清华大学计算机安全译丛

WILEY
Publishers Since 1807

无线Ad Hoc网络安全

Security for Wireless Ad Hoc Networks

Farooq Anjum Petros Mouchtaris 著
钱 权 译

清华大学出版社

清华大学计算机安全译丛

WILEY
Publishers Since 1807

无线Ad Hoc网络安全

Security for Wireless Ad Hoc Networks

Farooq Anjum Petros Mouchtaris 著
钱 权 译

清华大学出版社
北 京

Farooq Anjum, Petros Mouchtaris
Security for Wireless Ad Hoc Networks
EISBN: 978-0-471-75688-0

图书在版编目(CIP)数据

无线 Ad Hoc 网络安全/(美)安瑞(Anjum,F.),(美)穆什塔瑞斯(Mouchtaris,P.)著;钱权译. —北京:清华大学出版社,2009.3
书名原文:Security for Wireless Ad Hoc Networks
ISBN 978-7-302-19337-1

Ⅰ.无… Ⅱ.①安… ②穆… ③钱… Ⅲ.无线电通信: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(2009)第 015340 号

责任编辑:龙啟铭 李玮琪
责任校对:徐俊伟
责任印制:杨 艳

出版发行:清华大学出版社 **地 址**:北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**:100084
社 总 机:010-62770175 **邮 购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质 量 反 馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
印 装 者:北京鑫海金澳胶印有限公司
经 销:全国新华书店
开 本:185×230 **印 张**:15 **字 数**:334 千字
版 次:2009 年 3 月第 1 版 **印 次**:2009 年 3 月第 1 次印刷
印 数:1~2500
定 价:32.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。
联系电话:010-62770177 转 3103 产品编号:030184-01

序言

无线网路，无论是蜂窝网络还是无线局域网（LANs），已迅速成为我们生活中不可或缺的一部分。目前这种网络已广泛用于办公室、家庭、大学、飞机场和酒店的一些区域。除此之外，小型无线设备（如 PDA、移动电话、掌上电脑、建筑物上的一些小型设备以及传感器等）的广泛运用，使得无线 Nirvana 构想成为现实又向前迈了一步。无线 Nirvana 是一种无缝的无线操作状态，它可使得任何无线设备能够在任何时候、任何地点，连接到任何其他无线设备或网络，以满足用户的需求。显然，真正实现无线 Nirvana 还有很长的路要走。

无线移动自组网技术的发展，使得我们能够实现这一最终目标。但是无线网络中涉及的安全问题，使得广泛采用这种网络仍存在很大障碍。无线网络中的无线通信介质有很大的脆弱性，这些脆弱性很容易被利用从而实施对无线网络的攻击。此外，无线自组网不能依赖传统的企业网络环境中的基础设施，如可靠的电源、高带宽、持续连接、公共网络服务、众所周知的成员身份、静态配置、系统管理和物理安全等。因此，如果无线自组网没有足够的安全性，企业将避免使用它，政府机构也将禁止使用它。同时，国防部门同样因其无法保证人员在战场环境的安全性，用户也可能未实施任何行为，而承担莫须有的责任，从而放弃使用无线自组网。

因此，要让无线自组网得到广泛的应用，解决其安全性问题是一个很重要的方面。可以有两种方法。一种方法是该领域的研究人员提出无线自组网安全的开放性问题，并提供解决方案，这样无线自组网的安全性可以不断得到加强。尽管，让无线自组网更加安全，还需要做很多工作，但是经过数年的研究，已经取得了一些成果。这其中，也包含我们的一些工作。

第二种方法是，直接向该领域的初学者介绍无线自组网存在的安全问题。这样可让更多的人理解它，并且为扩展该领域的知识不断努力。遗憾的是，很少有人沿着这个思路去做。本书的重点就放在通过传播知识的方式介绍无线自组网中存在的安全问题。

- 第 6 章介绍了策略管理，它是网络自动化管理的基本方法，可允许网络管理员定义网络对各种事件，如故障、攻击等自动化应急响应。
- 第 7 章主要介绍 MANET 网络中的“安全定位”。无线 Ad Hoc 网络中的节点通常是移动的，节点定位对于许多无线 Ad Hoc 网络的应用至关重要。书中讨论了各种定位方法以及保证定位安全，预防攻击者攻击的措施。
- 第 8 章介绍了未来 Ad Hoc 一个非常有前途的应用，即无线 Ad Hoc 网络在车载网络中的应用，并且对全书做了一个总结。

从全书的内容可以看出，本书的适用对象很广泛。对于学习和理解无线网络安全的本科生及研究生，本书可以作为他们的教材或参考书目；而对于那些从事网络工程、网络安全的工程技术及研究人员，本书是一本很好的参考读物。

目前，国内在无线网络安全的方面的教材和参考书目还相对缺乏，而反映该领域最新研究进展的书目就更少。因此，本书的翻译出版，希望起到抛砖引玉的作用，相信随着国内外在该领域研究的不断成熟，将有更多的教材或参考书目出现，以满足广大读者的要求。

本书在翻译过程中得到了本书的作者，以及清华大学出版社龙啟铭老师的大力支持。感谢上海大学信息安全研究室同仁的大力支持，感谢研究生陈孟、桂林开、蔡玉华、权洪波、车弘毅等在本书初稿翻译中的辛苦工作。

翻译的过程也是学习的过程，在本书的翻译过程中，在充分尊重原著的同时，也加入了译者自己的理解，但由于本书涉及的学科广、内容新，翻译的难度较大；加之译者水平有限，书中难免有疏漏或错误，欢迎广大读者批评指正。

译者序

无线 Ad Hoc 网络又称为移动自组网、多跳网络或对等网络，最初起源于 20 世纪 70 年代的美国军事研究领域。该网络是一种开放的，多个节点聚在一起形成一个无人工干预的、无预设基础设施的自组织网络，它在有限范围内实现多个移动终端的互联。无线 Ad Hoc 网络因其组网灵活、快捷和高效，可广泛应用于军事通信、地震、水灾等自然灾害后的营救等无法或不便铺设网络基础设施的场合，具有十分广泛的应用前景。

遗憾的是，无线 Ad Hoc 网络因其极大的开放性，也使得它容易受到各种攻击。由 Wiley 出版的 *Security for Wireless Ad Hoc Networks*（Farooq Anjum 和 Petros Mouchtaris 著）就是一本专注于安全的无线 Ad Hoc 网络以及保护该网络的可能解决方案。该书试图解释大量针对无线 Ad Hoc 网络安全的解决方案和技术，讨论不同方法的优点和局限性。全书主要包括以下内容：

- 第 1 章作为绪论介绍了无线 Ad Hoc 网络的定义，无线 Ad Hoc 网络的应用以及该网络面临的安全威胁、攻击以及网络本身的脆弱性。
- 第 2 章介绍了保护无线 Ad Hoc 网络安全的关键保护机制——加密机制，它使恶意节点很难监听或篡改来自其他节点的通信，很难伪装成其他节点。
- 第 3 章介绍了无线 Ad Hoc 网络中节点间密钥共享方案。为了防御攻击者可能发动的各种攻击，确保实体间的通信安全，这在很大程度上需要依赖于网络实体间的密钥共享机制。
- 第 4 章介绍了 MANET 网络常用的路由协议，路由协议的攻击以及相应的安全方法。
- 第 5 章介绍了用于探测 MANET 网络恶意行为的入侵检测技术。再完善的保护机制也没有办法完全阻止攻击者对网络的渗透，因此探测网络的安全事件，采取恰当的应急响应和恢复措施是非常必要的。

就作者所知，本书是第一本针对无线自组网安全性方面的书，然而无线自组网安全性问题本身牵涉的内容很多，有安全网络协议、移动设备上的操作系统和各种应用等。本书的重点放在研究无线自组网的安全网络协议上，特别是无线自组网中两个设备通过无线接口进行相互通信时所涉及的安全问题。

本书的宗旨是能够让读者明白无线网络安全领域的基本原理以及尚未解决的一些问题。并希望不久的将来，在这个领域中取得更多的成就。本书对迄今为止无线自组网安全性问题的研究现状做了一个广泛而全面的概述，并讨论了各种解决方案的优缺点。

在写本书时，我们没有对一些概念的细节做详细解释。因此，要求读者应该对网络的基本概念有所理解。鉴于此，书中解释了无线自组网的一些基本概念。同时，希望读者能略懂安全方面的知识，且书中专门提供了一章来介绍基本的安全概念，这对理解本书的其他章节是很有必要的。

本书适合各种水平的阅读者。初学者可以从各种安全问题和解决方案的粗浅介绍中受益。同时，通过将现有无线自组网的安全方面的重要成果汇编起来，可让初学者学习起来非常方便。因此，本书可以作为一本无线自组网安全性方面的教科书。

对于侧重考虑无线网络安全协议设计的研究者来说，他们将受益于对已知安全问题的描述和响应的解决方案。对致力于无线自组网安全方案创新的研究者来说，也可以通过阅读本书中对已有方案的描述来获益，让他们知道，哪些已经做出来了，还需要做些什么。最后，对于侧重研究无线自组网在商业或军事环境中应用的研究者来说，本书同样有参考价值。以上这些群体都是本书适合的读者群。

当然，我们并不奢望这本书写得很完美，错误在所难免。可能您在阅读本书时，觉得某些很重要的论题在书中遗漏了，或由于我们的背景知识有限，导致我们对某些问题的叙述及其解决方案存在偏差，以及本书其他许多有待改进的地方，我们都乐意收到读者您的来信。因此，关于本书的任何话题，请随时写信给我们。如果你喜爱这本书，我们也想听到你的反馈。我们有一个博客，http://techraw.typepad.com/security/，在上面我们会发布勘误表以及对读者的意见进行的回应。标题可以通过下面的 FTP 站点获得：ftp://ftp.wiley.com/public/sci_tech_med/security_wireless/

同时，祝您阅读愉快！

Farooq Anjum
fanjum@telcordia.com

Petros Mouchtaris
pmouchta@telcordia.com

前言

在没有固定的基础设施下，快速自动地建立无线网络连接并获得服务，是通信最大的挑战之一。网络节点的快速且不可预知的移动以及动态改变的网络连接，加大了问题的复杂程度。无线移动自组网最有价值的地方在于通过优化使用资源，如频段、电源以及操作所支持功能的扩展等，达到其他方式很难达到的性能参数。衡量这种多学科问题的最终尺度是，所用的解决方案，在某种意义上，能够最大限度地减少因自然因素和恶意威胁所导致的连接中断，同时最大限度地确保授权用户能访问关键服务。本书抓住了当前无线移动自组网中所强调的安全和保障等核心问题。

最近十年，研究人员已发掘出无线自组网的许多潜在应用。研究范围覆盖基本理论、模型以及示范。最大的研究团体是政府机构。美国国防部在转型计划中，投入了大量的资源，用于开发无线自组网。Telcordia 在研究新的网络技术及针对这种网络的新安全方法上走在了前列。从基础科学问题构想到提出设计和部署这种网络的工程学原则，Telcordia 都提供技术支持。同时，对构造测试床进行验证、原型系统、示范以及将技术转换成一般应用所必需的步骤等方面 Telcordia 都提供支持。虽然仍有许多问题有待解决，但我们很高兴地看到，技术已经从构想变成了现实。在构想变成现实的过程中，获得了很多组织的大力支持，这些组织有美国陆军研究实验室（ARL）、美国陆军通信电子研究开发和设计中心（CERDEC）以及 DARPA。在商业和公共组织方面，技术发展还比较慢，但也已经发现了它的许多应用方向，包括交通运输网络、应急反应、执法机构和传感器系统。或许最大限度地使用该技术将填补依靠固定基础设施网络的空缺。通过混合蜂窝网络和无线自组网，可以真正实现公共无线网络系统向任何地点的用户提供应用服务。

在向读者展现本书所涉及的研究成果时，作者展现的不仅是相关网络安全知识，还包括对“真正”的通信系统及应用的直觉判断。在商业环境中，客户经常固定某个产品，那么在影响大规模客户群方面，解决方案的非功能属性

和功能属性同样重要。通过网络提供一项服务有时是很容易的，然而随着对服务的高可靠性、高可用性和高安全性需求成规模增长时，一个看似简单的问题就会突然变得很复杂。本书对部分已经解决的问题和部分仍然需要进一步研究的问题，都进行了详细的解释，这正是本书的价值所在。

最后，感谢 Petros Mouchtaris 和 Farooq Anjum，他们都有很高的专业素养和贡献精神，而且对工作质量都有极高的要求，为本书的出版付出了很多的精力。希望他们的努力能得到读者的肯定，我想他们应该会得到很高的满意度，正是因为他们在收集、编撰和阐明复杂文献材料方面的优异表现，才得以写成这本书。

Adam Drobot
President,
Applied Research
Telcordia Technologies

致谢

首先，感谢 Telcordia 使得我们写这本书的想法得以实现。多亏了'Telcordia'文化，版权问题也很快地解决了。尤其感谢应用研究所的主席 Adam Drobot，鼓励我们写这本书。

如果没有来自这个领域各方面工作者的大力支持，也不可能写成此书，他们提出并解决了很多问题。在书中，我们试图找出各种有趣的研究问题，并且讨论不同的研究者给出的各种解决方案。他们的名字以及所做的工作以参考文献的方式分散在全书的各个章节。

该领域的很多工作者对本书的各个章节都发表了不少评论，让我们受益匪浅。非常感谢 Srdjan Capkun、Peng Ning、Adrian Perrig、Santosh Pandey、Rajesh Talpade、Ritu Chadha 和 Mike Little 的评论，大大改进了我们的原稿。

写一本书对任何作者的家庭而言从来都不是一件容易的事。需要牺牲掉原本花在家庭及配偶身上的很多时间，同时，也需要配偶的辅助来帮助作者摆正心态。我相信，每个作者都很感激他们的配偶，这种付出是不能用价值来衡量的。为此，本书的第一、第二作者得非常感谢配偶 ambareen 和 Donna 的全力支持。

感谢 John Wiley，使本书的出版非常顺利。Whitney Lesch 也不能不提，如果不是他经常联系我们解决本书的一些问题，该书也无法完成。

CONTENTS

目录

CHAPTER ONE

第1章

引　言

1.1　无线 Ad Hoc 网络的定义

在过去几年里，我们看到无线通信技术迅速发展。如今，为满足庞大的终端用户的通信需要，无线通信技术在全球范围内正被广泛使用。有超过 10 亿使用移动设备的用户进行语音通信（如电话）和数据服务。其中，数据服务包括发送电子邮件、即时通信和访问网站等。事实上，在世界上的某些地区无线通信技术比传统的有线通信技术要更普遍。

目前无线通信技术的流行主要有几个方面原因。首先，无线设备成本的大幅下降允许供应商大幅降低无线通信服务的价格，使得终端用户能负担得起。其次，在新兴市场中，安装无线网络的成本已远低于安装有线网络的成本。再者，无线通信技术本身取得了长足进步，使得通过无线网络提供语音和数据服务成为可能。最后，无线网络提供的“随时随地”服务，这些对终端用户非常有吸引力。

在无线网络中，节点通过空气中的电磁传播来传输信息。节点传输的信号只能被位于特定距离内的节点所接收，这个距离通常称为信号传输范围。它不仅取决于用于传输的能量等级，还取决于地形、障碍物和具体的传输方案。为了简单起见，节点的传输范围通常被假设为一个以发送节点为中心的圆，如图 1.1 所示。

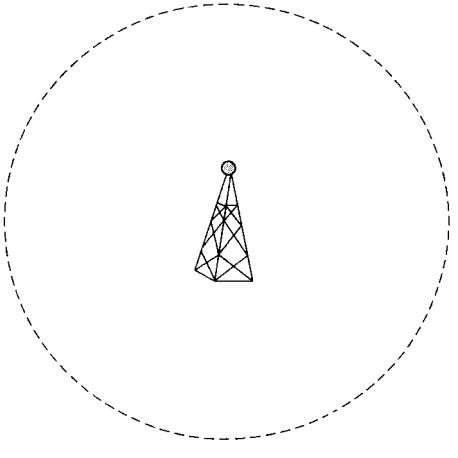

图 1.1　传输范围

典型情况是，当一个区域内存在多个节点时，通常这些节点需要利用无线媒介来进行通信。此时，如果在一个节点的传输范围内有多个传输同时进行，将导致传输冲突。冲突将使接收节点无法理解各个节点传输的数据。这类似于在许多人同时对一个人说话的时候，他将无法明白任何人说的话。因此，如何防止冲突或将冲突减到最小尤为重要。无线媒介的控制访问，以及

冲突避免/冲突最小化方案都是应对冲突问题的有效技术。

目前已经研究出许多冲突避免/冲突最小化的方案，在同时传输的无线节点间共享可用的无线频道。代表性的方案有：(1)时分多址(TDMA)，它把时间分割成小的时隙(Time Slots)，要求节点轮流在不同时隙中传输数据。(2)频分复用(FDMA)，它是将频带分成若干个子频带，每个节点使用不同的子频带传输数据。(3)载波监听多路访问(CSMA)，节点在特定频率上监听无线信道中的传输情况，当节点认为无线信道中没有其他节点传输时，传输自身的数据。(4)码分多址(CDMA)，允许多个节点同时传输信号，但要求每个节点使用不同的扩频码(Spreading Code)进行通信，使得来自不同发送节点的信号能够被接收节点所识别。

节点可能需要和位于它们的传输范围之外的其他节点通信，这时通常利用位于发送节点传输范围之内的其他节点接收并转发信号来完成。转发的结果是，位于转发原始信号节点传输范围内的那些节点接受数据。考虑到不同目的节点的位置，可能需要多个节点转发或重发数据才能完成。该过程如图 1.2 所示。

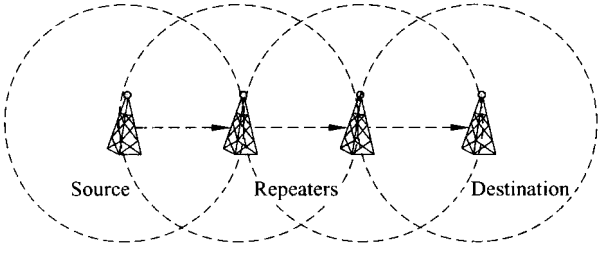

图 1.2 端对端传输

基于目前讨论的各种高层概念，已提出多种不同网络架构。这些网络架构允许无线服务并提供远距离用户间的端对端通信。图 1.3 是应用于蜂窝网络的典型架构。在典型蜂窝网络架构中，服务提供商在希望提供蜂窝服务的区域的建筑物顶部、大型塔或高地上搭建无线传输塔，因此这些无线传输塔是固定不动的。这些无线传输塔负责接收其他节点发送过来的数据，然后根据需要进行转发以到达目的地。使用这种蜂窝服务的终端用户设备通常都很小且是移动的(如手机)。终端设备通常情况下只直接与最近的无线传输塔通信。接着，无线传输塔可根据需要在其他传输塔的帮助下，负责将信息传输给期望接收该信息的节点。

在蜂窝网络中，无线传输塔之间通过静态有线网络(如同步光纤网 SONET)进行互连。终端设备向本地无线传输塔发送信息。如果通过本地无线传输塔无法直接到达目标终端设备，则通过静态有线网络转发给离目标终端设备最接近的无线传输塔，并由其负责将信息传给目标终端设备。

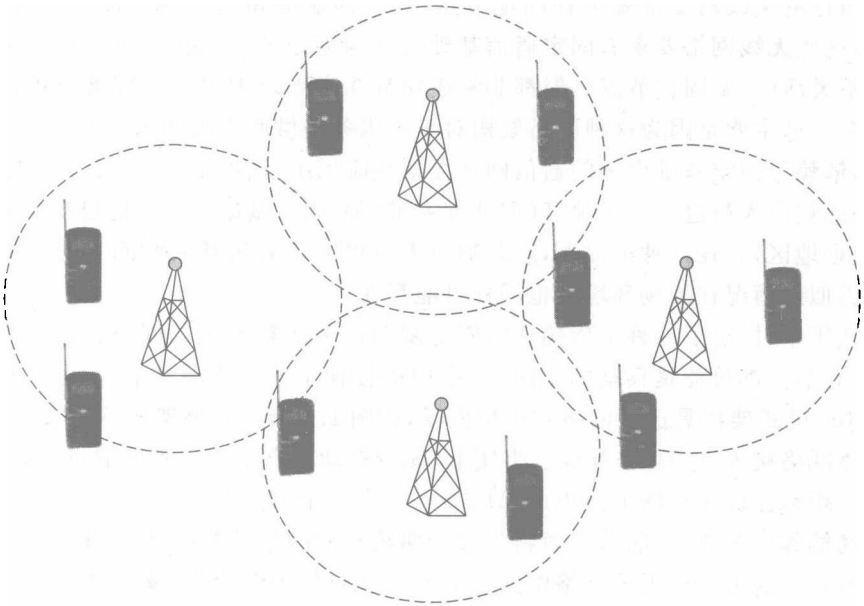

图 1.3　蜂窝网络架构

蜂窝技术并不是现有唯一的无线通信技术。另一个广泛使用的无线通信技术是基于 IEEE 802.11 的无线局域网(WLAN),即常说的 Wi-Fi。Wi-Fi 主要用于建筑物内个人台式电脑和笔记本之间的无线数据连接。相比于蜂窝网络,Wi-Fi 能使设备间更高速地通信(但作用距离相对较短)。事实上,之所以称为 WLAN,是因为其在建筑物内部提供类似于局域网(LAN)的网络连接功能。图 1.4 给出了目前 802.11 典型的网络架构。该架构利用固定的无线网络接入点(APs)来扮演蜂窝网络中无线传输塔的角色。AP 负责接收来自终端设备的信号,然后转发给目的终端设备。此外,AP 还负责将无线局域网连接外部网络,如互联网或其他无线局域网(通过与其他 AP 之间的有线连接)。

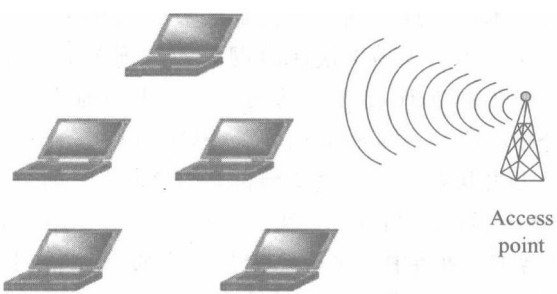

图 1.4　使用 802.11 技术的典型企业架构