现代通信网络技术丛书

无线通信网中的安全技术

徐胜波　马文平　王新梅　编著

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

现代通信网络技术丛书

无线通信网中的安全技术

徐胜波　马文平　王新梅　编著

人民邮电出版社

图书在版编目(CIP)数据

无线通信网中的安全技术/徐胜波，马文平，王新梅编著. —北京：人民邮电出版社，2003.7
（现代通信网络技术丛书）
ISBN 7-115-11053-0

Ⅰ. 无… Ⅱ. ①徐…②马…③王… Ⅲ. 无线电通信－通信网－安全技术 Ⅳ. TN92

中国版本图书馆 CIP 数据核字(2003)第 021078 号

内 容 提 要

本书主要介绍无线通信网络中的安全技术。第 1 章对无线通信网中的安全问题作了一般介绍，第 2 章介绍了一些基本的密码知识，第 3 章主要介绍对称密码系统和算法，第 4 章主要介绍非对称密码系统与算法，第 5 章主要介绍认证系统与算法，第 6 章主要介绍密钥分配与管理方案，第 7～9 章分别详细介绍移动通信网络、无线局域网络和无线个人区域网络的安全技术，第 10 章重点介绍无线应用协议所包含的安全技术，并分析其安全性，最后以网上支付为例介绍移动电子商务。

本书适合从事无线通信网络安全工作的工程技术人员和相关专业的学生学习参考，对该方面知识有兴趣的读者也可以阅读参考。

现代通信网络技术丛书

无线通信网中的安全技术

◆ 编　　著　徐胜波　马文平　王新梅
责任编辑　王亚明　李　健

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67129258
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：14.25
字数：340 千字　　2003 年 7 月第 1 版
印数：1-4 000 册　　2003 年 7 月北京第 1 次印刷

ISBN 7-115-11053-0/TN・2022

定价：23.00 元

前　言

无线通信通过空中传播的电磁波在通信双方之间建立连接，为通信用户带来了方便和自由。然而，电磁波在空中传播时很容易被截获，给无线通信带来了许多潜在的威胁，如通信内容可能被窃听、通信对方身份可能被假冒等，这就使得人们更加关注无线通信的安全性。

意大利物理学家 Guglielmo Marconi 发明的无线电报在 20 世纪初期很快就成为了军事通信的手段之一，并在两次世界大战中得到广泛应用。为了防止敌方窃听军事活动的内容，无线电报内容必须进行加密保护。自 1863 年 Kasiski 攻破著名的维吉尼亚(Vigenere)密码之后，世界各国的密码设计者设计了一些新的加密算法，以保护政府部门和军队的通信安全，其中很多加密算法后来也都用于保护军用无线电报的安全。然而，无线电报的广泛应用使得密码分析者可以很容易地获得密文，从而方便了密码分析，并导致一些加密算法的破解，对军事活动的胜败起到了举足轻重的作用。

自 20 世纪 70 年代以来，无线通信在民用通信领域得到了广泛应用。最典型的代表就是移动通信，它已经覆盖全球，可为人们提供无处不在的通信服务。然而，第一代移动通信网络的安全性在其发展初期并没有得到重视。第一代移动通信网络没有采用任何密码技术，导致用户通话很容易被窃听，而且大量的“拷贝”手机充斥市场，给网络运营商和服务提供商造成巨大的经济损失。鉴于上述教训，第二代移动通信网络采用了加密和身份认证技术，来保护移动用户的通话内容，防止非法用户访问移动通信网络，从而在很大程度上提高了移动通信网络的安全性。随着无线通信技术的发展，无线通信网络的应用范围不断扩大，特别是无线局域网络和无线个人区域网络的出现，把无线通信应用带入到工厂、企业、公司、学校和家庭。同时，随着新的无线通信服务的发展，特别是移动电子商务的发展，将无线通信网络的应用与公司、企业和个人的经济活动紧密相连。由此可见，无线通信网络的安全性不但关系到国家政治和军事活动的成败，它也越来越成为决定公司、企业和个人经济活动成败的关键。因此，采用适当的密码技术，保护民用无线通信网络的安全十分必要。

鉴于人们对无线通信网络安全性与日俱增的关注，本书将详细介绍几种无线通信网络(移动通信、无线局域网络和无线个人区域网络)中的安全技术，分析这些网络的安全性，并给出一些改进方法，以便于网络设计人员和管理人员提高网络安全性。为了帮助读者更好地理解无线通信网络中的安全技术，本书的第 1 章首先介绍无线通信网络的特点和其中存在的不安全因素。第 2～6 章将分别介绍一些基本的密码知识和密码算法如：传统单钥密码算法——包括流密码算法和分组密码算法如最新美国数据加密标准 AES，公钥密码算法——包括著名的 RSA 算法和椭圆曲线密码算法，认证技术——包括身份认证、完整性检测和数字签名，密钥分配与管理方案。第 7～9 章将分别详细介绍移动通信网络、无线局域网络和无线个人区域网络的安全技术，并分析它们的安全性。第 10 章则介绍建立在各种无线通信网络之上的无线应用协议，重点在于介绍无线应用协议所包含的安全技术，并分析其安全性，最后以网上支付为例介绍移动电子商务。

本书在编写过程中，先后得到了国家 863 计划项目的资助(项目号为：2002AA143201)和

国家973项目的资助(项目号:G1999035803)。

本书的第1和7～10章由任职于荷兰SAFENET公司的徐胜波博士编写,第3～6章由西安电子科技大学的马文平博士编写,王新梅教授编写了第2章并对全书进行了统编和修改。

由于我们水平有限,错误和遗漏在所难免,敬请读者批评指正。

作　者

目　录

第1章　无线通信网络安全概述

本章首先简要回顾一下无线通信网络的发展史，然后介绍无线通信网络环境并分析其中存在的不安全因素，最后介绍无线通信网络的安全需求以及实现它们所需要的密码机制。

1.1　无线通信网络的发展

从意大利物理学家 Guglielmo Marconi 发明了无线电至今，已有一百多年的历史了。无线通信的最大特点在于它不需要在通信双方之间铺设通信电缆，这不仅可以节省可观的电缆费用，而且将通信用户从通信电缆的束缚中解脱出来，可以实现移动中通信。更重要的是，无线通信可以在无法铺设电缆的“孤岛”之间建立通信连接。例如，畅游于海洋的舰队和船只之间以及它们与陆地上基地之间可以采用无线通信方式进行通信，遨游于太空的卫星和宇宙飞船也是通过无线通信与地球上的控制中心联络的。

在无线通信发展的初期，它的应用价值首先在军事通信领域得到认可，这是因为无线通信方便了战场上作战部队之间的通信联系，即使深入敌后作战的部队也可以通过无线通信与司令部保持联系。鉴于无线通信在军事通信领域的特别应用价值，它很快地就成为一种重要的军事通信工具。在第二次世界大战中，无线通信就已经得到广泛应用，并且一直沿用至今。除了服务于军事通信外，无线通信在其发展初期还被广泛应用于无线广播公司和政府部门。例如，1922 年 11 月 14 日英国广播公司 BBC 开始无线广播，1928 年 4 月 7 日美国底特律警察局开始使用可以从警察局总部到巡逻车的单向移动通信服务，这是移动通信的最早应用。

随着无线通信技术的发展，无线通信在民用通信领域的应用也逐渐增多，这主要体现在移动通信方面。1946 年，AT&T 公司的研究人员开发出一种无线电话，它可以将移动用户连接到公共交换电话网络(PSTN，Public Switched Telephone Network)。AT&T 公司基于此技术开发了最早的民用移动电话系统，称之为移动电话服务(MTS，Mobile Telephone Service)。后来该系统经过不断改进，其改进系统 IMTS 于 1969 年成为当时遍布美国的唯一的一个移动电话系统。IMTS 系统实现了人们想要摆脱通信电缆束缚的要求，然而该系统通信容量有限，不能满足日益增长的移动电话用户需要。到 20 世纪 70 年代末 80 年代初，随着蜂窝技术的发展日益成熟，第一代蜂窝移动通信系统在世界各地投入运营，如 1981 年由爱立信(Ericsson)开发的 NMT(Nordic Mobile Telephone-system)开始在瑞典正式投入公共通信服务，1984 年 AMPS (Advanced Mobile Phone Service)在北美开始运营，它们是第一代模拟移动通信网的代表。在 20 世纪 80 年代，数字通信技术、计算机技术和集成电路技术取得迅速发展，使得数字通信系统不仅可行而且比模拟通信系统更加经济。第一代模拟移动通信网只能提供语音通信服务，可是移动用户已经不再满足于传统的语音通信服务，他们要求新的通信服务如数据通信服务。在这些因素的推动下，移动通信进入了以数字化为特点的第二代，第二代蜂窝移动通信系统的典型代表有欧洲的 GSM(Group Special Mobile)、北美

的过渡标准(Interim Standard)IS-54 和 IS-95 以及日本的 PDC(Pacific Digital Cellular)。在20 世纪 90 年代，多媒体技术随着因特网的爆炸式普及而得到迅速发展。然而，第二代移动通信系统只能提供一些低速率数据传输业务服务，无法满足人们对多媒体业务的要求。因特网与移动通信网的结合也推动着移动通信网络向高速数据传输方向发展，这就是第三代移动通信的目标。第三代移动通信网络在 21 世纪初开始投入使用，日本的 DoCoMo 公司于 2001 年 10 月 1 日率先运营第三代移动通信网络。在国际电信联盟(ITU)的倡导和推动下，第三代移动通信网络标准在 3GPP 和 3GPP2 两个计划下逐步走向统一。

从 20 世纪 70 年代以来，移动通信进入了飞速发展时期，它经历了以模拟技术为特征的第一代、以数字技术为特征的第二代和以多媒体技术为特征的第三代，正在实现着人们无论在何时何地都可以与任何人进行通信的 3W 梦想。

在 20 世纪 90 年代初，随着笔记本计算机在公司、学校和政府部门等办公场所的广泛应用，人们对无线通信中的数据传输业务要求日益增长。鉴于移动通信借助于无线通信技术将移动用户从有线通信电缆的束缚中解脱出来，人们也希望能从计算机网络电缆的束缚中解放出来，实现移动办公，从而提出了无线局域网络的概念。无线局域网络采用与有线计算机局域网络相似的网络协议，而利用无线通信技术代替传统的网络通信电缆，从而使笔记本计算机等移动站可以在一定区域(通信距离与发射机功率成正比，典型通信距离为 100m)内自由移动。为了满足应用日益广泛的无线局域网络的需求，国际电机电子工程师委员会(IEEE, Institute of Electrical and Electronics Engineers)制订了 IEEE802. 11a 和 IEEE802. 11b 标准，其中 IEEE802. 11b 标准因可以提供高达 11 Mbit/s 的数据传输速率而得到广泛应用。此外，欧洲电信标准组织(ETSI , European Telecommunications Standards Institute)也于 1991 年开始制定高性能局域网(HIPERLAN, HIgh PERformance Local Area Network)标准。无线局域网络不受地理环境的限制，不需要电缆等网络设施，它可以根据实际需要随时搭建，而且赋予网络用户足够的自由，因而得到许多公司、企业、学校和政府部门的青睐。

在移动电话和笔记本计算机得以广泛应用的同时，个人数字助理(PDA, Personal Digital Assistant)于 20 世纪 90 年代末期悄然在人们的工作与生活中兴起，PDA 与移动电话和笔记本计算机等移动设备的结合应用大大地方便了人们的工作。如果能将人们在日常工作和生活中所使用的计算机、打印机、传真机以及上面提到的手机、PDA、笔记本计算机等设备通过无线通信技术连接起来，实现近距离范围内互通，那么人们的工作就会更加方便。这就是 20 世纪 90 年代末期兴起的无线个人区域网络的概念。实现无线个人区域网络，首先要解决的问题就是建立一个通用的无线空中接口标准，使不同厂家生产的便携式设备在没有电缆相互连接的情况下，也能在近距离范围内相互通信。1998 年 5 月，由 5 家世界著名公司——爱立信、诺基亚(Nokia)、东芝(Toshiba)、国际商用机器(IBM)和英特尔(Intel)联合发起的蓝牙(Bluetooth)计划为无线个人区域网络的发展提供了可能。另外，1998 年 3 月 12 日 IEEE 802 标准委员会也成立了无线个人区域网络 WPAN 研究组，研究关于在个人操作区域内的电子设备间提供一种低功耗、低复杂度无线连接所需要的新无线网络标准。经过一年的调研，该研究组于 1999 年 3 月 11 日升级为 802 LMSC 工作组，制定了 P802-15 标准，即无线个人区域网络标准。实际上，无线个人区域网络不仅可以在家庭和办公室环境中使用，而且也可以在商店、会议等场所使用；特别值得一提的是，通过无线个人区域网络可以实现无线支付等电子商务。

此外，OpenAir、HomeRF 等组织也在研发新的无线连接技术，它们的目标是建立家庭无线网，使家用计算机、计算机外设、无绳电话、电视机、录像机和音响等消费电子设备能够相互“交流”，实现资源共享和访问因特网等目的。家庭无线网区别于上述其他无线通信网络的特点是：它将通常的语音、高品质的音频和视频、计算机数据等信息结合起来，实现宽带连接。

无线通信技术的发展满足了人们对各种通信服务的需求，同时人们对新服务的要求又推动着无线通信网络不断向前发展。正是在这种推动力的作用下，无线通信技术逐步走进人们的日常工作和生活，而且也逐渐从空间域(即在通信距离方面)日益接近我们，从远在天边的卫星通信，到上百 km 的微波通信、几十 km 的移动通信、100m 的无线局域网通信，以至到 10m 以内的无线个人区域网通信，所有的这一切为我们勾划出一个光明灿烂的无线应用前景。

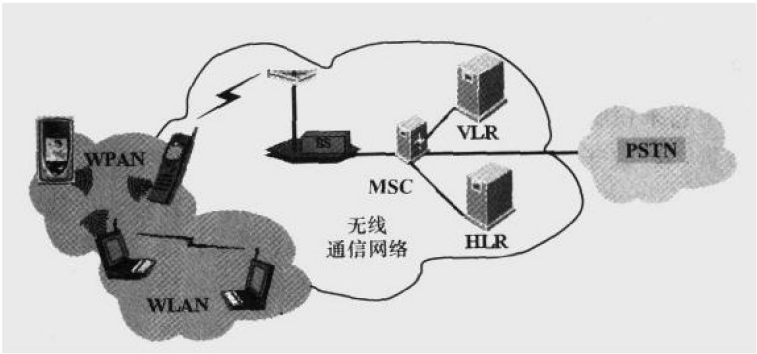

图 1.1　无线通信网络一览图

随着无线通信及其他相关技术的不断发展，无线通信网络的应用将会日益深入人们生活的方方面面。无线手持设备的体积在不断缩小而其功能则逐日增强，它可以用于通话、传输数据、收发电子邮件和浏览因特网，甚至可以帮助人们实现随时随地的电子商务，这就是所谓的移动商务。随着无线网络应用的不断增多，人们越来越关注无线通信网络的安全性。本书将详细介绍与人们紧密相关的移动通信网络、无线局域网和无线个人区域网中的安全技术。

1.2　无线通信网络中的不安全因素

无线通信网络之所以得到广泛应用，是因为无线网络的建设不像有线网络那样受地理环境限制，无线通信用户也不像有线通信用户受通信电缆的限制，而是可以在移动中通信。无线通信网络的这些优势都来自于它们所采用的无线通信信道，而无线信道是一个开放性信道，它在赋予无线用户通信自由的同时也给无线通信网络带来一些不安全性因素，如通信内容容易被窃听、通信内容可以被更改和通信对方身份可能被假冒等。当然，无线通信网络也存在着有线通信网络所具有的不安全因素。本节将详细分析各种无线通信网络中存在的所有不安全性因素。

1.2.1　无线窃听的内容、方法和手段

在无线通信网络中，所有网络通信内容(如移动用户的通话信息、身份信息、位置信息、

数据信息以及移动站与网络控制中心之间的信令信息等)都是通过无线信道传送的。而无线信道是一个开放性信道，任何具有适当无线设备的人均可以通过窃听无线信道而获得上述信息。虽然有线通信网络也可能会遭到搭线窃听，但这种搭线窃听要求窃听者能接触到被窃听的通信电缆，而且需要对通信电缆进行专门处理，这样就很容易被发现。而无线窃听相对来说比较容易，只需要适当的无线接收设备即可，而且很难被发现。

在蜂窝移动通信发展的初期，移动电话具有一个可以调节频率的旋钮，用户通过它来选择通话频率。这种移动电话除了可以用于正常的通话外还可以被用来窃听他人的通话。后来的移动电话可以自动实现频率调节，无需用户的操作，这不仅方便了移动电话的使用，而且也极大地避免了人为利用它来窃听。当然，经过特别改造的移动电话还是可以被用于窃听的，但这种改造需要专业人员的协助，一般人很难做到。另外一种可用于窃听蜂窝移动通信网络中通信信息的无线接收设备是无线频道扫描仪。无线频道扫描仪是一种测试设备，用于帮助无线设备制造商测试生产的无线通信设备，也用于协助无线网络运营商检修设备。由于它可以接收到移动通信网络中所有通信信道中的通信信息，它也可能被滥用于窃听；一些不法组织甚至专门利用它来窃听他人通信，或进行非法活动。在蜂窝移动通信发展初期，无线频道扫描仪比较昂贵，以致于人们认为它对移动通信网络的安全性不构成威胁。然而，到20世纪80年代中后期，900MHz无线频道扫描仪已经很容易买到。虽然一些国家如美国通过立法来禁止制造和进口可以扫描移动通信频道的无线频道扫描仪，但是由于市场上已经有了成千上万的无线频道扫描仪，因而这些法律不能保护移动用户的通信不被窃听。

对于无线局域网络和无线个人区域网络来说，它们的通信内容更容易被窃听，因为它们都工作在全球统一公开的工业、科学和医疗频带(如2.5GHz和5GHz的ISM频带)，任何个人和组织都可以利用这个频带进行通信。而且，很多无线局域网络和无线个人区域网络采用群通信方式来相互通信，即每个移动站发送的通信信息其他移动站都可以接收，这些使得网络外部人员也可以接收到网络内部通信内容。虽然无线局域网络和无线个人区域网络中通信设备的发射功率不是很高，通信距离有限，典型的无线局域网络通信范围是100m而无线个人区域网络则是10m，但是，试验证明通过高增益接收天线在上述距离外还是可以有效地进行窃听。

无线窃听可以导致信息(如通话信息、身份信息、位置信息、数据信息以及移动站与网络控制中心之间的信令信息等)泄露。移动用户的身份信息和位置信息的泄露可以导致移动用户被无线跟踪。无线窃听除了可以导致信息泄露外，还可以导致其他一些攻击，如传输流分析，即攻击者可能并不知道真正的消息，但他知道这个消息确实存在，并知道这个消息的发送方和接收方地址，从而可以根据消息传输流的这些信息分析通信目的，并可以猜测通信内容。

1.2.2 假冒攻击

在无线通信网络中，移动站(包括移动用户和移动终端)与网络控制中心以及其他移动站之间不存在任何固定的物理连接(如网络电缆)，移动站必须通过无线信道传送其身份信息，以便于网络控制中心以及其他移动站能够正确鉴别它的身份。由上一小节可知，无线信道中传送的任何信息都可能被窃听。当攻击者截获到一个合法用户的身份信息时，他就可以利用这个身份信息来假冒该合法用户的身份入网，这就是所谓的身份假冒攻击。