移动通信高新技术系列丛书

UMTS安全

Valtteri Niemi Kaisa Nyberg 著
宋美娜 宋梅 周文安 译

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

UMTS 安全

Valtteri Niemi　Kaisa Nyberg　著

宋美娜　宋　梅　周文安　译

宋俊德　审校

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

北京市版权局著作权合同登记号：01-2004-1383 号

版 权 声 明

图书在版编目（CIP）数据

UMTS 安全/（美）尼米（Niemi, V.），（美）纽伯格（Nyberg, K.）编著；宋美娜等译. —北京：中国铁道出版社，2005.6
（移动通信高新技术系列）
ISBN 7-113-06574-0

Ⅰ.U... Ⅱ.①尼...②纽...③宋... Ⅲ.移动通信—通信网—安全技术 Ⅳ.TN929.5

中国版本图书馆 CIP 数据核字（2005）第 067524 号

书　　名：UMTS 安全
作　　者：Valtteri Niemi Kaisa Nyberg
译　　者：宋美娜　宋　梅　周文安
审　　校：宋俊德
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：严晓舟　郭毅鹏
责任编辑：苏　茜　严　力
特邀编辑：刘　柳
封面设计：薛　为
封面制作：白　雪
责任校对：李　旸
印　　刷：河北省遵化市胶印厂
开　　本：787×960　1/16　印张：15.75　字数：334 千
版　　本：2005 年 11 月第 1 版　　2005 年 11 月第 1 次印刷
印　　数：1～4 000 册
书　　号：ISBN7-113-06574-0/TP・1533
定　　价：30.00 元

移动通信高新技术系列丛书审校委员会

主审：

宋俊德　（北京邮电大学教授、博士生导师，北京邮电大学学位委员会主席、原研究生院院长）

朱近康　（中国科学技术大学教授、博士生导师）

龚　克　（清华大学教授、博士生导师，清华大学副校长）

委员：（排名不分先后）

王文博　（北京邮电大学教授、博士生导师，北京邮电大学电信工程学院院长）

王　京　（清华大学教授、博士生导师，清华大学信息科学技术学院副院长）

张　平　（北京邮电大学教授、博士生导师，北京邮电大学无线通信新技术实验室主任）

李承恕　（北京交通大学教授、博士生导师，北京交通大学现代通信研究所名誉所长）

李少谦　（成都电子科技大学教授、博士生导师，成都电子科技大学通信与信息工程学院副院长）

刘元安　（北京邮电大学教授、博士生导师，北京邮电大学科技处处长）

杨大成　（北京邮电大学教授、博士生导师，无线通信中心主任）

范平志　（西南交通大学教授、博士生导师，西南交通大学计算机与通信工程学院院长）

周祖成　（清华大学教授、博士生导师）

李正茂　（博士，中国联合通信有限公司副总裁）

苏东林　（北京航空航天大学教授、博士生导师，北京航空航天电子信息工程学院副院长）

彭木根　（北京邮电大学移动通信专业博士）

宋美娜　（北京邮电大学博士）

丛书序

当今的社会已经进入了一个信息化的社会，没有信息的传递和交流，人们就无法适应现代快节奏的生活和工作。人们期望能随时随地、及时可靠、不受时空限制地进行各种信息交流，以提高工作效率和生活质量。

移动通信可以说从无线电发明之日就产生了，但移动通信的真正发展是在蜂窝移动通信正式商用化的20世纪70年代以后的事情。目前，移动通信是当今发展最快、应用最广和最前沿的通信领域之一，据专家估计，到2006年全球移动用户数有望突破20亿。随着通信技术不断的发展，移动通信正朝着为用户提供集语音、数据、多媒体业务为一体的第三代（3G）移动通信演进，向人们勾画了一幅实现人类在任何时间、任何地方、进行任何种类的通信（语音、数据和图像）的多彩画卷。

第三代移动通信技术以WCDMA为代表，它将为用户提供高速数据传输、因特网访问、移动视频业务和多媒体服务，同时支持全球漫游特性。目前3G无线系统遇到的各种困难已经基本解决并且已经可以投入生产和运营，但与此同时，无线电委员会已经开始讨论4G即下一代移动通信系统的设计。4G的设计很有可能不仅仅以当前有线无线通信系统的综合为重点，同时也要强调业务和用户的需求。基于这些因素的考虑，也就出现了技术和商业两方面的挑战，当然也有许多技术的解决方法可以帮助4G移动网络成为现实。

3G和4G移动通信业务发展的IP化、分组化、多媒体化、个性化以及生成简单化，在未来的业务生成中，将会形成新的业务链，从而形成运营业、制造业和信息服务业以及消费者组成的新的产业链和价值链，带动运营业、制造业和信息服务业整体产业链的发展。为了促进和推动我国移动通信产业的发展，并不断满足社会各界和广大通信技术人员系统学习和掌握移动通信前沿技术的需要，紧跟国际移动通信技术和网络技术发展的步伐，积极迎接WTO入关带来的各种竞争和挑战，以信息化带动工业化，提高我国通信业整体水平和竞争力，中国铁道出版社特别邀请国际和国内从事移动通信技术研究、教学、工程、策划和管理等工作的权威人士推荐、翻译和编著了这套《移动通信高新技术系列丛书》，以飨读者。

该丛书主要介绍目前移动通信领域的关键技术和热点技术，如通用无线分组业务（GPRS）、第三代移动通信技术、未来移动通信技术发展、移动通信业务、全IP网络技术、移动通信网络规划和优化以及天线技术和无线定位技术等内容。其特点是技术先进、内容权威、知识详实、讲解清晰、深入浅出。本套丛书大部分直接来源于国外的经典著作，已被国际权威人士和广大读者认可。本套丛书旨在帮助读者迅速掌握最先进和最全面的移动通信技术，在实际的工作和科研中学以致用、不断创新，把书本中的知识和解决问题的方法应用到

实际工作或移动通信系统的开发中；产学研相结合，尽早推出更先进、更可靠的中国自己的移动通信系统产品；推动运营企业与制造企业加强合作、相互支持，以达到共同发展，提高运营业和制造业的整体水平竞争力的目的，使我国移动通信朝着稳健、有序、健康的方向发展。

这套丛书的主要读者对象是从事移动通信系统深入研究与开发的电信工程师和工程管理人员，同时对在这个领域进行教学、研究和开发的教师及学生有很好的参考价值，可以作为高等学校相关专业本科生、研究生的教学参考书。

相信这套丛书的出版会为我国移动通信事业的发展贡献微薄之力，在此感谢参与这套丛书审稿、翻译、编著和审定的各位专家，感谢为这套丛书得以出版而付出大量心血的所有工作人员，在此我们表示衷心的感谢和诚挚的敬意。

宋俊德

2004 年 1 月

译者序

近几年来，移动通信产业呈现出了爆炸式的增长态势，它的发展速度异常迅猛。一个个新鲜而又令人兴奋的词汇一直活跃在人们的眼前：2G、3G、4G、WCDMA、CDMA 2000、TD-SCDMA 和 UMTS，每一个词汇代表的都是技术的最前沿。移动通信从最初的只能进行语音通信，发展到在 GPRS 系统中开展低速率的数据通信，进而演进到 3G 最高 2Mbps 的数据传输速率。最近，日本 NTT 公司宣布研制成功速率超过 1Gbps 的 4G 移动通信系统。人们已经开始享受高速的移动通信系统所带来的实惠：移动电子商务、移动流媒体和移动在线游戏已经使得人们可以在 ANYTIME、ANYWHERE 和 ANY-MOTION（任何运动状况）的条件下进行网上交易、收看新闻以及娱乐。现在移动通信正在越来越多地进入人们的生活，用手机看电视、遥控自己家里的各种家电或视频电话，已经不再是梦想。

在舒适地体验着先进的移动通信技术给工作生活带来的好处的同时，通信系统的安全问题也在越来越多地引起人们的注意。只有在安全的通信系统的保障下，各种基于移动通信的工作才能正常开展。谁也不希望自己的通话被窃听、电话被盗打，更不希望自己银行账户密码被窃取。那么，怎样的一个通信系统才是安全的，一个安全的通信系统有哪些要素，怎样才能构建一个安全的通信系统呢？《UMTS 安全》这本书解答了这些问题。

本书将 UMTS 作为讨论的焦点，从 UMTS 的安全结构和安全功能、加密算法的规范和分析两个部分对 UMTS 安全进行了深入的研究。将内容划分为两个部分的好处是，每一个部分可以使用相应的分析问题的方法，从而使得两个部分相对独立，可以分别进行阅读；同时由于安全性和加密之间内在的联系，书中这两个部分也不是截然独立的。第 1 部分由第 1～3 章组成，剩下的章节构成了本书的第 2 部分。第 1 章概括介绍了安全性以及 UMTS 的概念；第 2 章介绍了 UMTS R99 中的安全特性；第 3 章介绍了 UMTS R4 以及 R5 中的安全特性。进入到第 2 部分，本书开始介绍并分析各种加密算法。第 4 章概述了加密技术；第 5 章介绍 3GPP 算法规范原理；第 6 章介绍保密性和完整性算法；第 7 章介绍了核心算法 KASUMI；第 8 章介绍了认证与密钥生成算法。

通过对 UMTS 系统所提供安全服务的统一处理，这本书对 UMTS 网络的规划者、设计者、实现者以及使用 UMTS 通信网络构建服务的开发和分析人员尤为珍贵，并能起到立竿见影的作用。本书同样对从事现代通信安全技术工作的研究生和研究人员大有帮助。

参与本书翻译工作的还有刘鑫、杨旭、欧中洪、刘阳、余群和韩默等北京邮电大学PCN&CAD中心的研究生，同时要感谢编辑严力老师对我们的译文提出的诸多宝贵意见，使得本书能够顺利出版。

由于时间及水平有限，译文中难免有不统一、不确切的地方，欢迎读者批评指正，以便再版时更正。如果您在本书的阅读中遇到任何需要讨论的问题，请同我们联系。我们的邮件地址是 mnsong@bupt.edu.cn。

译者

2005.3.15

前　言

在无线技术中，物理信道从来就不是安全的。一条线缆只有两个端点，有线通信就有方法来保证通信的完整性，而在无线通信中，就需要有一种专用技术控制基本的端到端连接。这项保证通信完整性的技术，构成了现代无线通信系统的重要部分，我们将其称做安全性技术。

本书详细描述了 Universal Mobile Telecommunication System（UMTS，通用移动通信系统）的安全性解决方案。它给出了 UMTS 安全性规范的综合性描述，并且解释了安全性功能在 UMTS 中的角色。首先，本书旨在为整个 UMTS 网络的规划者、设计者和实现者描述 UMTS 安全系统。它还给出了一套统一的我们所希望的由 UMTS 提供的安全服务处理方法，这对 UMTS 通信网络面向应用的安全服务开发者和分析者来说是无价的。本书也可以作为高等院校现代通信安全技术课程的教科书。

为了实现全球通信系统的互联互通，通信系统需要标准化。标准化确保当系统中的实体被不同的移动网络运营商控制或由不同的厂商制造时，他们都能彼此相互通信。然而，允许运营商和制造商之间存在一定程度上的非标准化差别是有必要的。例如，网络实体的内部结构属于非标准化区域。

安全性在标准的和非标准的 UMTS 规范中都是必需的。举个例子，移动电话与无线网络之间的通信是由加密消息保护的。怎样加密和采用哪一种加密密钥一定要使用严格的标准，否则，接收端就不能进行逆操作从而恢复原文。在另一方面，通信双方都不得不严格保存密码，使其不被外来人员得到。这样做是很重要的，但我们对于怎样做并没有制定出标准。本书的重点是放在 UMTS 标准化的安全特性上的，而不是在其他方面。

这本书被分为两个部分，第 1 部分描述了 UMTS 的安全结构和安全功能，而加密算法的规范和分析在第 2 部分介绍，以这样的方式组织本书，我们希望对构建 UMTS 安全系统的两个不同的领域与方法提供不同的处理方法。而每一部分都能够独立地阅读，我们将这两部分内容包含在一本书中，使读者有机会熟悉安全性和加密之间的联系。

本书体现了安全专家组以及致力于安全性工作的个人广泛的、苛求的和积极的工作成果，是他们一起创立了 UMTS 安全规范。它大量吸收了世界上参与这项工作的重要专家们合作和讨论的成果。特别地，我们想向 3GPP SA3、ETSI SAGE 和 3GPP 算法任务组的成员表示感谢，当然还有我们诺基亚的同事们。

最后，我们想要感谢本书的出版商和编辑组，是他们卓越的工作把我们的文字变成了一本连贯的书。

目 录

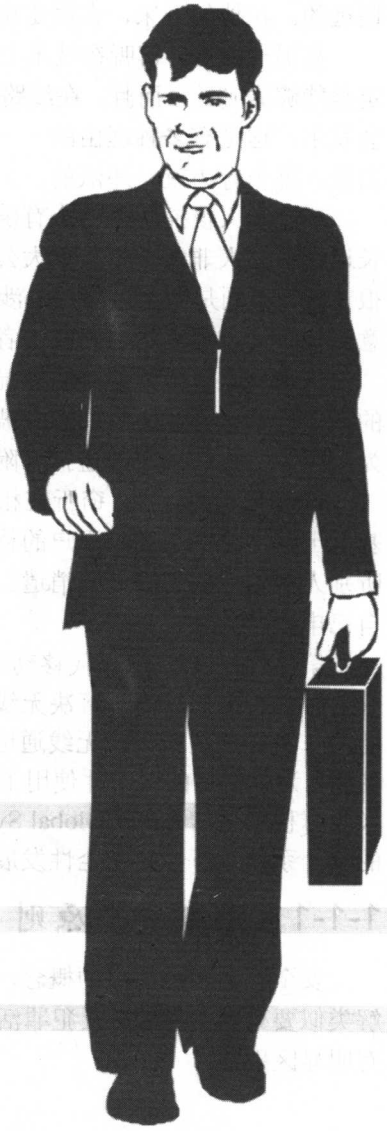
第 1 部分 UMTS 安全结构

第 1 部分

UMTS 安全结构

第 1 章

安全性和 UMTS 导论



UMTS 安全

1-1 通信安全

有线通信网络具有可靠的固有安全属性，网络运营商基本上可以把整个网络包括所有布线都安装在墙上的插槽中，用户可以简单地把终端线插入插槽中。这就意味着运营商可以保证在通话过程中网络配置保持固定，从而使得决定哪个用户该为某次通话付账变得简单。

同样明显的是，没有哪个偶然的旁听者能在固定电话的通话中偷听到谈话。事实上，要进行窃听，必须要放置窃听装置。从一般用户的观点来看，这些威胁的可能性对用户来说是遥远的。在他们看来，在固定电话的通话中是不可能有窃听的。

在另一方面，窃听在技术上没有什么高要求。如果有人真的要听某个用户的通话，也肯定是能够做到的。而且，在线路上安装窃听电话并不是那么困难。而实际上这种事情一般不会发生，这是有多种理由的——这种实行恶性攻击的动机与工作必需的花费是不合比例的，当然，整个行为就是违法的。

一个私人侦探为了一个有嫉妒心理的丈夫或妻子通常很可能去窃听，同样那些需要大量长途通信的人非常希望某个大公司为他们买单。然而，长时间这样做而不引起别人的注意是很难的，特别是如果这种行为涉及很广的范围。如果有人盗打了电话，受害者毫无疑问会注意到什么地方出了错，而攻击者早晚会被抓到。

当使用无绳电话的时候情况会相应地改变。无线通信能够在短距离内被窃听，其被抓到的可能性要比有线通信中盗打被抓到的可能性小得多。但是，盗打电话仍然是一种冒险的行为，因为盗打必须在被盗打者附近进行。

就蜂窝网络而言，窃听在相当大的范围内都是可能的。主动的通话窃听十分简单，网络基本上并不能真正控制用户的移动位置。事实上，在第一代的移动网络中使用模拟技术，窃听别人的电话成为时尚的消遣。同样在某些第一代的模拟系统中，计费仅仅简单的基于用户自己申报所拨打的号码。

第二代（2G，第二代移动通信系统）移动网络用数字技术代替了模拟技术。这就要求有一种全新的工具用于解决无线网络出现的安全问题。事实上，用数字化方法处理信号是可能的（例如，纠错码在无线通道中能被用于减少信道干扰）。在安全的环境下，加密方法被使用，为了通话的保密性使用了加密方法，为了防止电话被窃听应用了加密授权机制。GSM（全球移动通信系统，Global System for Mobile Communication）是最大的 2G 移动网络，它的安全系统是下一代安全性发展的起点。

1-1-1 一般安全原则

安全性是一个抽象的概念，想定义它并不容易，但当提起它时人们总是试图去更好地理解类似要处理的问题。反犯罪活动的保护方案是安全性的核心。安全性与容错性、鲁棒性是有明显区别的。