高新科技译丛

Springer

Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems

多天线无线系统中面向物理层安全通信的信号处理方法

【中国台湾】Y.-W. Peter Hong　Pang-Chang Lan　C.-C.Jay Kuo　著

杨炜伟　杨文东　管新荣　译

国防工业出版社

National Defense Industry Press

多天线无线系统中面向物理层安全通信的信号处理方法

Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems

[中国台湾] Y.-W. Peter Hong　Pang-Chang Lan　C.-C. Jay Kuo　著

杨炜伟　杨文东　管新荣　译

国防工业出版社

·北京·

著作权合同登记　图字：军一2017一033 号

图书在版编目（CIP）数据

多天线无线系统中面向物理层安全通信的信号处理方法/（中国台湾）林乐文（Y.-W. Peter Hong）等著；杨炜伟，杨文东，管新荣译. —北京：国防工业出版社，2018.12

书名原文：Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems

ISBN 978-7-118-11705-9

Ⅰ. ①多…　Ⅱ. ①林…　②杨…　③杨…　④管…　Ⅲ. ①无线电通信一通信系统一信号处理一研究　Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字（2018）第 250969 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号　邮政编码 100048）
天津嘉恒印务有限公司印刷
新华书店经售
*
开本 710×1000　1/16　印张 8　字数 145 千字
2018 年 12 月第 1 版第 1 次印刷　印数 1—2000 册　定价 69.00 元

（本书如有印装错误，我社负责调换）
国防书店：（010）88540777　发行邮购：（010）88540776
发行传真：（010）88540755　发行业务：（010）88540717

译者前言

随着移动互联网和无线多媒体数据业务的飞速发展，无线移动通信已经深深地影响了人们的生活。然而，无线通信信道的空间开放特性使得信息传输的安全保证无法令人满意。传统的通信安全体制主要建立在信息加密的基础上，然而鉴于无线链路的开放性和无线网络的动态性，对称加密系统的密钥分发管理问题和非对称加密系统的高计算复杂度问题愈加突出。在许多应用中无线终端由于自身在体积、功率、计算能力等方面的限制，无法负担传统加解密算法的计算与成本开销，而且许多新型业务也对加解密实时性、复杂度和延时等提出了更加严格的要求。此外，随着拥有迅速执行巨量复杂因数分解能力的量子计算机的出现，很多传统的加密方法也将不再可靠。

电磁波的传播特性表现为直射、反射、衍射、散射、折射等多种效应的组合，其广播特性导致无线信道易受到随机噪声和各种干扰的影响，这些机理决定了无线信道具有天然的随机性和时变性。而且，不同位置的用户观测到的无线信道特性不同，表明通信双方无线信道具有空间唯一性，第三方难以测量、重构、复制。无线信道的这些特点可以用于保障无线通信中的信息安全传输。近年来，如何利用无线信道的本质特性实现无线通信中的内生安全得到了国内外的广泛关注。作为上层加密方法的一种补充或代替，物理层安全利用信道的随机性、互易性、空间唯一性等特征来提高无线通信系统的安全性，其本质就在于利用信道的噪声和多径传播的不确定性来加密发送信息，使得窃听者获得保密信号的信息量趋近于零。

物理层安全的理论基础是 Shannon 信息论。Shannon 从信息论角度指出，严格意义上的绝对（理想）安全，要求密文数据和明文数据相互独立，即加密密钥至少达到“一次一密”时才能够达到绝对安全。随后 Wyner 引入了 Wiretap 窃听信道的模型，表明当窃听者的信道是合法接收者的退化信道时，存在某种方法能够实现安全传输。在 Wyner 模型的启发下，很多文献提出了在先验信道状态信息辅助下设计预编码矩阵的无密钥安全方案，其主要出发点是利用无线信道以及噪声内在的随机性使得合法接收者的信道优于窃听者。其中，在多天线系统中通过合理的信号设计，有效利用空间自由度，能够显著增强无线通信系统的物理层安全性能，受到了人们的广泛关注。

本书着重介绍了多天线无线系统中常用于增强物理层安全的信号处理方法。在数据传输阶段，讨论了多天线系统和分布式多天线系统中的安全波束赋形、预编码和人工噪声设计问题；在信道估计阶段，介绍了两种差别化信道估计方案，并通过优化设计人工噪声辅助训练序列增强物理层安全性能。相关内容有助于引导有志于从事无线通信可靠性和安全性理论和应用研究的高年级本科生和研究生以及相关专业工程技术人员快速进入该研究领域。

本书第1章、第2章、第6章和第3章部分内容由杨炜伟翻译，第4章和第3章部分内容由管新荣翻译，第5章由杨文东翻译，全书由杨炜伟统稿。翻译过程中，牟卫峰、陈德川、陶丽伟、吴阳、马瑞谦、鲁兴波、丁宁等研究生做了许多工作，在此表示诚挚的感谢。

本书得到了国家自然科学基金项目（编号61471393，61771487，61501512）、江苏省自然科学基金项目（编号BK20150718）的支持。

由于译者水平有限，书中不当或错误之处恳请各位业内专家学者和广大读者不吝赐教。

译　者

2018年4月

前　言

随着数据通信的迅猛增长和对无缝连接的高度需求，近年来物理层安全受到了广泛关注，尤其是在无线通信领域。不同于传统加密方法应对无线安全问题的解决方案，物理层安全采用信道编码和信号处理技术在源节点和目的节点间交互安全信息，同时保证信息不被窃听节点窃听。这些研究起源于信息论文献，它们常常关注是否存在能够实现物理层安全通信的信道编码，或者研究在安全约束（如安全容量）下能够实现的最大编码速率的基本边界问题。特别地，信息论结果显示，安全容量随目的节点和窃听节点处接收信号质量差异的增大而增加。由此，信号处理技术可应用于数据传输和信道估计阶段以最大化目的节点和窃听节点处接收信号质量的差异。一般来说，为了达到安全容量，编码和信号处理必须同时考虑。然而，最优的联合设计尚未可知，信号处理技术也能被用来增加安全速率或降低信道编码复杂度。这些技术在多天线无线系统中受到重视，其中空间自由度可以被开发来进一步增强安全性。

本书介绍了多天线无线系统中常用于增强物理层安全的信号处理方法。特别地，在数据传输阶段，我们回顾了安全波束赋形和预编码技术，其不仅能增强目的节点处的信号质量，也能降低窃听节点处的信息泄漏。同时还介绍了在信息传输同时利用人工噪声进一步恶化窃听节点处的信号接收质量的方法。进一步拓展这些技术在分布式天线系统和中继系统中的应用，在这些系统中多天线可能没有被部署在单个终端上，额外的空间自由度可以提供更高的设计灵活性和性能增益。但由于分布式终端间需要额外的协同传输以及系统内节节点的可信度问题，这将导致增加更多的安全威胁。在信道估计阶段介绍了所谓的差别化信道估计方案，其优化设计人工噪声辅助训练序列信号，增大目的节点和窃听节点处有效接收信号质量的差异。此时，需要的信号质量差异在发送私密信息之前就得到了增强，并且只需要在每个相干时间间隔内（而不是每个符号周期）执行一次。

本书共分为6章。第1章介绍了无线系统中保障安全性的重要性和挑战，并给出了物理层安全概念的简要背景。第2章简要总结了信息论安全理论的基本结论。第3章介绍了安全波束赋形预编码以及人工噪声设计，这些技术被用来增强数据传输阶段需要的信号质量差异。在第4章中，这些信号处理技术被

拓展应用到分布式天线系统和中继系统中。第5章介绍了差别化信道估计方案，用于实现在信道估计阶段的信号质量差异。最后，第6章进一步介绍了几种物理层安全应用场景和相应的研究方向。

本书的目的是强调信号处理在实现物理层安全中的重要作用，为有志于在该领域深入研究的研究生和科研人员提供当前的研究进展和该领域可能出现的挑战。应该指出的是，由于该领域研究成果众多，因此不太可能对文献资料进行详尽的梳理。但我们希望本文中涉及的材料能够覆盖相关基本结论，可以为研究生和科研人员在该领域的进一步研究提供有益的帮助。

新竹，中国台湾，2013年5月　Y.-W. Peter Hong
洛杉矶，美国，2013年5月　Pang-Chang Lan
C.-C. Jay Kuo

目 录

第 1 章　引言

摘要：本章简要介绍了无线通信系统中面临的安全问题，并指出物理层技术可以用于应对这些安全威胁。随后，介绍了物理层安全的不同技术方向，包括无密钥私密信息传输（这是本章的关注点），基于信道的安全密钥生成和低截获、低检测概率的信号传输。最后，给出了这些技术的相关背景和本书的内容安排。
关键词：安全；加密；物理层安全；安全密钥生成；低截获概率；低检测概率

1.1　无线通信系统中的安全问题

随着对移动性和无缝连接需求的增加，无线通信已经深入我们的日常生活中，对整个社会产生了深远的影响。大量私密的个人信息在无线介质上传输，如网上银行、电子商务和医疗信息。然而，由于无线传输的广播特性，无线通信信号常常会被非授权的接收者截获和窃听，如图 1.1 所示。因此，安全和隐私问题已经受到工业界和学术界的广泛关注，但许多问题仍然有待解决。

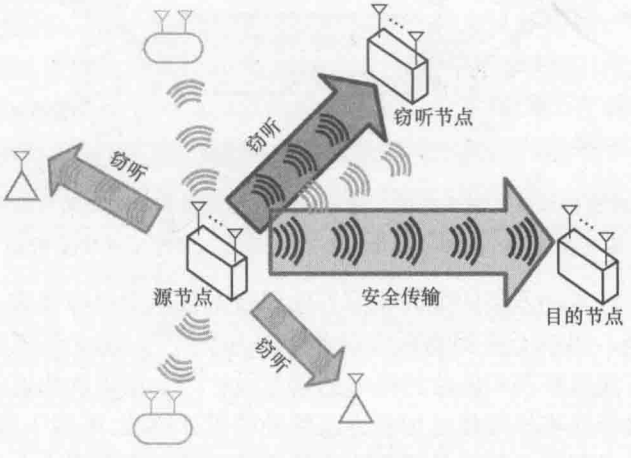

图 1.1　无线媒介中私密通信的窃听风险

一般而言，无线网络安全涉及众多内容，包括保密性、鉴权、完整性、接入控制和可用性等[1,2]。保密性是指阻止对信息非授权地窃取。鉴权是指对不同

终端身份的确认。完整性是指确保传输信息不被非法篡改。接入控制和可用性是指阻止拒绝服务攻击。过去这些安全问题主要在网络层以上的上层协议中通过加密和解密方法给予解决，如数据加密标准（Data Encryption Standard，DES）[3]和高级加密标准（Advanced Encryption Standard，AES）[4]。如图 1.2 所示，如果采用对称密钥加密系统，则一个私钥必须在两个用户间共享，用于对私密信息进行加解密。但这需要安全的通信信道或协议用于交互共享密钥，如 Diffie-Hellman 密钥交互协议[5]。在无线系统中密钥分发和管理的困难导致安全的脆弱性[6]。公钥加密系统，如 RSA [7]，允许用公钥进行加密，然后用独立的私钥解密。公钥对所有用户来说是公开的，但私钥仅被特定的接收者知道。然而，在未知私钥情况下上面提到的基于加密方法保障的信息安全依赖于解密信息的计算复杂度。随着计算能力的增强，特别是量子计算机的发展，用于设计加解密算法的特定数学问题的计算复杂性不再成立，这将导致现有的加密系统不再有效。

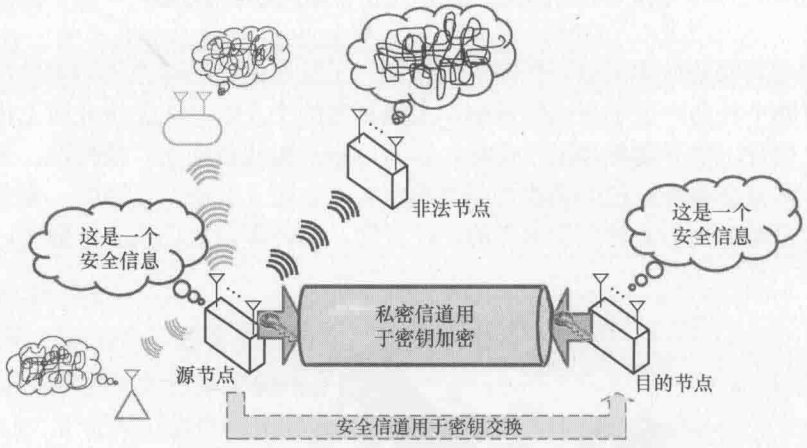

图 1.2　对称密钥加密机制示意图，该机制可以构建源和目的之间传输私密信息的安全信道，但需要先建立安全信道或协议用于交互安全密钥

近年来，许多物理层的编码和信号处理技术被用于保障和进一步增强无线系统信息安全，包括无密钥物理层安全传输方案[8-10]，基于信道的安全密钥生成方案[11]，实现低截获和低检测概率的信号设计[12]。信道的快速时变特性和无线介质的广播特性将导致传统加密方法额外的设计挑战。不同于传统加密方法，这些物理层技术利用（而不是避免）无线传输的特性提供更安全的通信信道。特别地，信道的空间变化被用于确保不同位置的接收信号是不同的。信道在时间上的变化保证了目的节点在某个特定的时刻会获得更好地信道条件（即使在平均意义上它较窃听节点经历更差的信道条件）。无线传输的广播特性为发送干

扰信号恶化窃听节点的接收提供了可能。这些物理层技术用于支撑和补充协议栈上层中的安全协议，但并不意味着将取代传统的加密方法。这些物理层技术将在下面的章节中详细介绍。

值得指出的是，虽然上面提到的诸多安全问题（如鉴权、完整性和可用性）是相当重要的，但本书主要关注的是信息传递过程中的保密性问题。而且，我们仅考虑存在被动窃听者的情况，即窃听节点窃听私密信息或检测通信行为，但不主动发送信号。主动攻击情况下，不同的攻击行为，如干扰、伪造和信息篡改，也可以限制安全性，但这些内容超出了本书的范畴，读者可以进一步阅读文献[1,2]中的相关介绍。

1.2 物理层安全的背景

本节我们简要介绍了 1.1 节中提到的三种物理层安全技术，包括无密钥物理层安全传输（这是本文的关注点）、基于信道的安全密钥生成，以及低截获和低检测概率的信号设计。重点强调了无密钥物理层安全传输，这也是本书的重点所在。

1.2.1 无密钥物理层安全传输

无密钥物理层安全传输方案的研究最早起源于Wyner对搭线窃听信道的研究工作[8]，随后其被拓展到高斯信道[9]和传输私密信息的广播信道[10]，其中私密信息经信道编码（结合随机分组和信道预处理技术）后传输，使得在目的端可靠译码的同时使窃听者产生实质上的混淆。这一领域早期工作大都聚焦在信息理论，主要关注被称为安全容量的性能指标，它被定义为在确保没有信息被窃听者窃听情况下源节点和目的节点间能够实现的最大传输速率。研究结果显示：如果源节点到目的节点的信道优于到窃听节点的信道，则源节点和目的节点间能够实现非零安全容量。这些结果表明在不采用安全密钥的情况下利用物理信道的特性对抗窃听者窃听，确保传输信息的私密性是完全可能的。这避免了传统加密系统中由于密钥的分发与管理导致的固有脆弱性。

随着无线应用的出现，无密钥物理层安全传输方案也被应用于无线系统，这时衰落信道的动态特性也必须加以考虑[13,14]。特别地，文献[13,14]表明，通过利用信道的时变性，即使当目的节点处的平均信道质量较窃听节点处更差，亦可获得正安全速率。最近，文献[15-18]将这些研究拓展到多输入多输出窃听信道，其中源节点、目的节点和窃听节点都配置多个天线。此时由多天线带来的自由度可以用于进一步增强物理层安全。特别地，如文献[16-18]所述，可以

先采用安全预编码技术将 MIMO 信道分解成多个并行的子信道，然后在每个子信道上进行安全编码以保证目的节点获得较窃听节点更优的接收信号质量。然而，该方法需要源节点精确已知主信道和窃听信道的信道状态信息，这在实际中可能无法实现。如图 1.3 所示，当窃听信道未知时，也可以在承载私密信息的信号上叠加发送人工噪声恶化窃听节点处的接收效果。由于源节点配置多天线，人工噪声可以加载在对目的节点干扰最小的维度上。由此，在目的节点和窃听节点处接收信号质量之差（可实现的安全速率）能被有效增加。中继和分布式天线系统也能提供需要的空间自由度，因此安全预编码和人工噪声技术也可被应用于这些系统。

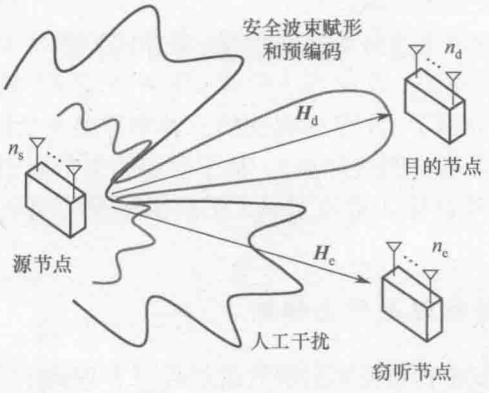

图 1.3　用于存在一个窃听节点的无线多天线系统中的安全波束赋形/预编码和人工噪声方案示意图

1.2.2　基于信道的安全密钥生成

基于信道的安全密钥生成方案利用两个用户（源节点和目的节点）间信道的唯一性作为两个用户在本地生成对称密钥的一致随机源。两个用户相互发送训练序列，然后每个用户根据自己收到的信号进行本地信道估计，获得信道信息。假设两个用户之间的信道具有互易性，则两个用户的信道估计结果是近似相等的，可以被用来作为产生安全密钥的一致随机源。然而，由于噪声影响，信道估计常常存在误差，这将导致密钥不一致。因此，密钥协商和隐私放大技术被用于差错检测和矫正。由于位于半波长范围外的窃听节点经历独立的衰落，它将无法探知源节点和目的节点之间生成的一致安全密钥。

文献[19,20]首先研究了在不同终端间利用一致随机性生成安全密钥。近来，文献[21-24]研究了利用信道特性作为一致随机源。这些方案利用信道幅度和/或相位的量化值消除噪声的影响，在两个终端产生一致的安全秘钥比特。文献

[25]也利用类似的方式生成群密钥。基于信道的安全密钥生成方案的性能通常采用密钥生成速率、密钥熵和密钥失配概率来衡量。这三个指标常受限于物理信道特性，如信道相干时间和信道质量。因此，能实现安全密钥生成速率和密钥失配概率之间最佳折中的技术尤显重要，近年来受到了广泛关注。读者可以在文献[11]中进一步了解这些技术。

1.2.3 低截获和低检测概率信号设计

实现低截获概率和低检测概率的信号设计是过去许多安全研究工作的关注方向[26,27]。这些方案通常采用扩频技术实现[28-30]，其将信号扩展到远大于原始带宽的频谱上进行传输。如直接序列码分多址接入（Direct Sequence Code Division Multiple Access，DS-CDMA）[31]方案中将信号乘以伪随机序列，使得信号隐藏在背景噪声中，减小了被检测到的概率。跳频（Frequency Hopping，FH）通信中，信号的中心频率在较宽的频率范围内随机的跳变，以增加截获或干扰传输的难度[32]。跳频技术通常用于军事通信和商业应用中，如蓝牙和无绳电话。

最近，多天线无线系统中通过利用空间和时间分集，实现低截获概率和低检测概率的技术受到人们的重视[12]。假设目的节点已知自己的信道信息，文献[12]研究了低截获概率和低检测概率约束下，源节点和目的节点间的安全容量和实现该安全容量的传输策略。这种依赖用户信道信息的方式可视为一种空间加密，其将信道系数作为加密的安全密钥。这个安全密钥通过信道估计阶段发送训练序列来分发给每个用户。

1.3 本书概要

本书回顾了无线多天线系统中用于无密钥物理层安全传输的各种信号处理技术。信息论研究结果表明，安全容量随源–目的节点信道质量与源–窃听节点信道质量之差的增加而增大。受此启发，在信号传输阶段和信道估计阶段，信号处理技术都被用于构建到目的节点的等效信道，以增大与窃听信道的质量差异。本书简述了这些相关技术。

第 2 章简要回顾了信息论安全的关键结论，包括不同窃听信道安全容量的研究结果，如离散无记忆窃听信道[8,10]、高斯窃听信道[9]、多天线高斯窃听信道[15-18]和组合窃听信道[33]。

第 3 章主要关注信息传输阶段的各种安全波束赋形和预编码方案。这些方案用于增大目的节点和窃听节点处接收信号质量的差异[15-18]。我们也讨论了将

人工噪声叠加在安全波束赋形和预编码后的信号上传输[15,16,34]，用于恶化窃听节点的接收信号质量，同时通过正确设计人工噪声以保证目的节点处的信号质量。这些技术也被拓展到更为一般的多目的多窃听场景。

第 4 章将安全波束赋形和预编码技术拓展应用到中继系统和分布式多天线系统[35-38]。中继的使用提供额外的空间自由度，可以被进一步用于增强安全。中继不仅可以用于辅助转发信号到目的节点，也可以发送人工噪声或干扰信号恶化窃听节点的接收。但是，由于有额外的节点参与传输，额外的信息泄漏风险也需要被考虑：一方面由于和中继通信需要进行额外的无线传输，另一方面来自于中继的可信问题。

第 5 章聚焦于信道估计阶段，介绍了用于增大目的节点和窃听节点处信道估计性能差异的训练序列发送方案。通过阻止窃听节点获得高质量的信道估计，使得其有效信噪比较差，从而降低了在信息传输阶段窃听信息的能力。文献[39，40]提出了这种训练序列发送和信道估计方式，命名为差别化信道估计（Discriminatory Channel Estimation，DCE）方案，并设计了反馈再训练差别化信道估计和双向训练差别化信道估计两种差别化信道估计方案。

第 6 章简要介绍了前面章节涉及的物理层安全技术的最新应用，包括认知无线电、OFDM 系统和自组织网络，并讨论进一步的研究方向。

参考文献

[1] Lou W, Ren K (2009) Security, privacy, and accountability in wireless access networks. IEEE Wirel Commun 16(4): 80–87

[2] Shiu Y-S, Chang S-Y, Wu H-C, Huang SC-H, Chen H-H (2011) Physical layer security in wireless networks: a tutorial. IEEE Wirel Commun 18(2): 66–74

[3] Data Encryption Standard FIPS-46, National Bureau of Standards Std., Jan 1977

[4] Advanced Encryption Standard FIPS-197, National Bureau of Standards and Technology Std., Nov 2001

[5] Diffie W, Hellman M E (1976) New directions in cryptography. IEEE Trans Inf Theory IT-22(6): 644–654

[6] Schneier B (1998) Cryptographic design vulnerabilities. IEEE Comp 31(9): 29–33

[7] Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public key cryptosystems. Commun ACM 21(2): 120–126

[8] Wyner A D (1975) The wire-tap channel. Bell Syst Tech J 54(8): 1355–1387

[9] Leung-Yan-Cheong SK, Hellman ME (1978) The gaussian wire-tap channel. IEEE Trans Inf Theory IT-24 (4): 451–456

[10] Csiszàr I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3): 339–348

[11] Ren K, Su H, Wang Q (2011) Secret key generation exploiting channel characteristics in wireless communications. IEEE Wirel Commun 18(4): 6–12

[12] Hero A O (2003) Secure space-time communication. IEEE Trans Inf Theory 49(12): 3235–3249

[13] Liang Y, Poor H V, Shamai (Shitz) S (2008) Secure communication over fading channels. IEEE Trans Inf Theory 54(6): 2470–2492

[14] Gopala P K, Lai L, El Gamal H (2008) On the secrecy capacity of fading channels. IEEE Trans Inf Theory 54(10): 4687–4698

[15] Khisti A, Wornell G (2010) Secure transmission with multiple antennas I: the MISOME wiretap channel. IEEE Trans Inf Theory 56(7): 3088–3104

[16] Khisti A, Wornell G (2010) Secure transmission with multiple antennas II: the MIMOME wiretap channel. IEEE Trans Inf Theory 56(11): 5515–5532

[17] Oggier F, Hassibi B (2011) The secrecy capacity of the MIMO wiretap channel. IEEE Trans Inf Theory 57(8): 4961–4972

[18] Bustin R, Liu R, Poor H V, Shamai (Shitz) S (2009) An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. EURASIP J Wirel Commun Netw 2009

[19] Maurer U (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39: 733–742

[20] Maurer U, Wolf S (2003) Secret-key agreement over unauthenticated public channels. IEEE Trans Inf Theory 49: 822–838

[21] Hassan A A, Stark W E, Hershey J E, Chennakeshu S (1996) Cryptographic key agreement for mobile radio. In: Signal digital processing, vol 6. Academic, San Diego, pp 207–212

[22] Azimi-Sadjadi B, Mercado A, Kiayias A, Yener B (2007) Robust key generation from signal envelopes in wireless networks. In: Proceedings of ACM computer and communications security, pp 401–410

[23] Jana S, Premnath S N, Clark M, Kasera S, Patwari N, Krishnamurthy S V(2009) On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of ACM international conference on mobile computing and networking

[24] Wilson R, Tse D, Scholtz R A (2007) Channel identification: secret sharing using reciprocity in ultra wideband channels. IEEE Trans Inf Forensics Secur 2: 364–375

[25] Wang Q, Su H, Ren K, Kim K (2011) Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: Proceedings of IEEE International Conference on Computer Communications (INFOCOM), 2011

[26] Dillard R A (1979) Detectability of spread-spectrum signals. IEEE Trans Aerosp Electron Syst AES-15(4): 526–537

[27] Gutman L L, Prescott G E (1989) System quality factors for LPI communication. IEEE Aerosp Electron Syst Mag 4(12): 25–28

[28] Flikkema P (1997) Spread-spectrum techniques for wireless communication. IEEE Signal Process Mag 14(3): 26–36

[29] Pickholtz R L, Schilling D L, Milstein L B (1982) Theory of spread-spectrum communications—a tutorial. IEEE Trans Commun 30(5): 855–884

[30] Kohno R, Meidan R, Milstein L B (1995) Spread spectrum access methods for wireless communications. IEEE

Commun Mag 33(1): 58–67

[31] Spellman M (1983) A comparison between frequency hopping and direct spread PN as antijam techniques. IEEE Commun Mag 21(2): 37–42

[32] Burgos-Garcia M, Sanmartin-Jara J, Perez-Martinez F, Retamosa J A(2000) Radar sensor using low probability of interception SS-FH signals. IEEE Aerosp Electron Syst Mag 15(4): 23–28

[33] LiangY, KramerG, PoorH V, Shamai (Shitz) S (2009) Compound wiretap channels. EURASIP J Wirel Commun Netw 2009: 5:1–5:12

[34] Goel S, Negi R (2008) Guaranteeing secrecy using artificial noise. IEEE TransWirel Commun 7(6): 2180–2189

[35] Dong L, Han Z, Petropulu A, Poor H (2010) Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process 58(3): 1875–1888

[36] Huang J, Swindlehurst A (2012) Robust secure transmission in MISO channels based on worst case optimization. IEEE Trans Signal Process 60(4): 1696–1707

[37] He X, Yener A (2010) Cooperation with an untrusted relay: a secrecy perspective. IEEE Trans Inf Theory 56(8): 3807–3827

[38] Jeong C, Kim I-M, Kim D I (2012) Joint secure beamforming design at the source and the relay for an amplify and forward MIMO untrusted relay system. IEEE Trans Signal Process 60(1): 310–325

[39] Chang T-H, ChiangW-C, Hong Y-W P, Chi C-Y (2010) Training sequence design for discriminatory channel estimation in wireless MIMO systems. IEEE Trans Signal Process 58(12): 6223–6237

[40] Huang C-W, Chang T-H, Zhou X, Hong Y-W P (2013) Two-way training for discriminatory channel estimation in wireless MIMO systems. IEEE Trans Signal Process 61(10): 2724–2738