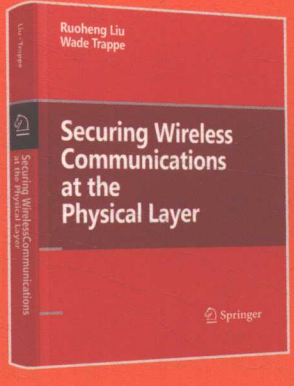
物理层无线安全通信

刘若珩（Ruoheng Liu）
[美] 韦德·特拉佩(Wade Trappe) 著
金梁　黄开枝　钟州　楼洋明　许晓明　译

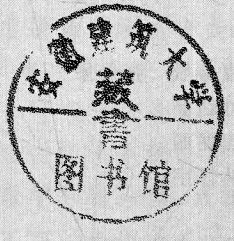
Securing Wireless Communications at the Physical Layer



Springer
清华大学出版社

物理层无线安全通信

刘若珩　[美] 韦德·特拉佩(Wade Trappe)　著
金梁　黄开枝　钟州　楼洋明　许晓明　译



清华大学出版社
北京

内 容 简 介

本书是物理层无线安全通信的入门读物。全书系统全面地论述了当前物理层无线安全通信研究方向中具有普遍性和代表性的基础理论、基本问题及其应用前景。全书内容包括保密传输、安全密钥、身份认证、协作安全，以及调制与编码识别。其中，保密传输包含保密容量、人工噪声技术、安全编码；安全密钥包含密钥容量、提取方案、实际测试；身份认证包含认证容量、认证策略。本书语言生动、论述严谨、内容丰富，并以详细的讲解和翔实的图表及实测数据来阐明重点内容。

本书适合作为通信工程、电子工程和信息安全等专业高年级本科生和研究生的教材或参考书，对于具有一定通信理论和信息论基础的工程技术人员也有很高的参考价值。

图书在版编目(CIP)数据

物理层无线安全通信/刘若珩，(美) 韦德·特拉佩(Wade Trappe)著；金梁等译. —北京：清华大学出版社，2018

书名原文：Securing Wireless Communications at the Physical Layer

ISBN 978-7-302-49891-9

Ⅰ. ①物… Ⅱ. ①刘… ②韦… ③金… Ⅲ. ①无线电通信－安全技术 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字(2018)第 207040 号

责任编辑：袁金敏　张爱华
封面设计：刘新新
责任校对：焦丽丽
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　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
课件下载：http://www.tup.com.cn,010-62795954

印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20.5　　**字　　数**：481 千字
版　　次：2018 年 9 月第 1 版　　**印　　次**：2018 年 9 月第1次印刷
定　　价：99.00 元

产品编号：053869-01

译者序

通信是一种泛在的社会现象，涉及人们生活的方方面面。通信中的安全问题关乎国家安全、金融安全、个人隐私等，历来备受关注。1949 年，Shannon 指出在密钥熵不小于信息熵时能够实现一次一密的完美保密，保密通信理论由此诞生。1975 年，Wyner 在搭线窃听模型中指出通过编码可以实现完美保密传输，并提出保密容量以衡量安全性能。1978 年，Csiszar 进一步研究了广播信道和高斯信道条件下的保密传输问题。1993 年，Csiszar 和 Maurer 则对物理层安全密钥生成的基本模型和密钥容量问题展开研究。上述开创性的成果为物理层保密传输和安全密钥生成奠定了理论基础。

通信中的安全问题种类繁多，本书关注无线通信中由于无线信道的开放性所衍生的安全问题。无线通信与有线通信最大的区别在于信道。电磁波的传播表现为直射、反射、衍射、散射和折射等各种效应的组合，其机理决定了无线信道具有随机性和时变性，是自然界中一种天然的随机源。同时无线信道还具有唯一性和多样性，即不同位置对应的无线信道所表现的特征属性不同。无线信道的复杂性使得用户的信道对于攻击者是不可测量、不可复制的。这一科学规律反映出无线信道具有内生的安全属性。物理层安全技术巧妙利用无线信道特征，从信号层面入手设计安全机制，为解决无线通信的开放性问题提供了全新视角。但是国内尚无系统全面、理论联系实际的通识教材，而该领域的从业人员（包括教学科研人员、科技工作者和管理人员）都希望有一本系统的涵盖理论、技术和应用的参考资料，本书基于上述需求应运而生。

本书以论文集的形式展开论述，各章节由该领域的领军人物编写，因此本书可以说是物理层安全领域集大成的权威著作。本书取材广泛，内容涵盖理论分析、方案设计、实地测量，理论与实际联系紧密、案例翔实，符合认知规律，更易为读者接受。相比于多数侧重信息论的物理层安全专著，本书内容大而全，通俗易懂。另外，本书可以满足不同读者的多元化需求，无论是想从事理论研究、算法设计或是工程开发，都可以以本书为启蒙读物，进而根据需要进行深入研究。更可贵的是，本书也可作为密码学等信息安全工作者进行思维碰撞的参考资料，因此我们从卷帙浩繁的专著中遴选该书进行翻译。

本书的翻译团队从 2009 年开始着手物理层安全研究，先后主持或参与多项国家自然科学基金和国家高技术研究发展计划项目，在通用软件无线

电平台、专用处理器件、商用物联网节点以及无人机等平台上从事物理层保密传输和安全密钥生成工程实践，具备深厚的理论功底和工程开发经验，对物理层安全有着深刻理解和独到见解。尽管如此，决定翻译本书时，仍然面临巨大挑战。由于本书包含物理层安全领域的所有主流分支且各章自成一体，导致相同问题在不同章节中的论述不尽相同。这就要求翻译者不仅要准确理解所述内容，而且要将不同章节中相同的问题进行一致化处理，以免引发歧义，因此该工作是一项“消化-吸收-再创造”的系统工程。

在翻译过程中我们发现原书各个章节之间符号体系不统一，这对长期从事物理层安全研究工作的同仁影响不大，但是对初次接触该领域的人士可能带来理解障碍和疑惑。因此，我们根据理解对书中符号体系进行了统一。同时，考虑文化差异，在翻译工作中我们尽力将理解后的思想用形象的汉语进行表述。另外，为了前后呼应，我们对本书中的专有名词进行统一，如失真度和疑义度的翻译等。因此，本书既可整体把握，又可摘选部分章节学习，方便读者学习理解。可以说，为了能够在流畅、轻松的氛围中准确传达原著的思想，我们做了大量工作，相信经过反复推敲、玩味，定会大有裨益。

为了便于进一步理解，在此对保密传输中保密容量和保密速率的关系，以及安全密钥生成中的度量单位“比特每信道使用”（一次信道使用指的是通信双方进行一次互发导频操作后获取信道信息的过程）进行说明。保密容量是保密传输技术所能达到的保密传输性能的理论上界，是由客观的无线信道环境决定的，因此保密容量不可改变；而保密速率是在某一给定的环境中采用某一保密传输技术（如人工噪声等）所能实现的保密传输速率，通过调整参数设置能够提高保密速率，但是保密速率不能超过保密容量。类似地，可以理解密钥容量和密钥速率。至于比特每信道使用，初次接触或许会觉得莫名其妙。实际上，在安全密钥提取过程中，通信双方将共享的无线信道作为共享随机源，该过程的基本操作是通信双方量化一次互发导频操作后获取的信道信息，经过信息调和与保密增强操作获取一致的密钥。通过对单位时间内信道使用数量的累积，可以将比特每信道使用转化为比特每秒。因此，两种度量单位本质上是相通的。但是比特每信道使用能够更好地表征无线信道的随机性，所以本书采用该指标衡量安全密钥的生成速率。

在知识总量不断激增的今天，科技发展日新月异，专业知识可能很快成为明日黄花。因此在本书的翻译过程中，我们除了介绍物理层安全研究的内涵和外延，更加注重思维方式的培养，力图阐明物理层安全是一套不断完善的科学体系。在可以预见的未来，物理层安全技术一定会在保护通信安全、构建信息安全长城中发挥重要作用。希望更多有识之士投身到这一大有可为、前景光明的事业中。

本书由金梁、黄开枝、钟州、楼洋明、许晓明翻译，为本书翻译提供帮助的还有马克明、夏路、肖帅芳、白慧卿、张胜军、杨静、朱宸、林钰达、江文宇等。同时，于大鹏以及西安交通大学的王慧明、王文杰、穆鹏程和殷勤业为本书翻译提供了专业而细致的指导，大幅提升了本书的专业性和可读性，在此表示感谢。全书最后由王旭统稿，并由金梁审稿。清华大学出版社的编辑为本书的顺利翻译和出版做了大量精细的工作，其严谨的态度和敬业精神令人敬佩。此外，本书的出版得到国家自然科学基金（61379006、61471396、61401510、61501516、61521003、61601514、61701538）的资助。

需要特别说明的是，北京邮电大学的陶小峰、徐璠、李娜，清华大学的周世东，北京理

工大学的何遵文、张焱，北京大学的程翔，中国科学院计算技术研究所的周一青，工业和信息化部电信传输研究所的李侠宇、崔媛媛，中国普天信息产业股份有限公司的张文传，国防科技大学的魏急波、马东堂、熊俊、李为，电子科技大学的文红，陆军工程大学的蔡跃明为本书的内容提供了许多有价值的意见与建议，在此一并表示感谢。

在本书的翻译过程中，我们尽了最大努力忠于原文，尽力使用朴素平实的语言准确阐述其中思想，但由于精力和能力有限，书中难免存在疏漏之处，欢迎各位读者不吝指正。

译　者

2018 年 3 月

前言

确保通信的安全是一项充满挑战的工作，最常见的方式是通过密码学原理和加密算法对信息进行加密，使敌方无法破解。然而，这并不能彻底保证整个信息交换过程的安全。仔细斟酌就会发现，安全难就难在如何建立一套完整的系统解决方案。例如，必须要确保所有涉及的通信对象都要有合适的、经过认证的加密手段；必须验证对方的身份；必须通晓通信的整个流程是如何进行的，以确保通信过程本身不会产生漏洞。

然而，构建安全手段时上述最后一个问题往往不受重视，使之成为众多现代安全研究的短板。信息安全类的文献充斥着大量基于密码学方法的文章（尽管密码学本身仍然存在很多理论上的障碍有待克服，但是其中的大部分都是学术上的，不太影响实际使用），目前有众多的密码学教材可以为如何应用密码学原理提供基础性的介绍；除此之外，信息安全文献的另一大类是有关如何构建安全协议方面的，例如有大量计算机安全方面的教材能够为此提供指导。然而遗憾的是，对“通信是如何进行的”这一基本安全问题的研究成果相对稀缺。再具体点说，信息在不同介质上传播造成的安全问题不同（如无线通信安全就不同于有线通信安全），人们对这一现象缺乏足够的重视。

事实上，尽管分层的通信系统设计方法（对应于一般的开放系统互连（OSI）参考模型）是网络安全协议设计中经常参考的方法，但是，据此产生的安全协议在不同层上往往是割裂的，更忽视了将信息进行编码和调制时所需的最基本的通信层——物理层。这的确令人扼腕，因为这意味着保障现代通信系统安全的手段实际上是不完备的。正如在安全领域经常提到的那样——系统的健壮性取决于其最薄弱的环节，因此必须给予足够的关注。

针对这一突出问题，编者整理了在物理层上研究安全问题的最新成果汇编成书。需要特别指出的是，书中所有文章的作者一致认为，无线通信的物理层是个性鲜明、明显不同于其他通信系统的物理层，因此，要应对物理层的安全威胁必须考虑无线传播媒质的特殊属性。因此本书的一个基调会在书中频频浮现：在具有丰富多径的典型无线场景中，与传播路径对应的信道响应是频率选择性的（或者在时域上称为衰落），而且是由空间位置决定的（即只要传播路径的间隔是波长量级的，那么这些路径对应的信道的相关性会随间隔的增大而迅速减小）。无线物理层这些特有的空间、时间和频率特性为在物理层上建立新的安全服务提供了强大的基础支撑。

本书的章节广泛取材于各个物理层无线安全通信研究团队的研究成果。在选择题材方面，尽可能涵盖物理层安全研究的谱系（从私密性到认证，再到可信度等），并且兼顾到理论和实际两方面。基于这些考虑，章节按不同主题松散编排。本书首先从研究物理层安全的保密性入手。经典意义下的保密通常关注加密算法，以保证只有合法双方才能解密信息，而在物理层安全的背景下，我们更加关心使用无线媒质来保证信息秘密传递的机制。但是，一般情况下该机制会造成通信速率比传统的非保密通信要低很多，因此物理层保密应该定位为传统保密的支撑手段。例如，可以在传统密码中用物理层保密机制完成密钥交换或密钥生成。

物理层的保密手段可以进一步细分为利用无线媒质的特点进行信息保密传输，以及从无线媒质中提取密钥。书中第1～8章安排了信息保密传输的内容，其中大部分内容探讨相关的基础理论并提出了一些基本观点。首先，典型无线通信场景中历经的衰落过程奇特而有趣，衰落越复杂越有利于增强通信的保密性；其次，无线的广播特性使得我们可以在传输时引入干扰来降低敌方的窃听能力，同时增强合法双方安全通信的能力。对于各种无线通信场合，获取信道状态信息对传输十分关键。同样，了解在信道信息不完全或者不准确条件下的保密通信性能也至关重要。除了保密传输的信息论基础之外，还有第5章和第8章研究一些特定编码方案的设计，这是保密传输由理论转化为实用的第一步。

第9～12章探讨了如何利用无线信道的空间、时间和频率特征的唯一性作为收发双方之间共享的私密信息源。如果能从无线信道中充分挖掘出这个可共享的私密信息，那么就能够以它为基础来产生保密通信的密钥。密钥提取技术就是利用物理层来提升安全性的一个非常有潜力的研究方向，因为支撑密钥提取的基本步骤（即获得信道估计值所需的无线信道探测）也是常规通信的一个基础步骤。也就是说，信道估计在大多数无线系统物理层中本来就是要完成的。研究密钥提取技术的章节中既包含大量的理论成果，同时也在物理层安全技术的实际应用方面提供了一些具体的支撑实例。许多章节都包含实验验证，而且还会有一个物理层安全机制实时实现的案例。

第13、14章转向研究有关安全认证方面的问题。认证一般要确保通信双方所声明的身份是真实的，或者消息确实来自于它们所声明的出处。而对于物理层来说，身份的概念有所不同，我们不太关心具体某个人是谁，而是更关心如何区分不同的发送者。在一般的无线认证问题中，我们关心的是有无攻击者主动在通信链路中注入信号，并谎称其发送的信息来自于一个合法的无线设备。有意思的是，在很多场合密码技术并不易于完成身份认证，因此通信方很希望能有办法甄别出信号是来自合法用户还是非法用户。物理层认证方法和密钥提取技术是天生一对，因为这两种方法都把无线信道特征作为安全的基础构件。不同的是，对于密钥提取来说，信道估计作为共享私密信息用于构建密钥；而对物理层认证而言，信道估计充当区分发送者和接收者的认证工具。物理层认证所面临的一个有趣挑战是当环境在变化、通信各方到处移动时如何保持认证的有效性。本书在物理层认证的两章中讨论了认证性能的理论界，并提供了对物理层认证的全面综述，尤其关注无线信道时变性影响方面的研究。

最后，第15、16章介绍了与安全和物理层通信相关的另外两方面内容：协作通信和调制识别。协作通信是一种提升无线通信系统信道容量的新兴技术，其中多个实体通过

彼此中继转发消息副本以协助信息的传输和译码。遗憾的是，传统的协作通信方案均假设所有的通信方是可信的且严格遵循通信协议，因此对存在恶意协作方的场景特别脆弱。我们用一章的内容研究协作通信中产生的安全问题，并提出了一种改进的设计方案来增强协作通信的安全性，该方案将信任的概念加入到协作通信协议中。我们在最后一章对调制识别进行讨论，其中包括如何在没有发送者先验知识的条件下识别其调制方式。一方面，对于新兴的无线通信系统（如认知无线电）这一点非常重要，因为发送者和接收者之间的任何先验关联信息可能会缺失，有必要在通信开始前先识别所采用的通信方式。另一方面，其中的安全分析对如何面向物理层展开攻击也同样重要，因为攻击者一旦掌握了通信的调制方式，不论是采用假冒实体的方法还是采用干扰实体的方法都便于找到最佳的攻击策略。

本书想要提醒读者注意的是，无线通信系统的物理层为提升安全性提供了令人耳目一新的手段，而且这些手段在传统密码学中是没有的。传统的高层安全方法肯定依然会在通信安全中扮演重要角色，这些已有的加密算法和安全协议在实际中得到了很好的验证，物理层安全技术并不能完全取而代之。但是，无线媒质的传播特性是一个强大的、包含特定物理域信息的源泉，可以作为已有传统安全机制的必要补充和增强，为追求无线系统安全的工程师提供新的工具和手段。本书中描述的方法可作为消除未来无线系统设计中潜在薄弱环节的基础，随着无线系统的日益普及，我们期待物理层安全方法能够在应对传统网络安全机制无法解决的安全问题方面发挥更重要的作用。

目录

第1章

独立并行信道的保密容量*

Zang Li, Roy Yates, Wade Trappe

1.1 引　　言

通信的私密性是确保网络安全的基础，对于无线通信系统尤为重要，因为无线传输的广播特性使得无线信号极易被窃听。传统方法是通过密码算法确保只有合法用户才能正确解密、第三方无法还原信息，而不是通过物理方法保障通信链路的私密性 。

到底多少信息泄露给敌对窃听者才是不安全的？这是现代密码学研究的核心问题，由此衍生出两大学派：基于信息论的安全和基于计算复杂度的安全。香农于1949年在参考文献[1]中首次阐述基于信息论的加密方法，其中假定窃听者拥有无限的计算资源，并且加密的目标是确保绝对没有任何信息泄露给窃听者。因此，在窃听者观测到加密消息(密文)时，除了随机猜测原始消息(明文)以外别无他法。相反，基于计算复杂度的加密则不考虑窃听者拥有无限计算能力的情况，而是假定窃听者的计算能力有限，从而利用庞大的计算量使得窃听者难以推断相应的明文。

这两类方法的共同点是都必须要求合法用户之间存在某种形式的共享信息，即通常所说的密钥。作为实现加密的重要参数，密钥必须要保持私密性。因此传统的做法是通过第三方(如证书颁发机构或密钥分发机构)来生成和管理密钥。遗憾的是，在许多无线场景下很难保证有第三方存在，因此这种依赖外部条件的密钥管理机制不可行。实际上，理想的情况应该是通信双方能够自主利用物理资源完成密钥共享，而不依赖于可信第三方，这是本章的指导思想，也贯穿于本书的大部分内容。信息论安全与传统的基于复杂度的安全相比，提供了一种更适合于在无线应用中发挥优势的保密通信手段。特别是由于无线传播环境的复杂性，不同位置的用户会收到污染程度不同的信号副本，而正是这种差异使得用户之间信息(包括密钥)的保密传输成为可能。

信息理论安全起初是Wyner(见参考文献[2])用来研究传统搭线窃听信道的，他发现提高合法信道(主信道)的传输速率与增加窃听者接收信息的疑义度之间存在矛盾，

Zang Li(✉)
无线信息网络实验室，罗格斯大学，北布伦瑞克，新泽西州 08902，美国
电子邮件：zang@winlab.rutgers.edu

* 本章部分内容来自于：Secrecy Capacity of Independent Parallel Channels, Proceedings of the Forty-Fourth Annual Allerton Conference, 2006.