetLab [EB/OL]. <http://www.planet-lab.org/>.
- [6] The FP7 4WARD Project: Overview[EB/OL]. (2008-12). <http://www.4ward-project.eu/index.php?s=overview>.
- [7] AKARI [EB/OL]. <http://akari-project.nict.go.jp/>.
- [8] BRADNER S, MANKIN A. IP: Next Generation (IPng) White Paper Solicitation[R]. IETF RFC1550.1993.
- [9] DEERING S, HINDEN R. Internet Protocol, Version 6 (IPv6) Specification[R]. IETF RFC2460.1998.
- [10] ITU-T Y.2613. The General Technical Architecture for PTDS[IS].2010.
- [11] 何宝宏. 2020 年前后将发生互联网革命[J]. 电信网技术,2010 (3):30-31.
- [12] NSF Announces Future Internet Architecture Awards[EB/OL]. (2010-08-27). [www.nsf.gov/news/news\\_summ.jsp?cntn\\_id=117611](http://www.nsf.gov/news/news_summ.jsp?cntn_id=117611).

收稿日期:2010-11-23

### 作者简介



何宝宏,工业和信息化部电信研究院互联网研究领域主席、通信标准研究所互联网中心主任、中国通信标准化协会 IP 与多媒体工作委员会副主席、ITU-T Q24/16 报告人;长期从事互联网技术、标准、产业和政策等研究;已主导完成国际标准 10 余项,发表文章 60 余篇。



# 分布式智能开放运营架构及关键技术

## Architecture and Key Technology of Distributed Intelligent Open Systems

**摘要:**随着电信运营商 3G 网络的部署、网络带宽的提速以及互联网应用高速发展的冲击,电信运营商面临前所未有的压力。运营商需要发挥网络和客户优势,转向对业务、平台、客户、界面等商业资源运营,并且整合网络与客户资源,创造新的商业模式。文章首先给出了电信行业面临的新威胁与挑战,分析电信运营商转型的优势、运营和商业模式转型的方法,提出分布式智能开放系统(DIOS),重点讨论了系统架构和关键技术。

**关键词:**DIOS; 公众计算通信网(PCCN); 云计算

**Abstract:** High-speed large-bandwidth networks and growth in rich Internet applications has brought unprecedented pressure to bear on telecom operators. Consequently, operators need to play to the advantages of their networks, make good use of their large customer bases, and expand their business resources in service, platform, and interface. Network and customer resources should be integrated in order to create new business ecosystems. This paper describes new threats and challenges facing telecom operators and analyzes how leading operators are handling transformation in terms of operations and business model. A new concept called Distributed Intelligent Open System (DIOS)—a public computing communication network—is proposed. The architecture and key technologies of DIOS is discussed in detail.

**Key words:** DIOS; Public Computing Communication Network(PCCN); Cloud Computing

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2011) 01-0045-04

童晓渝/TONG Xiaoyu  
张云勇/ZHANG Yunyong  
房秉毅/FANG Bingyi  
(中国联通研究院 北京 100048)  
(China United Research Institute, Beijing 100048, China)

台与终端的配合机制。

文章基于对目前信息通信服务环境的分析和电信运营商商业模式的转型,提出分布式智能运营架构。该架构是未来公众计算通信网(PCCN)的核心系统<sup>[1]</sup>,它能够实现网络智能管理、业务智能开发、服务智能提供,并可利用、整合公共性平台资源,缩短业务创新周期,共同维护共生共存的产业生态系统。

### 1 分布式智能开放运营架构的内涵和目标

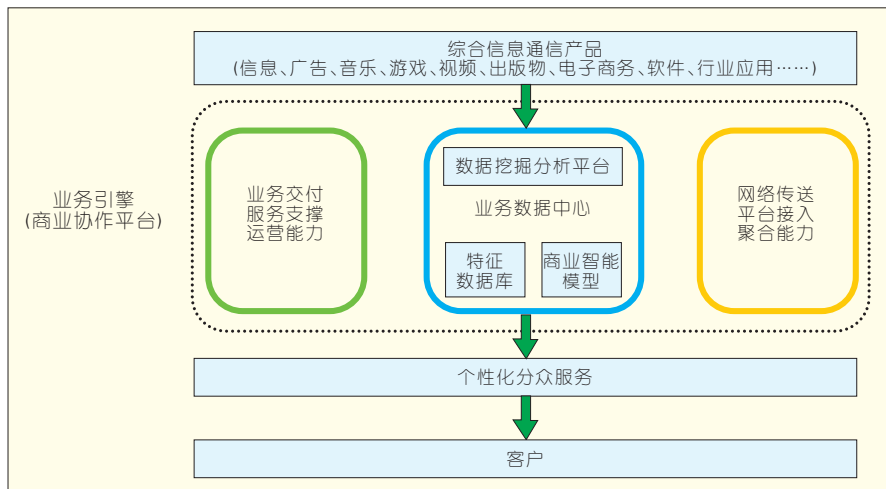
分布式智能开放系统(DIOS)是为适应电信运营商商业模式的转型而提出的,从主流电信运营商的策略来看,主要有以下几种方式<sup>[2]</sup>:

- 向“通信+商业渠道”转型。优化通道掌控、应用汇聚、终端体验,尤其是客户需求分析,实现产品、服务与需求价值匹配,形成规模经营、快速交付、精确营销的新型渠道能力。
- 向“通信+媒体广告”转型。利用丰富的客户需求信息资源,创建数据挖掘分析能力;利用通道与终端交付能力,形成“泛终端”、“富媒体”分众立体式广告模式。
- 向“通信+信息服务”转型。利

中国电信重组完成后,随着电信运营商 3G 网络的部署和互联网升级提速,运营商之间的竞争更加激烈。越来越丰富的应用正在大量地消耗带宽,电信运营商既没有从通道服务中获得合理的投资回报,也没能在高附加值的信息服务领域创造更大的企业价值。互联网已经形成了以各类服务与应用为主的巨大产业规模、企业价值和社会影响,成为“渠道为王”、“内容为王”、“应用为王”的时代,与此同时,产业链的控制权、话语权发生了转变。广电系统正在全面进行广播电视网数字化整体转换和双向改造的部署,积极推进

“三网融合”,已经成为信息通信服务业新竞争者。

随着 3G 时代的到来,移动互联网的发展,IT、互联网、传媒、电信、零售行业正在加速融合与渗透,行业的边界变得越来越模糊,正逐步演变成一个全新的产业生态系统。新的变革客观要求产业生态系统的参与者更加开放、合作,以实现共存、共生、共同进化。从电信行业的视角来看,一个全新的“后电信时代”正在到来。作为平台型企业的电信运营商需要更加开放,提升创造价值和分享价值的能力、平台架构能力、标准化能力、网络的再设计与优化能力、平



▲ 图1 转型网络架构

用公众通信网基础性和安全可信的运营能力,基于宽带通信与云计算技术的发展,形成信息设施、信息生产、信息应用的服务,即“云计算”服务。

- 向“前+后”收费模式转型。基于渠道、媒体特征开发后向收费模式,通过降低用户通信与信息费的方式,加快用户发展(快速聚合),增加使用时间(提高浏览量),增强渠道和媒体效用,提高代理费、广告费等创收能力。

- 建立以“客户价值为核心”的运营构架。在原运营构架基础上,增加“业务数据中心系统(BDCS)”为重要的核心运营系统,构成电信运营商新的运营构架。

电信运营商转型应发挥网络和客户优势,由网络转向对业务、平台、客户、界面等商业资源的运营。为了适应向“通信+商业渠道+媒体广告+信息服务”的商业模式转型,电信运营商在原来通信网络传送、平台接入的聚合能力和业务交付、服务支持的运营能力的基础上,增加一个重要的核心运营系统,即业务数据中心,如图1所示。运营商从以网络为中心的运营转型为以客户为中心的运营,而通信网络只是实现客户接入业务的通道及用户聚合的手段,各种新商业模式的运营都将基于数据中心对用户信息的挖掘,经过特征数据库和

商业智能的分析后,再由PCCN以个性化分众服务的方式传送给客户,使客户得到良好的终端体验。

因此,在网络服务日益趋于信息服务、信息管理服务的背景下,业务的提供需要大量的计算能力做支持。随着网络带宽变大,计算能力应用变广,通信技术与业务的发展趋于计算技术与应用技术,而计算技术与应用技术的发展又趋于网络与服务的提供。现今的公众通信网逐渐演进为PCCN,而DIOS则是未来PCCN的核心系统,它具有分布式、智能、开放、统一化系统特性,能够实现网络智能管理、业务智能开发、服务智能提供。

DIOS以分布式存储、分布式计算资源、分布式数据库和文件系统为基础,通过云网络整合统一资源,实现按需弹性扩展能力;通过数据挖掘、分析和智能调度,实现网络智能自组

织和可重构,以及业务与资源、应用与服务、终端与用户的最佳匹配;建立能力引擎开放平台,向第三方开发者开放云资源,全面快速响应服务;统一虚拟化标准,降低成本,实现统一资源共享最大化;统一管理平台,提高集中管理效率,实现电信级可运营可管理。

## 2 未来公众计算通信网

PCCN基于虚拟化和云计算构架,以云计算技术为核心,融合电信网和计算机网的信息处理网络。利用云计算的虚拟化技术可以建立支撑网、业务网及统一基础设施资源池;利用云计算的理念可以对基础设施资源池进行组织和运用。在原有公众通信网的接入、交换、路由、传输要素的基础上,PCCN实现了计算处理能力、虚拟分配、调度管理等主要技术,如图2所示。

## 3 分布式智能开放系统

DIOS是PCCN的核心系统,可以看作是PCCN的具体实现,其组网拓扑如图3所示。

DIOS系统自上而下,自内而外可分为如下的6层架构。

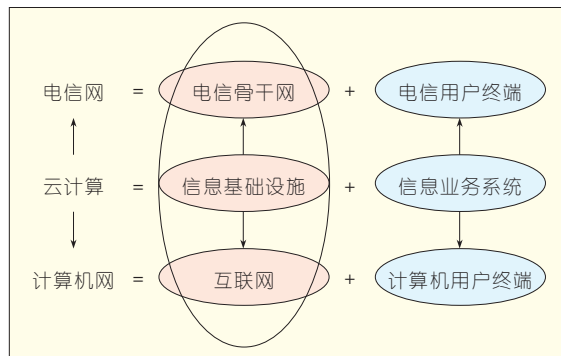
第1层:数据中心层

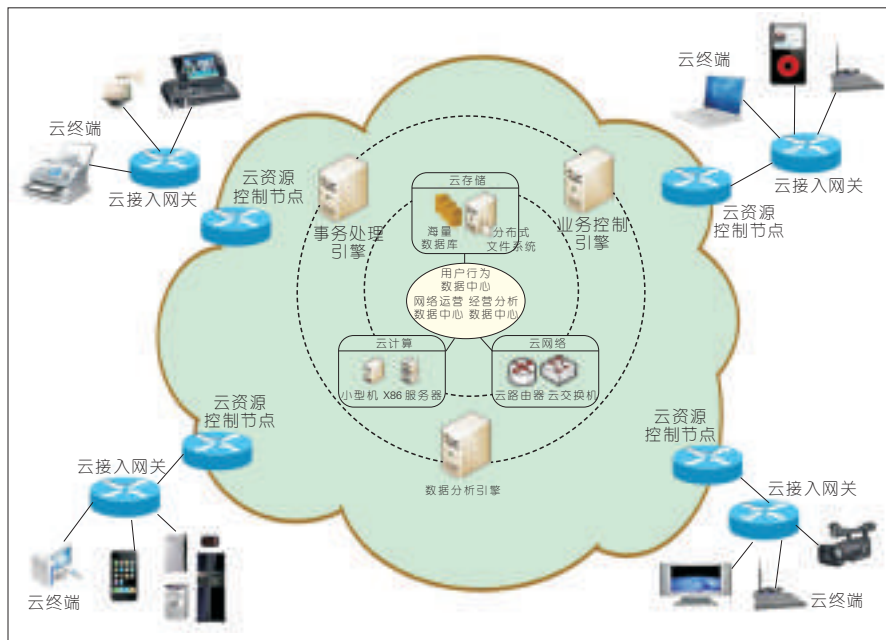
数据中心层是由“网络数据中心”、“用户数据中心”和“业务数据中心”3个子系统构成的BDCS。

第2层:云资源系统层

云资源系统由云存储、云网络和云计算设备3部分组成,包括:海量数据库和分布式文件系统;可编程、

图2  
PCCN与电信网、云计算、计算机网





▲图3 PCCN组网拓扑图

可虚拟化和增强资源共享的云交换机和云路由器构成的精简架构；异构混合的小型机和X86服务器等云计算物理设备。

#### 第3层：能力引擎层

能力引擎由事务处理引擎、业务控制引擎和数据分析引擎组成。

事务处理主要是指基于工作流的业务流程和管理流程实现过程，如：营运支撑(BSS)、合作伙伴关系管理(PRM)、运维支撑(OSS)、运营数据存储(ODS)、办公自动化(OA)等。

数据分析主要是指基于特定的计算规则对结构化数据和非结构化数据进行计算处理，以期从海量信息中得到规律性的认识，如：商业智能(BI)、客户关系管理(CRM)和搜索引擎业务。

业务控制主要是指：根据预先设定的规则，对网络组织、业务控制、应用适配、服务交付等进行的策略管控，如：会话边界控制器(SBC)、呼叫会话控制功能(CSCF)、用户数据中心(SDC)/归属位置寄存器(HLR)/归属用户服务器(HSS)、认证授权计费(AAA)、应用程序编程接口(API)、会话描述协议(SDP)等。电信增值业务平台中的

业务控制模块、计费系统的用户信用控制模块都是这方面的典型应用。

#### 第4层：云资源控制节点层

云资源控制节点层基于分布式架构技术，屏蔽云内复杂的物理和逻辑结构，实现可扩展的自适应负载均衡能力和动态资源智能适配能力，并进行不同业务间的引擎适配，形成自动智能调度。

#### 第5层：云接入网关层

通过云接入网关将终端接入云中，包括物理接入网关和业务平台接入网关，屏蔽物理设备和业务平台的差异，并进行不同终端接入的智能适配，实现统一接入。

#### 第6层：云终端层

由云终端物理设备和客户端软件组成。其中云终端物理设备包括瘦终端和哑终端（如：物联网传感器等）、智能软终端和浏览器等。

DIOS系统架构图如图4所示。

## 4 DIOS 关键技术

### 4.1 统一虚拟化技术

虚拟化技术是整个DIOS系统的基础，它采用的技术种类较多，应用

到的主要技术有服务器虚拟化、存储虚拟化以及网络虚拟化等。具体包括异构资源虚拟化、异构虚拟机热迁移技术、虚拟化容错灾备技术、承载层虚拟化、控制层虚拟化、可重构智能网络等。其中异构资源虚拟化是在目前各种系统并存的情况下所必须的，已经成为网格和数据中心环境下成功实现提供定制资源的强有力的技术，它为数据、计算能力、存储资源以及其他资源提供了一个逻辑视图，而非物理视图，从而能屏蔽很多物理的、结构的细节。只有采用统一的虚拟化技术，异构资源才能发挥最大效力，便于管理和使用。

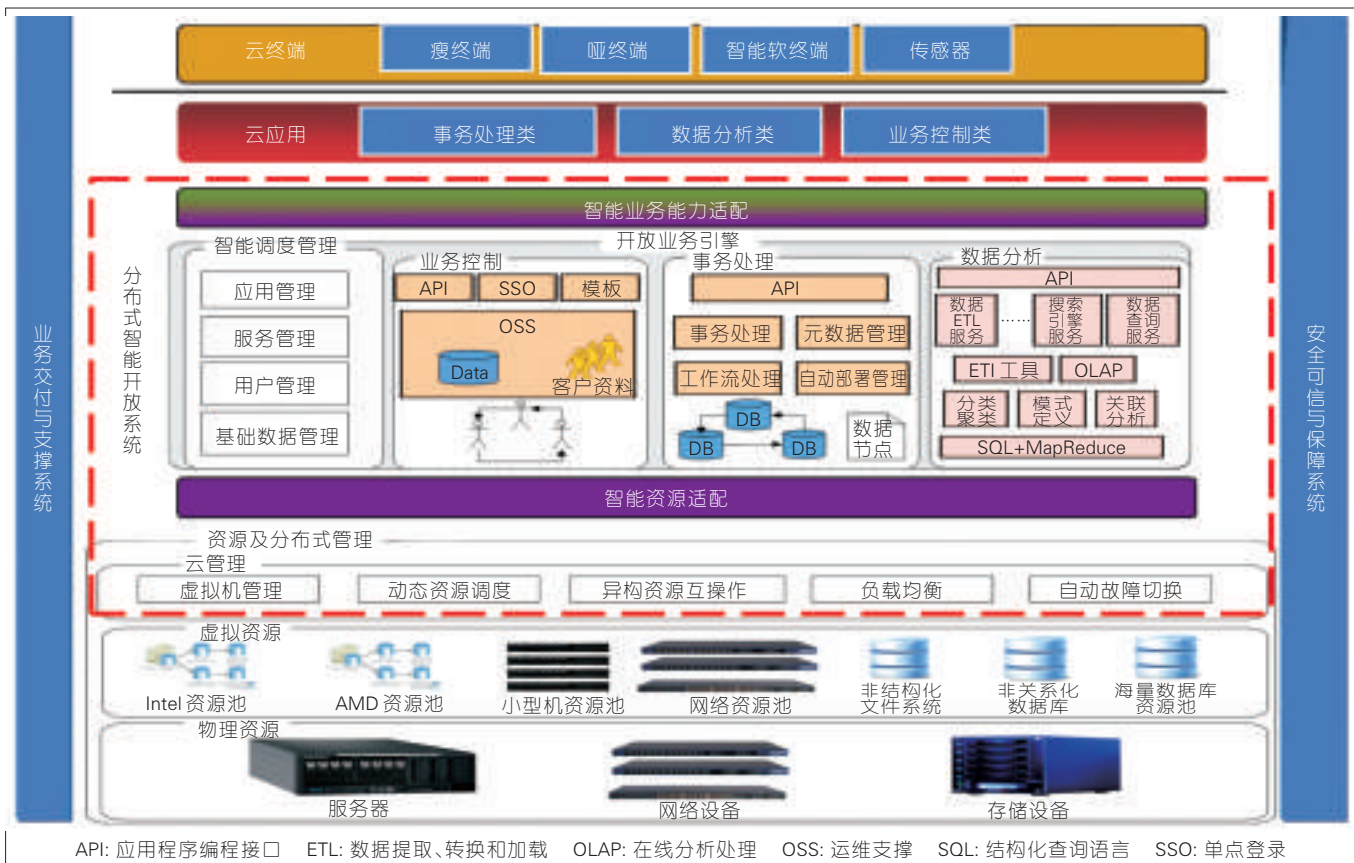
### 4.2 统一云管理技术

DIOS系统需要对复杂的实际应用进行资源匹配和资源调度以及并行/并发执行，使资源得以最大化利用的同时也提高整个网络系统的执行能力和运行性能，为用户提供更高质量的服务。统一云管理包括对虚拟服务器资源自动配置和调度的虚拟机调度管理；支持操作系统和应用的自动化安装和配置，批量部署的部署管理；实现异构存储资源整合，远程复制功能（同步及异步）、远程镜像复制、快照的存储管理。

### 4.3 开放业务能力引擎

第三方服务提供者是电信业长尾的主力，丰富的业务需要大量第三方开发者参与其中，业务能力组合、混搭成各种特性的应用需要大量的第三方用户参与开发。运营商的主要职能就是打造开放业务能力引擎，第三方开发者则通过开发低成本的业务，增强业务创新能力，参与、使用、吸引更多的用户。DIOS可以为电信业务提供全新的应用场景，通过能力引擎开放平台，如业务控制、事务处理、数据分析等，向第三方开发者开放云资源，全面快速响应服务。DIOS业务开放能力引擎包含两个维度：第一个维度是基本业务能力，包





▲ 图4 DIOS系统架构

括业务控制、事务处理、数据分析等；第二个维度是融合业务能力，如支持各种网络的接入能力提供信息通信技术(ICT)服务。同时，需要提供开放业务能力引擎的管控，负责对开放服务接口发送过来的各种业务请求进行统一的用户和能力鉴权、负载均衡、路由分配和会话控制，业务能力引擎管控组件统一管控，实现有关BSS和OSS功能。管控功能包括：接入控制、策略管理、配置管理、计费管理、故障管理、监控管理以及统计分析等。

#### 4.4 智能资源适配

当业务能力引擎开放给第三方应用时，还需要使用到底层的各种资源。智能资源适配根据业务类型，智能适配不同的计算、网络、计算资源，并对各类业务能力引擎的资源进行集中调度和管理，使上层应用效用最

大化。

## 5 结束语

电信运营商正经历史无前例的挑战，处于转型和创新的关键期。作为平台型企业的电信运营商需要更加智能开放的业务系统，在原运营构架基础上，增加“BDCS”为重要的核心运营系统，通过分布式和虚拟化资源提供方式，构成电信运营商新的运营构架，同时整合研究开发、产品制造、网络建设、应用开发和服务提供等各方面，构建更加开放的生态体系和商业模式。

## 6 参考文献

- [1] 童晓渝,张云勇,戴元顺: 公众计算通信网架构及关键技术[J]. 通信学报,2010,31(8):134-140.
- [2] 童晓渝,吴钢,张云勇,等. 后电信时代[M]. 北京: 人民邮电出版社,2010.

收稿日期:2010-11-23

## 作者简介



**童晓渝**, 中国联通研究院副院长、教授级高级工程师,信息管理硕士、工商管理博士;主要研究方向为大型分布式异构网络、智能信息处理;曾参与多项信息通信领域重大项目,并曾多次获得科技进步奖、管理创新奖和发明专利;出版专著4部,发表论文30余篇。



**张云勇**, 中国联通研究院研发部副经理、高级工程师,博士后,中国通信学会、电子学会、计算机学会高级会员,中国人工智能学会会员;主要研究方向为下一代开放网络、固定移动融合核心网、移动互联网及业务、公共运算;出版中文论著14部,英文论著1部,发表论文58篇。



**房秉毅**, 中国联通研究院高级工程师、工学博士;主要从事云计算、核心网新技术的研究;发表论文20余篇。

# 基于业务感知的认知网络 QoS 自适应控制技术

## QoS Self-Adaptive Control in Cognitive Networks Based on Service Awareness

顾成杰/GU Chengjie, 张顺颐/ZHANG Shunyi, 孙雁飞/SUN Yanfei

(南京邮电大学 信息网络技术研究所 江苏 南京 210003)  
(Institute of Information Network Technology, Nanjing University of Posts and Telecommunications,  
Nanjing 210003, China)

中图分类号: TP393 文献标志码: A 文章编号: 1009-6868 (2011) 01-0049-04

**摘要:** 文章研究并提出了基于业务感知的认知网络服务质量(QoS)自适应控制架构。该架构在智能业务感知和分类模型的基础上对数据包进行分类和识别,并借鉴控制理论通过基于端路协同的认知网络业务流 QoS 自适应控制机制实现对网络流量的控制。在认知网络环境下,该架构可以构建 QoS 的自动感知、分析、关联、反馈、决策、配置和实施机制,进行资源的优化调整分配,适应网络环境的变化,优化网络端到端的性能,保证用户的服务质量。

**关键词:** 认知网络; 业务感知; 自适应控制; QoS

**Abstract:** This paper analyzes the Quality of Service (QoS) self-adaptive control architecture of cognitive networks based on intelligent service awareness. In this architecture, packets can be identified and classified using an intelligent service-aware and classification model. Drawing on Control Theory, network traffic can be controlled with a self-adaptive QoS control mechanism that has side-road collaboration. In this architecture, perception, analysis, correlation, feedback, decision making, allocation, and implementation QoS mechanisms are created automatically. These mechanisms can adjust resource allocation, adapt to a changeable network environment, optimize the performance of the end-to-end network, and ensure QoS for users.

**Key words:** cognitive network; service-awareness; self-adaptive control; QoS

### 1 认知网络的概念

当前网络业务类型众多,网络环境复杂且动态多变,传统的端到端保证技术因缺乏智能推理和自

学习能力,难以根据网络行为的动态变化迅速且自适应地为用户提供理想的服务<sup>[1]</sup>。现行网络系统的显著问题是不能充分感知终端用户的服务需求,不能根据网络系统的内外环境变化有效、动态地改变终端用户服务质量(QoS)<sup>[2]</sup>。针对这些问题,学术界已着手在下一代网络中融入认知元素以克服当前网络的固有缺陷,并提出并阐述了认知网络概念。

认知网络的研究源自于认知无线电, Mitola 等人<sup>[3]</sup>于 1999 年提出了认知无线电(CR)的概念及认知环架构,他们认为认知无线电系统通过感知,获取周围环境的频谱使用信息,依据优化目标,确定 CR 的重构方案,达到适应频谱环境变化的目标。认知网络(CN)的概念由 Motorola 及 Virginia Tech 公司在认知无线电的基础上率先提出<sup>[4]</sup>,该概念指出认知网络是一种具有自我认知能力的网络,能够感知自身及周围环境变化,并根据当前网络环境来规划、决策并行动,给出了双闭环控制的 FOCAL 架构。2003 年 D.Clark<sup>[5]</sup>等学者在 SIGCOMM 会议上提出的互联网引入知识平面(KP)的思路,其关键思想是知识平面能获得它自己的行为,随着时间的推移,使之能更好地分析问题,调整其运作,增加其可靠性和稳健性。2006 年美国弗吉尼亚工学院的学者 Thomas<sup>[6]</sup>进一步明确了认知网络的定义,指出认知网络是具有认知过程,能感知当前网络条件,然后依据这些条件作出规划、决策和采取动作的网络。2007 年 Baldo 等学者采用模糊逻辑来有效地处理认知网络实现中的模块化、解释性、不精确性等问题<sup>[7]</sup>。2008 年 Siebert<sup>[8]</sup>等学者指出认知网络的一个重要特点就是能以自治的方式完成任务,比如自我管理、自我优化、自我监测、自我修理、自我保护、自我治愈等。2009 年 Carolina Fortuna 等人在文献[9]中指出 Thomas 定义的认知网络并不完善,知识表示和认知环是认知网络最重要

**基金项目:** 国家高技术研究发展(“863”)计划(2006AA01Z232、2009AA01Z212、2009AA01Z202); 国家自然科学基金(61003237); 江苏省重大科技支撑计划项目(BE2008134)

的两个元素。目前在美国电气和电子工程师协会(IEEE)正在讨论异构无线接入网络融合架构的标准化,采用了认知网络的概念。认知网络被认为是提高网络整体及端到端系统的性能、简化网络管理的新途径,是下一代通信网络发展的必然趋势<sup>[10]</sup>。

作为一个新兴的研究热点,认知网络在中国和其他国家的研究才刚刚起步,相关的理论和技术均需要深入的研究。与传统网络相比,认知网络能够感知网络状态,进行智能决策并重新配置,提高资源利用率,优化网络性能<sup>[11]</sup>。作为一种新型的智能网络,认知网络借助人工智能领域的相关技术,通过分布式智能代理实现认知功能。具有学习推理能力的智能代理部署于网络中的各个节点,监测并搜集周围环境信息。这些代理之间可以进行信息交互和协作,使得网络能够感知当前状况,基于当前网络状态,以实现端到端目标为目的,基于知识库中的知识,进行网络资源的评估、预测、规划、调整和分配,使得网络具有自感知、自学习、自优化、自修复和自配置的能力,实现真正意义上的网络可测、可控、可管和可信。

文章所提出的认知网络 QoS 控制架构,其核心思想就是网络系统能够感知网络环境变化,实时调整网络系统的配置,动态智能地适应环境并指导网络的自主决策。自适应控制技术一方面能够对有限的网络带宽进行合理高效地规划与分配,在很大程度上改善网络性能;另一方面,根据业务特性对网络流量进行管理和控制,提高单位带宽收益率。因此对认知网络进行精细化的自适应控制是解决网络 QoS 问题的根本途径之一。

## 2 认知网络 QoS 的关键技术

2006 年美国弗吉尼亚工学院的 Thomas 首次明确给出以下的认知网络定义:认知网络是具有认知过程,能感知当前网络条件,然后依据这些条件作出规划、决策和采取动作的网

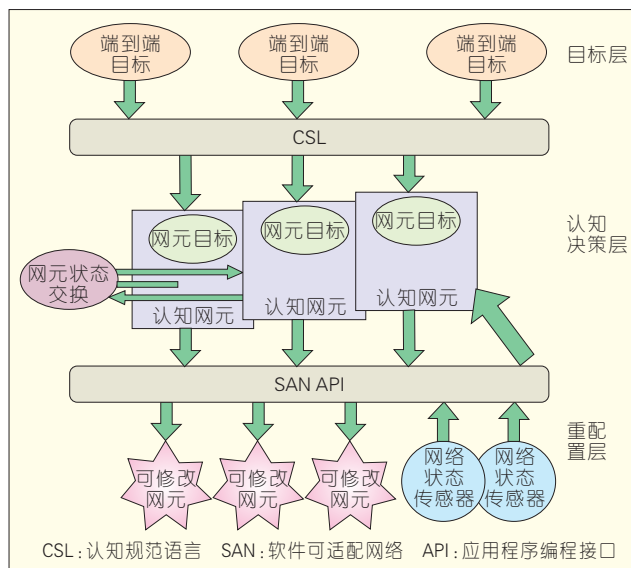
络。认知网络具有对网络环境的自适应能力,具有对于以前决策的评判和未来决策判定的学习能力,决策要达到的都是端到端的目标。

根据上述定义可将认知网络结构抽象为“目标—认知决策—重配置”3 个层次,如图 1 所示。目标层反映由应用、用户或资源提出的目标需求,这些目标通过认知规范语言(CSL)映射为特定的机制要求,

反馈送给一个或多个相关的认知网元。认知决策层根据目标层的要求,完成相关网元之间状态交换以及感知的当前网络状态,并按照一定的方法得出网元配置的决策。重配置层也称为可适配网络层,认知决策层的决策将通过应用编程接口发送给对应的实体网元,并通过调整该网元的配置,以满足目标层的需求,同时将网络状态通过传感器反馈给认知决策层。

### 2.1 上下文感知

迅速准确地感知网络环境信息是认知网络得以发挥作用的基础。认知网络需要及时观测当前的网络环境信息。这些信息将用于后面的规划、决策等认知处理过程,以判断当前网络是否能满足用户要求,如果不能满足就要采取相应的重配置手段来保证满足用户要求。环境感知的内容包括网络类型、网络拓扑、可用资源、接口协议、网络流量等影响端到端传输性能的状态信息<sup>[12]</sup>。上下文感知是提高认知网络智能性的重要途径,它关注的是如何发现上下文信息的变化,并且根据上下文的变化进行自适应调整。当网络环境动态变化时,网络应该做出相应的自适



▲ 图 1 认知网络层次图

应调整。上下文感知主要采用基于反射机制和策略机制的方法来实现上下文自适应,通过策略定义,网络可以预先制定上下文发生变化时的调整方法。

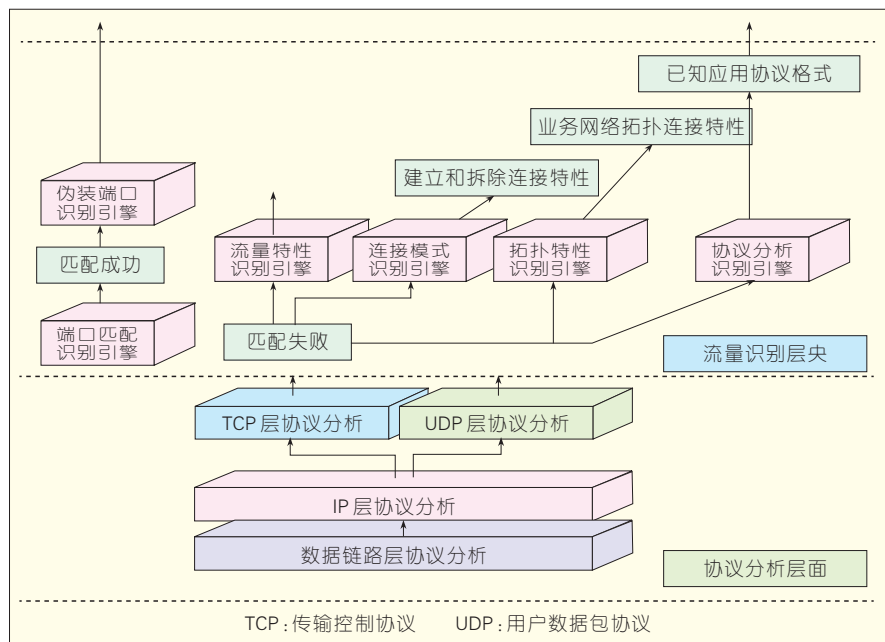
### 2.2 跨层设计

跨层设计的本质思想是打破传统的网络系统框架,以满足通信系统的 QoS 的要求为目的,将通信系统资源的状态参数和服务的 QoS 参数在协议层中传递,从而达到各协议层联合设计,充分利用系统资源,为用户提供更好服务的目的<sup>[13]</sup>。认知网络的最终目的是根据认知的网络信息调整相关网元的协议栈或协议层参数,以保证用户的端到端性能。认知网络中的认知处理层需要知道网络各层的状态信息,然后根据优化算法确定适当的行动,重新配置网络参数和协议栈来实现端到端的目标。

### 2.3 重配置

如果当前的网络条件无法保证用户要求的端到端目标,认知网络则需要根据这个目标调整相关网元的协议栈参数,以保证用户所要求的端到端目标,这个调整过程就是网络的重配置<sup>[14]</sup>。认知网络强调端到端的





▲图2 基于综合特征的智能业务感知和分类模型

目标,它应该具备端到端的重配置能力,相对于软件无线电技术仅限于终端的重配置而言,它涉及到某个流所经过的各个网元和协议标准的所有层次,是一种更具有前瞻性的目标保障方案,它的端到端的重配置考虑得更全面。认知网络的实现最终要落实到网元重配置,重配置过程也是通过软件实现的,但是其重配置的技术层次更高。不但包含终端重配置,还包含网络重配置和业务重配置;同时不限于单个节点,可能覆盖端到端路径上的多个网元,称之为端到端重配置(E2R),其复杂度和重要性远高于终端重配置。

### 3 基于业务感知的认知网络 QoS 控制架构

#### 3.1 业务感知

从网络业务组成情况来看,近几年网络新业务层出不穷,有常规数据业务、对等网络(P2P)、VoIP 语音、流媒体、互动在线游戏和虚拟现实等。新业务的大量出现对网络的流量模型和应用模式产生了很大的冲击,尤其是 P2P 应用的飞速发展,其流量爆

发式的增长和不加限制的带宽使用,极大地增加了网络负担,使网络拥塞现象日趋严重。由于简单的扩容无法满足业务容量增长的需要,因此借助认知网络技术对网络传输业务进行主动的感知、分析、决策和控制是解决目前网络问题的根本途径之一。

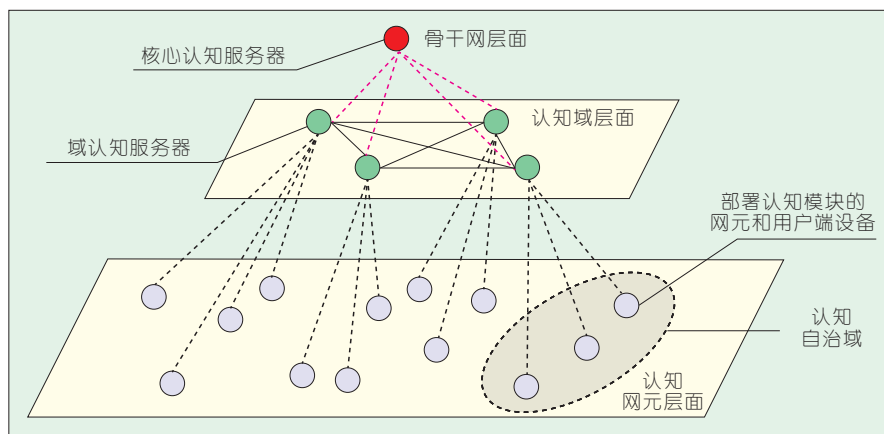
认知网络以业务为驱动,需要网络系统主动感知网络上存在的各类业务,包括终端用户业务状况和各网元设备业务状况。基于业务流的主动智能感知与分类是认知网络以业务为中心对网络自身进行资源配置、路由调整、动态自适应流量控制的基

础。在业务感知技术领域,认知网络概念引入之前,多采用传统的静态端口方法、净荷特征方法以及流统计特性方法,这些方法对常规业务的感知是比较有效的,但无法准确、高效地感知很多新的业务。

引入认知网络概念以后,网络具备了分析与决策能力,具有了很好的智能性,因此本节建立新的基于综合特征的业务感知模型来主动、智能并实时地感知各类业务。如图2所示,该模型在认知网络获取网络常规参数的基础上,建立基于流统计特性、连接模式、拓扑特性、内容特征等特性的综合特征识别模型,并针对每种特征建立识别引擎,通过策略智能地触发和感应不同的识别引擎,从而准确、高效地识别已知或未知的、加密或明文业务流。通过建立基于综合特征的智能业务感知模型,实现对已知或未知、加密或明文的区分服务,为基于业务感知的认知网络 QoS 自适应控制架构奠定了技术基础。

#### 3.2 认知网络 QoS 三级自适应控制架构

如图3所示,认知网络 QoS 决策与控制架构采用三级分层结构,由网元(设备)认知模块、自治域认知服务器和中心认知服务器组成。各部分均具有认知能力(自感知、自学习、自决策)能力。网元(设备)认知模块是认知网络 QoS 感知、分析和控制系统



▲图3 认知网络 QoS 三级自适应控制架构

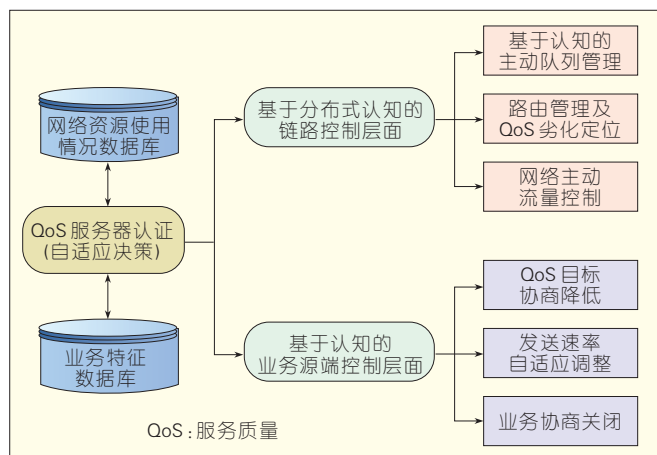


图4  
基于端路协同的认知网络 QoS 控制框架

的基本单元,不仅具有感知与决策的能力,还具备动态调整网元设备参数或配置的能力。部署认知模块的网元和用户端设备组成一个认知自治域。认知自治域内设一个具有认知能力的域认知服务器,负责对域内网元设备、业务流、网络资源等的管理与控制。同时该架构中设置一个中心认知服务器,负责对整个网络的运行情况进行全局性监测、认知与管理。分层结构能够有效地降低中心认知服务器的负载,即使该服务器临时失效,也不影响全网业务的 QoS 保证与管理。自治域认知服务器之间进行分布式组网、通信,相互进行实时的信息交流,域认知服务器之间采用分布式管理的出发点是增加系统的可靠性、灵活性和可扩展性。在自治域内每个网元之间,实现相邻节点的互相通信,进行分布式协作监测和自适应处理。该架构充分结合了集中式架构和分布式处理技术的特点。

### 3.3 端路协同的认知网络业务流 QoS 自适应控制机制

认知网络端到端 QoS 由认知网元保障。认知网元之间相互协作或独立运作,通过实时感知网络当前状况,并结合网络历史态势,综合分析网络状况,根据既定的策略进行自配置,进而实现端到端 QoS 的目标。

这一章节在认知网络业务感知的基础上,参考资源预约的理念,借

鉴控制理论,在认知网络环境下采用业务源端 QoS 控制与链路 QoS 控制相结合的方式,提出基于端路协同策略的认知网络 QoS 自适应控制机制,以解决业务流端到端 QoS 保证问题。该机制利用反馈控制,将获得的实时网络相关参数通告自治域认知服务器(或中心认知服务器),形成终端网元、路由器设备相结合的认知网络业务流 QoS 自适应控制方式。通过将网络历史状况与当前状况相对比生成控制策略,并通过自学习对策略库进行更新,使其保持控制策略的最优性。该机制能够在保证单个网元设备正常工作的基础上,充分体现认知网络的特征,协调周边各相关网元设备,对有限的宝贵资源进行合理的协商分配,提升用户用户体验(QoE),保障业务 QoS,进而实现业务端到端的有效控制,最终实现全网性能最优化。如图4所示,主要分为基于认知的业务源端控制层面和基于分布式认知的链路控制层面。

基于认知的业务源端控制主要通过源端发送速率自适应调整、业务主动关闭、QoS 目标主动降低来实现。传统网络中业务源端在发起业务时,不会考虑当前网络状况,而认知网络的业务源端由于具有一定的感知功能,它的感知信息来源于域服务器或者中心控制服务器。只有满足一定条件的时候(比如带宽足够、网络中的资源能够接纳其他业务流

的接入)才会与对端进行业务流传输。当高优先级的用户需要进行业务传输,而此时网络没有足够的资源来满足其服务等级协议(SLA)中签署的相关需求时,则中心认知服务器(或域认知服务器)需要与业务源端的用户进行协商。如果此用户接受降低业务预期的 QoS 目标的服务,则源端按照协商的结果来进行业务流的传输。若高优先级业务不能降低 QoS 要求,则认知服务器会根据资源分配策略对正在使用的网络资源进行一定的回收,甚至强制关闭某些低优先级的业务。

基于分布式认知的链路控制主要通过网元流量的主动控制、路由管理及 QoS 劣化定位和基于认知的主动队列管理等来实现。通过对全网信息的感知和决策,网络中具有认知功能的交换机或路由器等网元设备都能够主动控制其内部各类业务流的流量,保证可信任业务流和关键业务流的流量,并限制“不安全流”或非关键流的流量。同时随着网络业务需求和网络资源的实时动态变化,通过认知路由管理和 QoS 劣化定位可以及时发现端到端网络资源的瓶颈网段或 QoS 劣化部分,及时进行分析与决策,并对业务流进行重路由。另外也可以借助智能主动队列管理算法来决策认知网络的网络拥塞问题。基于认知的主动队列管理以服务器协同策略驱动为导向,结合主动队列管理方法,改进现有的资源预约算法及路由器缓存管理模式,对路由器或端系统进行合理的资源预约。

## 4 结束语

随着网络技术和应用的飞速发展,网络的接入形式以及网络应用日益复杂、异构和泛在等特点,当前网络所提供的服务质量 QoS 远不能完全满足用户的需要。认知网络被认为是提高网络整体及端到端系统的性能、简化网络管理的新途径,是下

→下转第 56 页

# LTE 网络覆盖规划技术研究

## Research into LTE Network Coverage Planning

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2011) 01-0053-04

**摘要:** 为了保障高质量的网络部署, LTE 系统的覆盖规划对网络的建设成本及质量发挥着至关重要的作用。文章基于 LTE 实际组网的规划需求, 结合系统化的理论及仿真分析, 对 LTE 无线接入的链路及网络特征进行了深入的研究。在此基础上, 开发形成一套完整的 LTE 蜂窝网络覆盖规划理论及应用方法, 为 LTE 无线网络规划提供了基础性的技术指导。

**关键词:** 覆盖设计; 几何因子; 功率控制; 干扰余量

**Abstract:** For efficient LTE network deployment, coverage planning is important to reduce construction costs and ensure network quality. This paper considers actual network planning requirements and combines theory with simulation analysis to study LTE wireless access link and network characteristics. A theory for LTE cellular coverage planning and application methods is then proposed, which lays the basic foundation for LTE cellular networks.

**Key words:** coverage design; geometry factor; power control; interference margin

顾军/GU Jun  
盛韧/SHENG Ren

(中兴通讯股份有限公司, 广东 深圳  
518004)  
(ZTE Corporation, Shenzhen 518004, China)

随着无线业务需求的不断增长, 目前的 2G、3G 网络承载能力日趋饱和, 为了应对移动网络的不断凸显的供需矛盾, 第三代合作伙伴计划 (3GPP) 长期演进技术 (LTE) 逐步从理论走向现实。强大的业务承载能力、高效的系统资源利用方式、低廉的网络建设和运营成本、灵活的网络部署模式使 LTE 越来越受到各主流运营商的青睐<sup>[1]</sup>。

LTE 系统标准化的不断成熟有效地推动了相关产业。从目前来看, 3GPP 在 Release-8 的相关工作已经冻结, 在此基础上各设备商已经展开了 LTE 产品的研发工作, 同时各类实验局的部署和测试也在有序的进行之中。从整个产业来看, 虽然 LTE 产品的研发取得了实质性的进展, 但是 LTE 系统的高度复杂性和灵活性带来了各种不确定性, 因此业界对于

LTE 系统特征、建网思路、优化策略尚处于初级的摸索阶段。就 LTE 网络规划而言, 系统性理论体系及应用方案的缺失成为 LTE 能够高效、精确部署的主要技术障碍。

在 LTE 系统中, 空中接口采用了正交频分复用 (OFDM)、多输入多输出 (MIMO)、高级编码调制方式 (AMC)、混合自动重传 (HARQ) 等先进的无线链路技术, 并通过动态调度、小区间干扰消除技术 (ICIC)、功率控制等无线资源管理算法提高空口资源配置的效率和灵活性<sup>[2-3]</sup>。从 LTE 的网络设计来看, 上述无线技术在提升网络性能的同时, 也大大增加了系统分析的复杂度。要实现高效、可靠的 LTE 网络覆盖规划方案, 需要通过系统化的理论、仿真、测试等, 从而对系统的技术特征进行全面的分析和研究。与 2G、3G 网络相比, LTE 网络在资源共

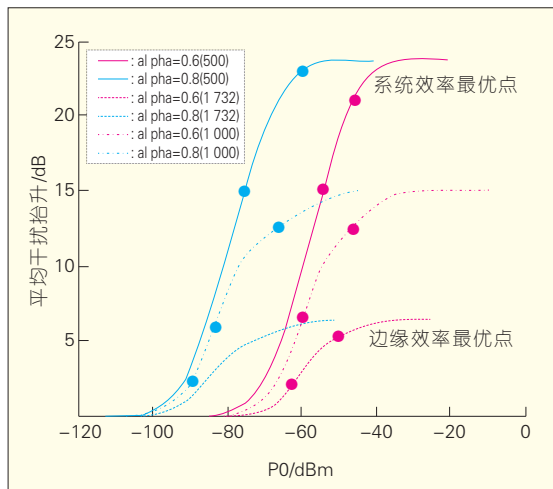
享方式、系统干扰特征等影响网络覆盖性能的核心因素方面有着根本性的不同, 传统的覆盖规划及链路预算思路 and 方案已远不能满足 LTE 实际建网的需要<sup>[4]</sup>。鉴于上述原因, 对于 LTE 系统的覆盖规划, 需要分析和总结网络建设的潜在需求, 剖析 LTE 系统的技术和网络特征, 总结出适合 LTE 网络建设的覆盖规划体系和方案, 并不断完善。另外, 增强频谱效率是提升 LTE 竞争力的核心内容之一, 因此它和频组网下的 LTE 系统网络设计是文章关注的重点。

### 1 LTE 网规流程及覆盖规划策略

总体来看, 频分双工 (FDD) LTE 的网络规划流程和 2G、3G 规划流程基本保持一致, 包含需求收集和分析、覆盖和容量设计、站点选择、规划仿真、报告撰写五大部分。其中, 覆盖和容量设计是整个网络规划的核心要素, 需要根据用户的具体需求, 结合对网络特征的深入分析, 对网络规模进行全面估算。文章主要对 LTE 系统的覆盖规划方法进行分析。

FDD LTE 系统覆盖规划的主要目标是基于实际的小区边缘覆盖需求, 在一定的系统参数设置下, 估算基站





▲ 图1 上行干扰特征与建网策略

能够实现的覆盖距离,从而得到网络规模需求。根据应用场景和实际的规划需求,FDD LTE 系统的覆盖规划策略一般主要分为3类:

- 基于上行边缘速率要求的网络规模估算

第1种策略主要应用于只限制了上行边缘速率的覆盖需求。基于上行速率,在一定的链路预算参数输入下,计算出上行的覆盖半径;并根据得到的上行覆盖半径预测下行可实现的边缘速率;

- 基于下行边缘速率要求的网络规模估算

第2种策略主要应用于只限制了下行边缘速率的覆盖需求。基于下行速率,在一定的链路预算参数输入下,计算出下行的覆盖半径;并根据得到的下行覆盖半径预测上行可实现的边缘速率;

- 基于上行和下行边缘速率要求的规模估算

第3种策略主要应用于同时限制了上下行边缘速率的覆盖需求。基于上下行速率,在一定的链路预算参数输入下,分别计算出上下行的覆盖半径;并通过比较即可得到受限的覆盖半径。

在实际的网络规划中,需要根据不同的具体需求和应用场景选取合适的覆盖规划策略,灵活应对网络规

划中出现的问题。

## 2 LTE 上行覆盖规划关键技术

要解决 LTE 覆盖规划的问题,关键在于如何根据上行或下行的边缘业务速率要求得到相应的覆盖范围。对于一些特殊的场景或业务,还要考虑控制信道的相关覆盖性能。文章主要讨论业务信道受限场景下的覆盖规划问题。在给定的业务速率需求下,需要从 LTE 的链路及系统两个方面对网络的

技术特征进行深入的分析和总结。

对于 LTE 上行覆盖规划技术的研究,主要包含两个方面:系统级研究和链路级研究。由于 LTE 系统上行引入了基于单载波-频分多址(SC-FDMA)的多址接入方式,小区内的用户之间互相正交,干扰主要来自于邻小区的激活用户,上行功率控制策略的选择直接影响小区间的干扰模式及干扰强度<sup>[5-6]</sup>。在 LTE 上行覆盖设计中,干扰余量作为网络规划的核心依据之一,直接取决于功率控制方法、应用场景等因素,并需要通过系统级仿真对不同环境下的干扰进行深入研究,为上行覆盖规划提供较为贴近实际应用的参考设置。

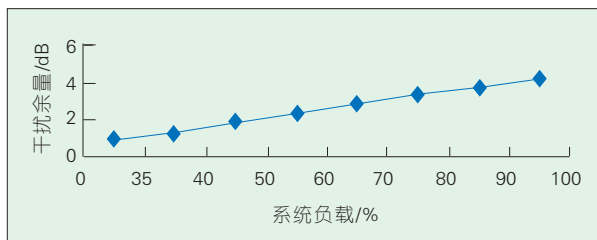
根据建网侧重点的不同,上行干扰特征会受到功率控制策略等方面因素的主导。对于 LTE 系统,上行干扰特征最直接的衡量就是平均干扰抬升(IOT)。因此上行 IOT 的分布特征取决于实际的应用场景及上行功率控制参数。LTE 上行功率控制分为开环功控和闭环功控。一般情况

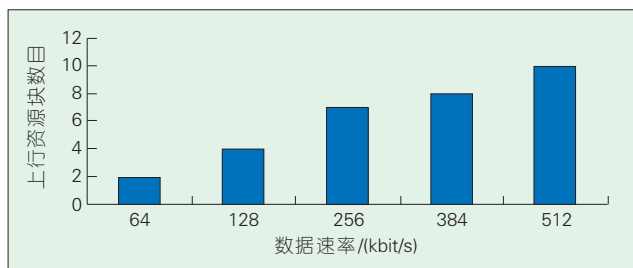
下,系统的开环功控基本决定了系统的干扰模式,闭环功控主要用在实际的网络运行中根据业务及干扰的变化对系统参数进行适当的调整。具体来看,开环功率控制主要通过对功控参数  $P_0$  和  $\alpha$  的确立来满足特定的网络设计需求,不同的参数集合会带来不同的网络覆盖和容量特征。为满足实际规划的需求,需要在不同的应用场景下对上述参数进行深入的研究和分析,总结出满足特定要求的参数,同时在相应的参数设置下研究系统的干扰特征,即平均 IOT,并分析相应的上行干扰余量。基于上述分析,不同的参数会带来差异化的系统性能指标及干扰特征,在实际的规划过程中要根据实际情况进行合适的选择,如图1所示。

在 LTE 系统的建网初期,网络设计主要关注的是覆盖。根据上述讨论,在以覆盖准则为导向的规划设计中,可以设计相应的功控参数来满足覆盖的最大化(降低干扰),由于网络负载的设计目标各不相同,需考虑不同负载下的网络干扰水平,以此作为覆盖规划的参考依据,如图2所示。

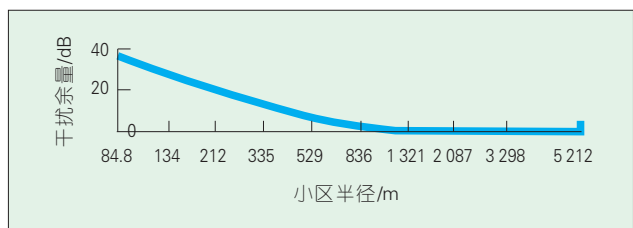
在链路研究方面,该设计主要考虑的是给定数据速率下用户带宽的优化配置。对于特定的边缘数据速率需求,可以通过给用户分配不同的带宽来实现,但同时会带来不同的覆盖性能。通过对信道容量的研究及链路级仿真结果系统性的全面分析,在给定的数据速率要求下,对配置带宽的优化可以增强业务的覆盖性能。该设计是根据链路仿真及实际系统测试中对链路性能的分析,从终端功率使用效率出发,对特定的业务速率、不同用户带宽分配下的性能进

图2 ▲ 上行干扰余量与系统负载的关系





◀ 图3  
给定数据速率下的上行  
带宽配置示例



◀ 图4  
下行干扰余量与小区  
覆盖的关系

行深入的分析。在此基础上,不同的业务速率需求,可以得到优化的上行占用带宽,实现较好的覆盖性能,如图3所示。

以上分别从系统及链路两个方面确定了上行链路预算的核心内容:干扰余量及上行发射带宽(与之对应的调制编码格式及目标信号与干扰噪声比由链路仿真给出)。在此基础上可以根据传统的链路预算、计算方法计算出给定边缘数据速率下的上行最大允许路径损耗(MAPL)。

### 3 LTE 下行覆盖规划关键技术

与上行类似,下行覆盖规划设计包含系统及链路两个方面的研究,其中链路技术的研究主要是通过不同链路设置,如调制编码格式(MCS)、带宽等下的链路仿真,分析不同信道环境、业务速率对链路质量(载干比)的需求,以此作为覆盖规划的依据;系统级的研究方面,主要是依托系统仿真,对覆盖区域中不同位置的接收信号强度、干扰强度、干扰余量、载干比等在不同应用场景及覆盖范围下进行深入的仿真分析:一方面研究传统的基于干扰余量的链路预算方案的局限性,另一方面,建立在信号与干扰之间的纽带,对现有的覆盖规划思路作进一步改进。

LTE下行干扰情况受到组网方式(干扰协调方式)、系统负载等因素的影响,并且随着小区半径的变化而变化。同时,链路预算中的关键参量干扰余量也随之变化,如图4所示。由于干扰余量与小区半径的强相关性,传统的基于给定干扰余量计算小区半径的思路已不再适用于现行情况,需要重新寻找相对比较稳定的中间参数来分析。

经过大量的系统分析,几何因子(GF, GF=本邻小区信干扰之比)以其

独到的特性为下行链路预算提供了一个理想的桥梁。在满负载(100%)全同频组网(Frequency Reuse Factor=1)的情况下,通过对不同小区半径下的几何因子累积分布函数(CDF)可以看出:在不同的覆盖半径下,几何因子的分布几乎重合(如图5所示),该特征为LTE下行链路预算提供了一个稳定的中间参数。

在网络设计中,一般选取95%的区域覆盖所对应的几何因子作为覆盖规划的参考依据,在全同频组网、满负载条件下,如图6中仿真结果,几何因子为3 dB。实际组网中的设计目标不同,因此需要考虑不同系统负载下几何因子的差异性,并以此作为相应负载条件下的参考取值,通过利用几何因子,在下行覆盖分析中,可以在干扰噪声比(SINR)间建立起明确的数学关系。具体来看,在实际的链路预算中,根据特定的需求确定下行边缘所需要的 SINR,并在此基础上计算出边缘所需的最低接收信号强度,根据基站的发射功率,可以计算得出 MAPL(如公式1—3)。

$$SINR_{require} = \frac{S_{require}}{1+N} = \frac{S_{require}}{GF \times S_{require} + N} \quad (1)$$

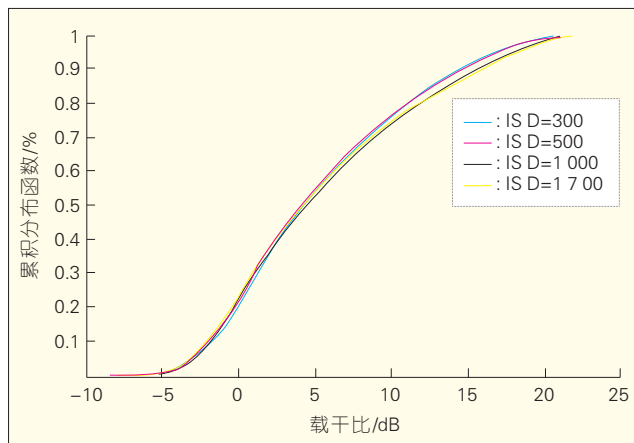


图5 ▶  
下行几何因子累计分布  
函数

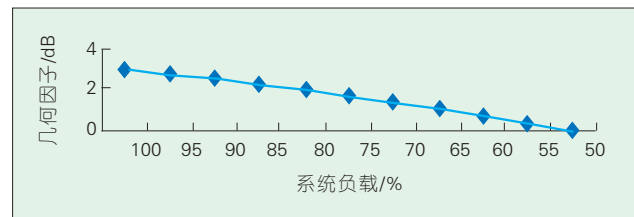


图6 ▶  
几何因子与系统负载

$$S_{\text{require}} = \frac{SINR_{\text{require}} \times N}{1 - G \times SINR_{\text{require}}} \quad (2)$$

$$MAPL = P - S_{\text{require}} - sh\_margin - Loss + Gain \quad (3)$$

其中  $SINR_{\text{require}}$  是目标信干噪比,  $S_{\text{require}}$  是接收端需要的最小接收功率,  $P$  为基站发射功率,  $sh\_margin$  为阴影余量,  $Loss$  为包括馈线损耗在内的所有设备损耗,  $Gain$  为包含天增增益在内的所有设备增益。

#### 4 结束语

LTE 的开放性及其灵活性给网络设计带来了极大的挑战,从整个业界来看,对于 LTE 实际组网的研究处于初步的探索阶段。文章通过对 LTE 网络规划流程和需求的理解,结合覆盖规划中关键技术分析及对系统特征的深入研究,一方面给出了 LTE

覆盖在不同需求下的规划思路,为商业需求到技术需求的转化提供了明确的指导;另一方面,提出 LTE 系统上下行链路预算的整体技术思路、关键参数的取值分析及应用方法,为 LTE 实际网络的设计奠定了初步的理论基础和应用指导。

#### 5 参考文献

- [1] SESIA S, TOUFIK I, BAKER M. LTE .The UMTS Long Term Evolution[M]. New York, NY, USA: John Wiley & Sons, 2009.
- [2] 3GPP TS36.300. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Overall Description[S]. 2008.
- [3] 3GPP TS 36.213. Evolved Universal Terrestrial Radio Access (E-UTRA): Physical Layer Procedures[S]. 2008.
- [4] SYED Abdul Basit. Dimensioning of LTE Network[D]. Helsinki, Finland: Helsinki University of technology, 2009.
- [5] QUINTERO N J. Advanced Power Control for UTRAN LTE Uplink[D]. Barcelona, Italy: University of Catalonia, 2008.

- [6] MUHAMMAD B. Closed Loop Power Control for LTE Uplink[D]. Aalborg, Denmark: Aalborg University, 2008.

收稿日期: 2010-10-14

#### 作者简介



顾军, 北京邮电大学毕业; 现任中兴通讯 CDMA&LTE 产品支持部三级主任工程师; 长期从事 3G、B3G 系统关键技术研究, 目前在从事 LTE FDD 网规网优相关技术的工作; 已发表学术论文 2 篇, 拥有国际专利 1 项, 国家专利 5 项。



盛勃, 合肥工业大学毕业; 现任中兴通讯服务规划部一级主任工程师、LTE FDD 产品总监; 长期从事移动通信网络规划及优化研究, 目前从事 LTE FDD 产品服务规划的相关工作。

#### 上接第 52 页

一代通信网络发展的必然趋势, 对于保障复杂异构网络的性能有着重要的意义和实用价值。

文章提出基于业务感知的认知网络 QoS 自适应控制架构, 在业务感知基础上实现认知网络 QoS 自适应控制。该架构可以看作解决下一代网络端到端 QoS 保证问题的一种新的探讨, 其部分技术已经应用于国家“863”项目——“基于网络行为模型的认知网络 QoS 关键技术”的实验平台, 并形成监测设备应用于某电信运营商的网络优化中, 体现了良好的技术实用性和系统稳定性。

#### 5 参考文献

- [1] 林闯, 单志广, 任丰原. 计算机网络的服务质量 (QoS) [J]. 北京: 清华大学出版社, 2004.
- [2] 林闯, 王元卓, 任丰原. 新一代网络 QoS 研究[J]. 计算机学报, 2008, 31(9): 1525-1535.
- [3] MITOLA J, MAGUIRE G Q. Cognitive radio: Making Software Radios More Personal[J]. IEEE Personal Communications, 1999, 6(8): 13-18.
- [4] THOMAS R W. Cognitive Networks[D]. Blacksburg, VA, USA: Virginia Polytechnic and State University, 2007.
- [5] CLARK D D, PARTTRIGE C, RAMMING J C, et al. A Knowledge Plane for the Internet [C]// Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM '03), Aug 25-29, 2003, Karlsruhe, Germany. New York, NY, USA: ACM, 2003: 3-10.
- [6] THOMAS R W, FRIEND D H, DASILVA L A, et al. Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives[J]. IEEE Communications Magazine, 2006, 44(12): 51-57.
- [7] BALDO N, ZORZI M. Fuzzy Logic for Cross-Layer Optimization in Cognitive Radio Networks[J]. IEEE Communications Magazine, 2008, 46(4): 64-71.
- [8] SIEBERT M. Self-X Control in (future) Mobile Radio Networks [C]// Proceedings of the European-Chinese Cognitive Radio Systems Workshop, May 26-27, 2008, Beijing, China.
- [9] FORTUNA C, MOHORCIC M. Trends in the Development of Communication Networks: Cognitive Networks[J]. Computer Networks, 2009, 53(9): 1354-1376.
- [10] 邵飞, 汪李峰, 伍春. 基于认知层的认知网络结构及其认知方法[J]. 北京工业大学学报, 2009, 35(4): 1181-1187.
- [11] FRIEND D H. Cognitive networks: Foundations to Applications[D]. Blacksburg, VA, USA: Virginia Polytechnic Institute and State University, 2009.
- [12] BALAMURALIDHAR P, PRASAD R. A Context Driven Architecture for Cognitive Nodes[J]. Wireless Personal Communications, 2008, 45(1): 423-434.
- [13] SRIVASTAVA V, MOTANI M. Cross-Layer Design: A Survey and the Road Ahead[J]. IEEE Communications Magazine, 2005, 43(12): 88-95.
- [14] PITCHAIMANI M, EWY B J, EVANS J B. Evaluating Techniques for Network Layer Independence in Cognitive Networks[C]//

- Proceedings of the IEEE International Conference on Communications (ICC '07), Jun 24-28, 2007, Glasgow, UK. Piscataway, NJ, USA: IEEE, 2007: 6527-6531.

收稿日期: 2010-12-06

#### 作者简介



顾成杰, 南京邮电大学信息网络技术研究所读博士研究生, 主要研究方向为通信网与 IP 技术、分布式网络管理、认知网络。



张顾硕, 南京邮电大学教授、博士生导师; 中国通信学会会士兼 IP 应用与增值电信技术委员会主任、中国电子学会通信分会副主任、江苏省通信与网络技术工程研究中心主任; 主要研究方向为计算机网络通信、通信网与 IP 技术。



孙雁飞, 南京邮电大学博士、副教授、硕士生导师; 主要研究方向为网络性能监测与优化、QoS 控制与管理、多媒体网络通信。



# 分组通信网的同步与定时技术

1

王文鼎,王斌,糜正琨

(南京邮电大学 通信与信息工程学院,江苏 南京 210003)

[编者按] 分组通信网同步与定时,其技术需求源于分组网与传统通信网的互连互通,是分组网承载电路仿真业务和实时型业务的前提条件,是移动回传网、音视频桥和无线传感网等应用的关键技术之一。无线分组网的定时与同步,面向无线传感网和物联网的控制与应用,具有广阔的发展前景。本讲座从技术发展、有线和无线环境3个方面,分期论述分组网同步与定时技术:第1讲概要介绍同步与定时的技术概念、需求和现状,第2讲着重讨论以太网为主的同步技术标准,第3讲对无线分组网的同步算法及性能进行综述和介绍。

中图分类号:TN929.11 文献标志码:A 文章编号:1009-6868(2011)01-0057-04

**同**步是通信系统和通信网的基本技术之一。以固定时分复用(TDM)技术为基础的公众电话交换网(PSTN),其同步质量主要通过专门的数字同步网来保障<sup>[1]</sup>;以异步复用技术为基础的分组通信网,对同步的质量要求远低于TDM系统,就传送而言,并无全网同步的需要。通信网在向分组化演进的今天,TDM业务的分组化承载、TDM系统与分组网的互通、新型实时业务的创新,对分组通信网提出了同步与定时的要求<sup>[2]</sup>。

## 1 同步与定时的技术概念

### 1.1 时钟技术

#### (1) 时钟种类

时钟产生的时钟信号,单位时间内相对理想时钟的偏差称为准确度,相对自身平均频率的偏差称为稳定度。在通信技术中得到应用的时钟,主要有:原子钟、石英钟和卫星钟。卫星钟同步于卫星发送的原子钟信号,并不是一种独立运行的时钟。

原子钟利用了原子核超精细能级的稳定性,以能级跃迁过程中吸收或发射的微波频率作为时钟振荡源

的参考。原子钟有非常好的稳定性。2010年,基于铝(Al)原子的原子钟创造了稳定度达 $8.6 \times 10^{-18}$ 的最高记录<sup>[3]</sup>。目前,常规的高精度原子钟基于铯(Cs)、铷(Rb)的同位素,精度好于 $10^{-8}$ 。

石英钟以石英晶体片的压电效应作为产生周期信号的物理基础,它通过调整交变电压的频率,与固定尺寸石英晶体的机械振动达到谐振,从而产生较为精确的时钟频率。石英钟的频率稳定度很宽,在 $10^{-12} \sim 10^{-4}$ 范围之内,工艺、温度和老化是影响稳定度的主要因素,可参考如表1所示的常见时钟性能参数。虽然精度远低于原子钟,但由于在价格和集成化方面具有显著优势,石英钟是信息通信设备的首选元器件。

#### (2) 时钟同步

在一段物理链路两端,收端正确判决发端信息数据的前提是触发判决的时钟信号,其相位同步于接收信号中的时钟信号。这种作用于一段链路的同步称为位同步。

图1给出了收端接收数字信息的功能结构。其中,本地时钟触发读出模块从缓冲存储器读取位信息。当本地时钟慢于接收时钟,即收端时钟慢于发端时钟,会产生周期性的漏读现象,如图2所示。当收端时钟快于发端时钟,则会产生周期性的多读现象。这两种因时钟频率失步产生的数字损伤,称为滑动。

在PSTN系统中,以复用帧(比如E1/DS1帧)为单位完成收发处理,帧头对位显得尤为重要。通过设置一定量的缓存器,可以减少失步损伤的影响程度,这种方法称为帧同步。国

▼表1 常见时钟的性能参数

时钟类型	稳定度	准确度	技术成本
铯原子钟	$10^{-12} \sim 10^{-11}$	$10^{-12} \sim 10^{-11}$	高
铷原子钟	$5 \times 10^{-10} \sim 5 \times 10^{-9}$	$10^{-9}$	中
石英钟	$1.0 \times 10^{-5} \sim 2.0 \times 10^{-5}$	$10^{-5} \sim 10^{-4}$	极低
温控石英钟	$2 \times 10^{-6} \sim 5 \times 10^{-6}$	$10^{-6}$	较低
GPS钟	$10^{-13}$	$4 \times 10^{-8} \sim 10^{-11}$	低
GPS: 全球定位系统			

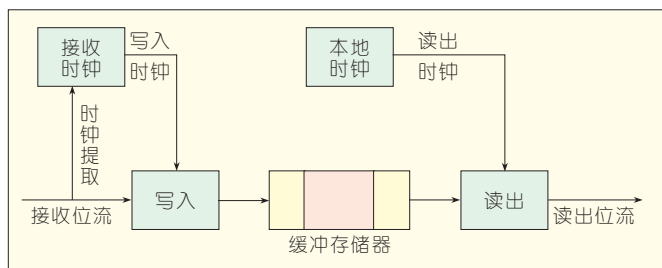


图1  
固定时分复用通信设备接收数据的处理功能结构

际电信联盟(ITU)制订了一系列建议,规范通信网络的同步性能指标,以满足通信业务的质量要求。

## 1.2 网同步方式及性能指标

### (1) 网同步方法

为达到全网范围内的时钟同步,需要综合考虑业务需求、时钟性能、成本、可靠性、安全性等技术要求。对地理分布广、采用分级管理的通信运营企业,一般采用主从同步或外基准同步的网同步方法。

所谓主从同步,就是在通信网中部署少量高性能时钟设备(比如铯钟),通过专用的数字传输链路将高性能时钟信号直接传送给网中的其他时钟设备,以便后者跟踪于前者。提供时钟信号的设备称为主时钟;接收时钟信号并跟踪于主时钟的设备称为从时钟。对于大规模网络,通常部署三级主从同步网络,因此,时钟设备细分为一级参考钟(PRC)、区域参考钟(LPR)、二级钟和三级钟<sup>[4]</sup>。

外基准同步是主从同步的一种特殊形式,主时钟部署在定位卫星上,或者部署在地面通过卫星上时钟简接提供时钟参考,同步信号通过无线方式传递到地面接收设备。

### (2) 时钟同步性能

同步网的主时钟以自由方式运行,稳定度和准确度是衡量其性能的主要参数。对从时钟而言,正常工作时需要同步跟踪于主时钟,而当时钟信号中断时,则需要能类似于记忆的形式工作,因此从时钟的工作模式包括:自由运行方式、跟踪方式和保持方式。

从时钟的同步跟踪能力,通过牵

引范围来度量,它是指从时钟能够锁定的输入时钟信号最大频率变化范围。输入信号频率超出此范围,从时钟失去跟踪能力。进一步细分,可以把从不能跟踪进入到能跟踪的牵引范围,称为牵引引入范围;而把从能跟踪进入不能跟踪的牵引范围,称为牵引引出范围。

在实际应用中,稳定度和准确度两个参数不能反映短时间内的时钟质量。为此,引入时间间隔误差(TIE)来度量准确度的时变特性,并把短周期(变化频率大于10 Hz)的TIE称为抖动,长周期(变化频率小于10 Hz)的TIE称为漂移。

## 2 分组通信网的同步需求

### 2.1 电路仿真的同步需求

通过分组网提供传统TDM业务的承载服务,以保证现有网络的平滑演进,这种业务称为电路仿真业务(CES)<sup>[5]</sup>。CES最早出现在异步传输模式(ATM)技术中,通过互连功能装置或设备实现分组网与PSTN的互通,目前被延伸到电信级以太网等分组

传送网。

虽然分组网本身采用异步通信方式,并不需要全网同步,但为满足与PSTN互通的质量要求,同步是不可少的。实际应用中存在3种CES部署结构:第1种部署在骨干网,并与TDM形成串接;第2种部署在接入网;第3种则单独构成骨干网。表2中列出了ITU-T G.8261给出的时钟质量指标。

### 2.2 移动回传的同步需求

移动回传位于小区基站和基站控制器(BSC)之间,它将分布的小区或小区汇聚点连接到BSC及核心网。在以TDM为基础的PSTN/2G网络中,时钟传递并不是主要问题,这是因为TDM已具有较好的同步机制。在以分组传送网为基础的移动回传中,同步性能不能得到保证,可能影响话音业务质量、越区切换和干扰控制,易导致业务中断、业务质量劣化、频谱效益下降<sup>[6]</sup>。

表3列出了不同移动技术的同步与定时需求。全球移动通信系统/宽带码分多址(GSM/WCDMA)采用异步基站技术,只需要做频率同步,精度要求0.05 ppm。而码分多址(CDMA)/CDMA 2000、时分同步码分多址(TD-SCDMA)、长期演进(频分双工)(LTE(TDD))和全球微波互联接入(WiMAX)中,空口技术采用同步基站方案,需要做时钟的相位同步,同步的精度分别为3 μs、1.5 μs、2.5 μs

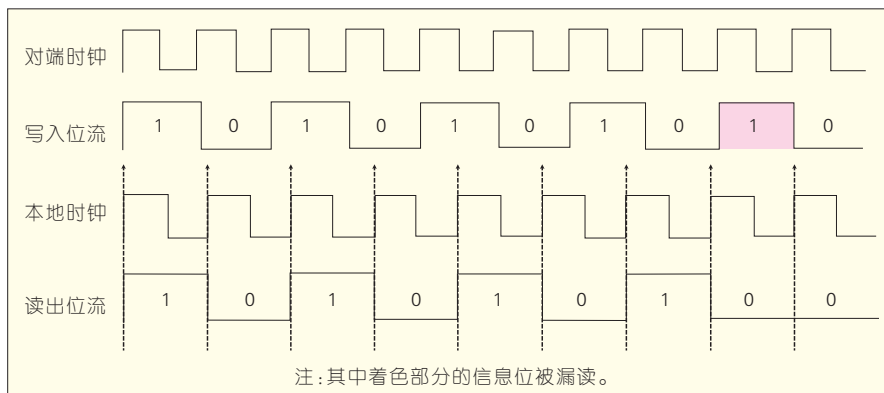


图2 本地时钟慢于对端时钟时滑动的时序

▼表2 分组通信网 CES(2 048 kbit/s 接口)的时钟质量要求

部署类型	时间间隔/s	MTIE/ $\mu$ s
类型1:与TDM串接	$0.05 < \tau \leq 0.2$	$10.75 \tau$
	$0.2 < \tau \leq 32$	2.15
	$32 < \tau \leq 64$	$0.067 \tau$
	$64 < \tau \leq 1\,000$	4.3
类型2:接入网	$0.05 < \tau \leq 0.2$	$40 \tau$
	$0.2 < \tau \leq 32$	8
	$32 < \tau \leq 64$	$0.25 \tau$
	$64 < \tau \leq 1\,000$	16
类型3:单独承载	—	—
CES:电路仿真业务 MTIE:最大时间间隔误差 TDM:固定时分复用		

▼表3 移动回传网的同步与定时需求

移动技术	时钟频率要求/ppm	时间同步要求/ $\mu$ s
GSM	0.05	—
WCDMA	0.05	—
CDMA 2000	0.05	3
TD-SCDMA	0.05	1.5
LTE(FDD)	0.05	—
LTE(TDD)	0.05	2.5
WiMAX	0.05	1
CDMA:码分多址 GSM:全球移动通信系统 LTE(FDD):长期演进(频分双工) TDD:时分双工 TD-SCDMA:时分同步码分多址 WCDMA:宽带码分多址		

和 1  $\mu$ s。

步质量规范要求。

2.3 专业级多媒体音视频桥的同步需求

以太网技术所具有的高带宽特性,促进了它在高端多媒体领域内的应用,包括专业级音视频的应用场合,如大型体育运动会、会展中心和音乐厅等。但传统局域网设备不能满足实时多媒体的应用需求。为此,IEEE 802.1AVB 工作组开展标准化工作,涉及系统体系结构、定时同步、传送质量控制、桥接传输等<sup>[7]</sup>。

AVB 应用的网络结构如图 3 所示,其中“AVB 云”由支持 AVB 协议的以太网桥、无线 AP 和终端组成。AVB 终端包括音视频服务器、分布的音频和视频播放设备等,其上时钟为普通时钟。无线 AP 的时钟为边缘时钟,AVB 网桥的时钟为点对点(P2P)透明时钟。表 4 说明了 AVB 业务的同

2.4 无线传感网的同步需求

无线传感网(WSN)通过 WiFi 和 ZigBee 等无线通信手段,连接数量大、分布广、环境复杂的传感器,通常需要将传感测量的数据进行汇总,并用于向分布的控制器传送控制信息。

WSN 所进行的数据汇总,时间同

步是重要前提之一。研究表明<sup>[8]</sup>,WSN 的频率稳定度要求小于 1%,频率准确度要求则小于 1 000 ppm。根据应用的不同,定时信号的抖动要求在 1 ms~n min,漂移要求在 1 ms~1 min。

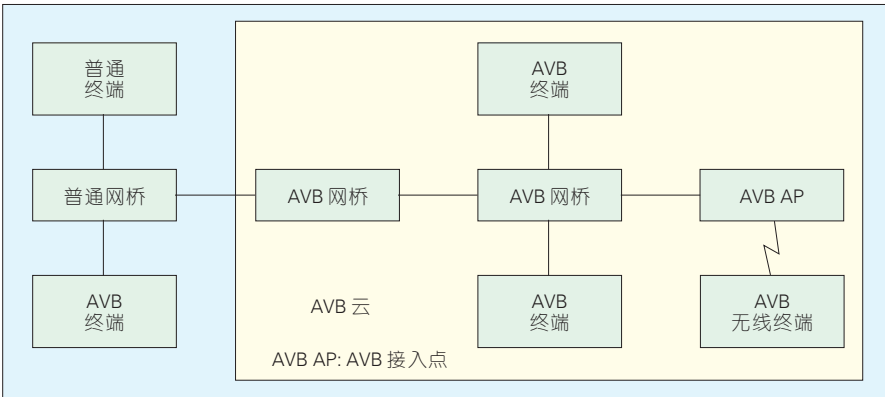
由于 WSN 节点通常使用共同的无线通信资源,在节点数较多时,无线资源的合理分配成为提高通信容量的主要手段。以 WiFi 为例,在同一冲突信道内,如不同节点交替占用信道,则需要节点间达到准确同步。对于数据帧长小于 200  $\mu$ s 的无线局域网<sup>[9]</sup>,如同步准确度小于 200  $\mu$ s,则可实现通信资源的高效分配。

3 分组网同步技术及应用

3.1 网络时间协议

网络时间协议(NTP)是一个最早的 IP 分组网时钟同步协议,于 2010 年 6 月成为 Internet 工程任务组(IETF)的建议标准。NTP 同步系统采用分级组织结构,顶层(Stratum 0)为高精度原子钟或 GPS 时钟,第 1 层(Stratum 1)时钟直接同步于顶层参考时钟源,并向第 2 层(Stratum 2)时钟提供定时服务,依次向下,最多可达 256 层。

NTP 服务器之间可采用 3 种方式校时,包括:广播/组播方式、对称方式和客户机/服务器方式。其中,广播/组播方式适用于局域网环境,对称方式适用于同层服务器之间,而客户机/服务器方式适用于上下层服务器之间<sup>[10]</sup>。



▲图3 AVB结构及其与普通以太网的关系



▼表4 AVB业务及接口的同步与定时需求

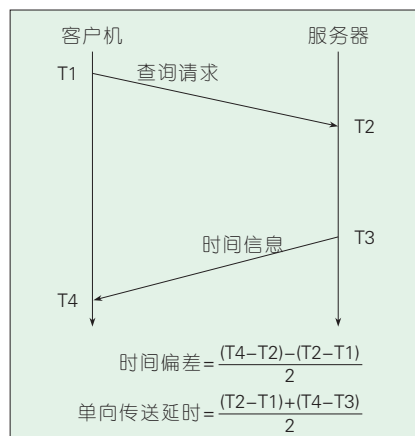
性能	无压缩 SDTV	无压缩 HDTV	网络传送的 MPEG-2	用户接口 数字音频	用户接口 数字视频
宽频抖动	0.2 Ulpp	1.0 Ulpp	50 $\mu$ s (峰峰相位差)	0.25 Ulpp	0.25 Ulpp
高频抖动	0.2 Ulpp	0.2 Ulpp	50 $\mu$ s (峰峰相位差)	0.2 Ulpp	—
频偏/ppm	$\pm 2.79365$ (NTSC)	$\pm 10$	$\pm 30$	$\pm 50$ (1级)	$\pm 1$ (1级)
	$\pm 0.225549$ (PAL)	—	—	$\pm 1\ 000$ (2级)	$\pm 10$ (2级)
频漂/ppm	0.027937(NTSC)	—	0.000278	—	—
	0.0225549(PAL)	—	—	—	—
HDTV: 高清晰度电视 MPEG: 动态图像专家组 NTSC: 美国国家电视标准委员会 PAL: 逐行倒相(制)					
SDTV: 标准数字电视					

NTP 采用 Marzullo 算法完成时间校时,其基本计算原理可用图4来说明。客户机向服务器发送查询请求,并记录发送时的本地时钟值 T1;服务器在收到请求后,记录收到时的本地时钟值 T2,并回应时间信息,将 T2 和发送该信息的时间 T3 返回给客户机;客户机收到时间信息后,记录收到时的本地时钟值 T4。通过简单计算,可在客户机一侧得到单向传送延时和时间偏差,客户机就可以调整本地时间,实现与服务器的同步。

### 3.2 精确时间协议

IEEE 1588 工作组自 2002 年开始制订精确定时协议(PTP),并于 2008 年发布了第 2 版本<sup>[11]</sup>。PTP 最初面向控制和测量的应用需求,用于增强局域网的同步定时性能,目前主要应用于以太网之中,因此也被称作工业以太网。

与 NTP 相比,PTP 同步控制过程



▲图4 NTP校时流程

需要4次握手,且用于同步计算的时间值均要求取自物理层,以减少软件处理产生的抖动,并避免局域网内冲突及回退所产生的干扰。PTP的从时钟,其准确度可达亚微秒量级,远好于NTP。但与NTP一样,PTP不能保证短期稳定性,也不能直接提供频率同步。

### 3.3 同步以太网

ITU 分别于 2006 年和 2007 年发布了 G.8261/Y.1361 和 G.8262/Y.1362 建议,明确了同步以太网的概念、体系结构和性能要求,规定了同步以太网网络设备中使用的时钟最低性能指标。

同步以太网通过以太网物理层传送时钟信号,通常以专用方式独占以太网设备的物理端口,并支持类似于 TDM 的线路编码方式传送时钟信号。同步以太网设备可选用的时钟信号输入输出接口,包括 2 048 kHz、2 048 kbit/s、STM-N 等传统 TDM 接口和同步以太网接口。

同步以太网提供时间频率同步,采用专用接口传送时钟信号时,同步的准确度可优于 10 ns,但时间同步需要采用其他技术手段。同步以太网是电信以太网的重要基础之一,有望在移动回传和分组传送网中得到应用。

(待续)

### 4 参考文献

- [1] YD/T 1012-1999. 数字同步网节点时钟系列及其定时特性[S]. 1999.
- [2] 李勤. PTN 时钟同步技术及应用[J]. 中兴通讯

技术, 2010, 16(3):26-30.

- [3] CHOU C W, HUME D B, KOELEMIEJ J C J, et al. Frequency Comparison of Two High-Accuracy All-Optical Clocks[J]. Physical Review Letters, 2010, 104(7): 070802.
- [4] YD/T 5089-2005. 数字同步网工程设计规范[S]. 2005.
- [5] ITU-T G.8261/Y.1361. Timing and Synchronization Aspects in Packet Networks[S]. 2006.
- [6] Juniper Networks Inc. Mobile Backhaul Reference Architecture[EB/OL]. <http://www.juniper.net/us/en/local/pdf/reference-architectures/8030008-en.pdf>, 2010.
- [7] IEEE 802.1Qav. Standard for Local and Metropolitan Area Networks--Virtual Bridged Local Area Networks Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams[S]. 2010.
- [8] RODRIGUES S, LINDQVIST K. TICTOC Requirement[R]. draft-ietf-tictoc-requirements-00. 2009.
- [9] IEEE 802.11. Wireless Local Area Networks[S]. 2007.
- [10] Mills D, Martin J, Burbank J, et al. Delaware Network Time Protocol Version 4: Protocol and Algorithms Specification[R]. IETF RFC5905. 2010.
- [11] IEEE 1588. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems[S]. 2008.

收稿日期: 2010-11-23

### 作者简介



王文骥, 南京邮电大学教授, 南京大学博士毕业; 现从事新一代网络技术方面的教学与科研工作; 公开发表的学术论文超过 50 篇, 近 30 篇被 SCI/EI 检索。



王斌, 南京邮电大学副教授, 北京邮电大学博士毕业; 现从事低轨道卫星通信、LTE 移动通信、电信级以太网保护和高性能交换等方面的教学和科研工作; 公开发表论文 12 篇, 其中 5 篇被 SCI/EI 检索, 申请国内发明专利 31 项, 申请国外发明专利 8 项。



糜正琨, 南京邮电大学教授、博导; 目前主要研究方向为下一代网络技术和异构网络融合技术; 曾获江苏省科技进步二等奖一项, 信息产业部科技进步二等奖和三等奖各一项; 已发表 SCI、EI 收录论文 40 余篇, 出版专著和国家级教材 8 部, 申请国家发明专利 4 项。