WLAN 安全技术应用

林铭芳

广州市盛通建设工程质量检测有限公司，广东省广州市，510000；

摘要：论文深入调研了 WLAN 安全及其关键技术，特别是 WLAN 物理层安全技术的现状与应用。本文详细分析了 WLAN 物理层安全技术的原理、特点及其在实现过程中的挑战，并针对其应用情况调研，提出了需要进一步研究的问题。同时，本文还围绕 WLAN 安全技术与标准的最新进展进行了阐述，包括强健安全网络机制、WPA3 安全协议以及 802.11ax 标准的最新技术进展，这些进展对提升 WLAN 安全性能具有重要意义。此次调研为后续完善 WLAN 安全技术提供了理论基础和实践指导，对未来加强 WLAN 安全技术在各种应用场景中的表现具有重要意义。

关键词：WLAN；安全技术；物理层安全

DOI:10.69979/3041-0673.25.05.021

1 WLAN 物理层安全技术

1.1 发射信号方式安全技术

在 Wyner 的窃听信道模型中，为了获得大于零的保密容量，必须假设窃听信道的容量小于合法接收信道的容量[1]。然而，如果窃听信道的质量优于合法接收信道的质量（例如，窃听者的位置比合法接收者更靠近发送者），则保密容量为零，并且合法通信双方不能保证通信的保密性[1]。为了解决这一问题，Goel 和 Negi 提出在信道中加入人工噪声来恶化窃听信道，从而保证合法通信双方的“最低保密容量”(Minimum Guaranteed Secrecy Capacity)[2]。这个想法基于无线衰落信道的场景。假设发送方（或功率放大器中继器模拟）的发射天线数量严格大于窃听方的接收天线数量，发送方可以使用部分可用功率产生人工噪声，并通过多个天线将其传输到信道[1]。

发送端产生的人工噪声必须设计为仅干扰窃听信道，而不影响合法接收信道的信息传输[1]。然而，该技术要求对信道状态信息（CSI，Channel State Information）有准确的了解，并假设 CSI 是完全公开的，即通信的保密性独立于 CSI，因此在实际应用中受到限制[1]。

1.2 扩频和跳频加密技术

自 20 世纪 50 年代以来，美国军方一直在研究扩频通信。由于其优良的抗干扰性能，它一直是军事通信独有[1]。直到近三十年，它才逐渐应用于民用卫星通信和移动通信[1]。由于跳频也是扩频的一种形式，为了区别开来，本节中描述的扩频特别指直接序列扩频。目前应用最广泛的 WLAN 物理层加密技术无疑是扩频加密和跳频加密[1]。它主要用于具有高安全标准的军事卫星通信系统和战术无线通信系统，如美国军方的联合战术信息分发系统（JTIDS）[1]。直接序列扩频需要使用高频伪随机序列进行扩频调制/解调，实现信号扩频；跳频还需要使用伪随机序列来控制载波跳频的时间和持续时间，从而实现跳频规律的伪随机性[1]。扩频和跳频对伪随机序列的依赖性使得它们自然地适用于对称密码的传统加密机制[1]。

1.3 信道编码加密技术

信道编码不仅可以用于纠错，还可以用于公钥加密系统。Mcelice 在 1978 年提出了一种基于代数编码理论的公钥密码系统，它首次将纠错和加密结合起来。[3]这种结合使得人们可以通过信道编码和密码系统的集成设计来满足通信系统可靠性和安全性的要求，从而减少系统开销，降低资源需求，提高处理速度[1]。因此，信道编码与加密技术受到了学术界的广泛重视。学者们很快意识到，如果没有精良的设计，系统的可靠性和安全性将同时降低，因此这个问题相当具有挑战性[1]。

Mcelice 公钥密码系统最初使用 Goppa 代码。它的缺点是密钥开销大，信息率低[1]。随着信道编码技术的不断发展，人们对基于上述密码体制的各种信道编码进行了研究，并衍生出了一种基于 McEliece 系统的对称加密算法，即类 McEliece 加密算法。最近的研究主要集中在使用低密度奇偶校验（LDPC）码的加密系统上。其中，准循环（QC-，Quasi-Cyclic）LDPC 码因其在以下四个方面的优势而受到特别关注：①QC-LDPC 码结构

简单，易于设计，与一般随机构造的 LDPC 码相比，具有优异的性能；②由于其校验矩阵的低密度准循环阵列结构，可以基于相同的码长、度分布等决定码性能的参数构造大量不同的 QC-LDPC 码，从而提高系统的安全性；③QC-LDPC 码易于编码和解码，电路结构相对简单，可以在编码/解码速率和硬件复杂度之间实现很好的折衷，支持高速加密/解密；④由于校验矩阵和规则数组结构的稀疏性，即使代码长度很长，也只需要很小的密钥开销[1]。

1.4 WLAN 物理层安全技术的应用及需研究的问题

WLAN 物理层安全技术具有易实现、易维护等优点，可应用于基于设备指纹的无线目标识别和定位；新一代接入认证交换机；未来移动通信的无线接入安全；车载网、物联网、无线传感器网络的无线信道安全防护；军事无线通信安全等[4]。多载波、多天线、新型信道编码等技术的广泛应用为物理层安全技术研究提供了广阔的空间。多载波技术和多天线技术可以为安全技术的设计提供频域和空域的自由度，而物理层的帧结构可以为加密方案的设计提供丰富的资源[1]。此外，物理层信号的细微特征可以用来识别设备硬件的唯一性，从而达到设备认证的目的[1]。卫星通信和雷达系统中的射频指纹技术可以应用于无线通信系统的物理层认证[1]。

如何有效利用 WLAN 物理层安全特性来辅助上层的安全设计，是目前 WLAN 通信安全领域在实现跨层安全设计上仍需研究的问题。

总之，WLAN 在物理层安全方面取得了很大进展，相信它在未来仍有广阔的应用前景，也将开创通信安全技术发展的新局面。

2 WLAN 安全技术与标准最新研究

2.1 强健安全机制

IEEE802.11-2016 标准定义了强健安全网络（RSN）和强健安全网络关联（RSNA）。两个终端必须相互验证身份并建立关联，并通过四次握手生成动态加密密钥。两个终端之间的关联称为 RSNA。换句话说，任何两个无线接口之间必须共享唯一的动态加密机制。强健安全网络使用 CCMP/AES 作为强制加密机制，TKIP/ARC4 作为可选加密机制。

强健安全网络是一种只能创建 RSNA 的网络，可以通过 802.11 管理帧的强健安全网络信息元素（RSN IE）字段以标识。信息元素是管理帧中的可变长度可选字段。RSN IE 字段始终出现在四个不同的管理帧中：信标帧、查询响应帧、关联请求帧和重新关联请求帧。如果接入点和漫游客户端启用 802.11r 功能，则重新关联响应帧还将包含 RSN IE 字段。RSN IE 字段用于识别每个终端密码套件（cipher suite）和身份验证功能。除了 RSNA，IEEE802.11-2016 标准标准还允许创建预 RSNA（pre-RSNA），换句话说，相同的 BSS 支持传统安全机制和强健的安全机制。如果强健安全机制（如 CCMP/AES）和遗留安全机制（如果 WEP）可以在同一 BSS 中共存，则称为过渡安全网络（TSN），但大多数供应商不支持过渡安全网络。

2.2 WPA3

2018 年 1 月，Wi-Fi 联盟宣布启动 WPA3 认证项目。WPA3 致力于改进目前在 802.11 无线接口中使用的 WPA2，并提供了一些新功能来保护个人网络和企业网络。

（1）对等实体同时验证：WPA3 通过 SAE 提供了更安全的身份验证机制。SAE 使用零知识证明密钥交换，用户或设备必须证明他们掌握了密码，而不会泄露密码。Wi-Fi 联盟认为，SAE 将在未来取代预共享密钥认证。

（2）管理帧保护：WPA3 要求设备必须支持 MFP，以防止许多常见的数据链路层拒绝服务攻击。

商业国家安全算法：WPA3 定义了与商业国家安全算法（CNSA）套件一致的 192 位加密安全套件。此可选算法旨在进一步保护具有高度敏感要求的政府、国防和工业 WLAN[5]。最初的 WPA3 认证还包括两个其他功能，但它们已从 WPA3 中分离出来，成为一个独立的 Wi-Fi 联盟认证项目。

（3）Wi-Fi Easy Connect：此身份验证利用新的设备配置协议（DPP）定义了简化的访问安全机制。对于具有有限或无显示接口的 Wi-Fi 设备，Wi-Fi Easy Connect 可简化安全配置过程。DPP 适用于智能手表等可穿戴设备，也可能在未来提高物联网设备的安全性方面发挥作用。用户只需使用智能手机扫描传感器或物联网设备上的二维码即可完成 WPA3 认证设备的服务开通。

（4）Wi-Fi Enhanced Open：此身份验证使用机会无线加密（OWE）协议，定义了开放网络中改进的数据隐私机制，并致力于提高开放 Wi-Fi 热点的安全性。OWE 为每个热点用户提供一个单独的加密密钥，无需任何身份验证，但客户端和访问点必须支持 OWE。

截至 2023 年，WPA3 的普及程度已经显著提高，正在逐步取代 WPA2 成为主流安全机制。尽管 WPA2 在部分旧网络中仍在使用，但随着设备更新和技术升级，WPA3 将成为 WLAN 安全的标准配置。

2.3 802.11ax

2017 年，Wi-Fi 芯片组出货量超过 30 亿，全球安装的无线接口数量预计超过 100 亿。今天，802.11 设备的数量超过了世界人口。2018 年早些时候发布的一项研究表明，仅未经许可的频谱就为美国经济贡献了 8300 多亿美元。另一项研究指出，移动设备产生的所有 IP 流量中有 50%~80%是通过 WLAN 传输的。与此同时，技术也在进步。802.11ax 设备已于 2018 年投放市场。该技术致力于改善物理层和 MAC 子层，并有望实现千兆数据速率、调度访问和新的多用户访问。

在每一项 802.11 修正案中，电气和电子工程师协会（IEEE）将提出 802.11 技术的改进机制。2009 年，IEEE 发布了 802.11n 修正案。该修正案实现了从单输入单输出（SISO）无线接口向多输入（MIMO）无线接口的转变。MIMO 无线接口的变化是 802.11 无线接口工作模式的重大变化。在 802.11 修正案获得批准之前，多径现象可以说是一场噩梦;在 802.11n 修正案获得批准后，多路径实际上有利于 802.11n MIMO 无线接口。802.11n 修正案迫使 Wi-Fi 工程师重新学习 802.11 技术的原理，重新思考 WLAN 设计问题的相关问题。2013 年，IEEE 宣布了 802.11ac 修正案，该修正案引入了更多机制来改进 MIMO 无线接口。802.11n 和 802.11ac 技术有助于提高数据速率，但可能无法提高效率。虽然这两种技术确实可以提高网络性能，但它们非常复杂，可能会导致 WLAN 设计和故障排除中出现新问题。

3 结束语

在局域网出现后的一段时间内，由于价格高、数据传输速率低、安全性差、注册手续复杂，WLAN 的发展相对缓慢。20 世纪 90 年代初以来，随着人们工作生活节奏的加快和移动通信技术的飞快发展，WLAN 逐渐进入市场。无线局域网（WLAN）以其方便、高传输速率和低廉的价格成为最常用的上网方式。

在这样一个背景下，本文对 WLAN 物理层安全技术、WLAN 安全技术与标准最新进展进行深入调研；针对 WLAN 物理层安全及其应用调研，提出了需要进一步研究的问题；最后围绕 WLAN 安全技术与标准的最新进展进行阐述。

参考文献

[1]刘在爽,王坚,孙瑞,等.无线通信物理层安全技术综述[J].通信技术,2014(2).DOI:10.3969/j.issn.1002-0802.2014.02.002.

[2]GOEL S,NEGI R. Guaranteeing SecrecyUsing Artificial Noise[J]. IEEE Transactions on Wireless Communica. tions,2008,7(06)：2180-2189.

[3]MCELIECERJ. A Public—Key Cryptosystem Based on Algebraic Coding Theory[R]. USA：JPL DSN Progress Report, 1978.

[4]胡爱群.物理层安全技术及其应用[J].视听界(广播电视技术),2019(03):4-17.

[5]程序圆.Wi-Fi 联盟宣布 WPA3，将重点放在安全增强[DB/OL].https://baijiahao.baidu.com/s?id=1589097869402506610&wfr=spider&for=pc,2018-01-09/2021-12-30