无线通信物理层内生安全：关键技术、优势与未来挑战

鲁信金[1,2]，施育鑫[3]，雷菁[2]，杨志飞[1]，杨小军[1]
（1.电子信息系统复杂电磁环境效应国家重点实验室，河南 洛阳 471000；2.国防科技大学电子科学学院，湖南 长沙 410000；
3.国防科技大学第六十三研究所，江苏 南京 210007）

摘　要：无线通信的高速发展对通信的安全架构设计提出了更高的要求。无线系统的广播性和开放性，使得信息传输容易受到截获、窃听和干扰，带来了相当程度的安全威胁。无线通信物理层内生安全是从无线信号传输的最底层——物理层出发，利用无线信道内在特征和通信相关技术来补充已有的安全机制并改善无线传输的安全性。根据未来无线通信安全发展趋势，围绕无线通信物理层内生安全关键技术展开论述，概括了无线密钥生成技术、无线身份认证技术以及无线加密传输技术的研究现状，分析了无线通信物理层内生安全优势，即唯一性、兼容性、异构性以及可再生性，探讨物理层内生安全设计面临的挑战，即如何实现物理层构架的去冗余和物理层功能的再利用，最后给出了无线通信物理层内生安全关键技术的未来工作展望。

关键词：无线物理层安全；无线内生属性；无线密钥生成；无线身份认证；无线加密传输
中图分类号：TN918.4
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024210

Endogenous security in the physical layer of wireless communications: key technologies, advantages and future challenges

LU Xinjin[1,2], SHI Yuxin[3], LEI Jing[2], YANG Zhifei[1], YANG Xiaojun[1]
1. State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang 471000, China
2. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410000, China
3. The Sixty-third Research Institute, National University of Defense Technology, Nanjing 210007, China

Abstract: The rapid development of wireless communications has put forward higher requirements for the design of security architectures for future communications. The broadcast and openness of wireless systems make information transmission vulnerable to security threats such as interception, eavesdropping and interference. Wireless endogenous security utilizes the intrinsic characteristics of the wireless channel and communication-related technologies to complement existing security mechanisms and improve transmission security. According to the development trend of wireless security, the key technologies of endogenous security in the physical layer of wireless communication were discussed. Research overviews of wireless key generation technology, wireless authentication technology, and wireless encrypted transmission technology were given. The wireless communication physical layer endogenous security advantages, i.e., uniqueness, compatibility, heterogeneity, and reproducibility, were analyzed. Explore how to realize the de-redundancy of the physical layer architecture and the reuse of physical layer functions. Future work on key technologies for endogenous security in the physical layer of wireless communications is outlined.

Keywords: wireless physical layer security, wireless endogenous properties, wireless key generation, wireless authentication, wireless encrypted transmission

收稿日期：2024–09–18
通信作者：施育鑫，shiyuxin13@nudt.edu.cn
基金项目：国家自然科学基金资助项目（No.62171445, No.62201596, No.62201592, No.62471477）
Foundation Items：The National Natural Science Foundation of China (No.62171445, No.62201596, No.62201592, No.62471477)

0　引言

5G 的迅猛发展使得无线通信网络的安全形势日益严峻[1-2]，其三大场景增强移动宽带（eMBB, enhanced mobile broadband）、超可靠低时延通信（uRLLC, ultra reliable and low latency communication）和大规模机器类型通信（mMTC, massive machine type communication）都对安全提出了更高的需求[3]。在 6G 的发展和推进中，数以亿计的设备将会接入无线通信网络中，无线通信网络的安全问题将严重限制未来无线通信业务的广泛开展[4-5]。人工智能、卫星互联网与 6G 通信技术的深度融合，也使得数据的隐私保护面临着前所未有的新挑战[6-7]。

业界希望强化一体化、内生型安全技术的研究，以解决通信与安全“两张皮”和“补丁式安全”等问题[8-9]。如图 1 所示，传统的密码算法和复杂的密码管理方法已难以满足现代通信系统对轻量级安全通信的需求，特别是在密钥的存储和分发方面。因此，本文提出了一种创新的视角，即通过设计高效的安全机制，不仅保障通信网络的轻量级和机密性传输，而且通过物理层内生安全技术的引入，为通信网络带来自主防御的能力[10]。利用信道估计获取时变的随机密钥，在不同通信场景中为实现数据高速传输的安全性和完整性提供轻量级解决方案。利用动态、时变的无线信道特征作为“位置戳”，在信号层面拓展认证维度，实现物理层安全认证。将无线密钥生成与新型传输技术结合设计，使得通信安全管理体系向具有自主防御能力的内生安全架构演进。

为应对未来日益增长的安全威胁，满足通信领域对无线通信网络的安全需求，5G 以及 6G 安全将在新型通信网络架构的基础上，设计具有抵御已知安全威胁、防范未知安全风险的技术方案。无线通信物理层内生安全以提高无线通信传输的安全性为目标，在满足通信关键性能指标（KPI, key performance indicator）的前提下，提供一种计算复杂度低、灵活可调控、多场景适用的无线内生安全机制。无线密钥生成技术、无线身份认证技术和无线加密传输技术是无线内生安全的机制 3 个重要研究方向。无线密钥生成技术是指通信双方通过提取无线信道特征，并设计可实时生成、无须分发的快速密钥更新手段，从而实现“一次一密”的加密效果。无线身份认证技术则在信号层面研究认证参数生成方法，将认证参数与信号传输路径和信道特征绑定，从而实现对通信用户身份的认证。无线加密传输技术是利用已有的通信传输技术如编码、调制、跳频等进行加密设计，在不影响系统可靠性的前提下进一步保证传输层的安全。三者相互联系、相互结合，并根据不同的应用场景和安全需求进行动态调整，以提供更加全面和可靠的安全保障。

本文不仅全面回顾了无线通信物理层内生安全关键技术的最新进展，包括无线密钥生成、无线身份认证和无线加密传输技术，而且还特别强调了这些技术在提供轻量级、高效能安全解决方案方面的独特优势。此外，深入分析了实现这些技术所面临的挑战，并提出了创新的设计思路，旨在通过物理层内生安全设计，优化现有通信网络架构，实现去冗余和功能的再利用，从而为无线通信网络的安全提供更加全面和可靠的保障。这些创新的思路和解决方案将为无线通信安全领域带来新的视角和价值。

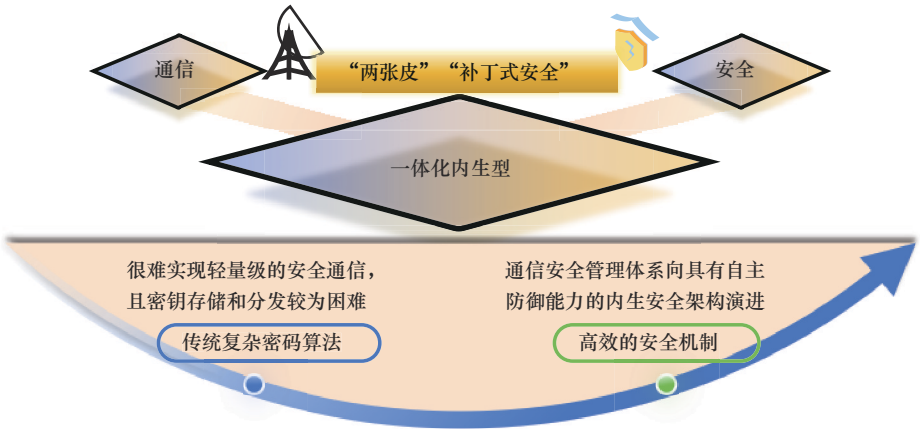


图 1　内生型安全技术的研究趋势

协议栈	功能	安全机制
应用层	应用服务	端到端的密码体制
传输层	端到端的数据交换机制	安全套接层协议
网络层	路由和寻址	虚拟专用网（如IPSec协议）
链路层	介质访问控制	接入控制（如Wi-Fi接入控制）
物理层	信道编码和调制	?

图2　协议栈及其各层的功能和安全机制

1　无线通信物理层内生安全概述

无线通信的安全性是通信网络为用户提供稳定可靠服务的关键。图2给出了标准传输控制协议/网际协议（TCP/IP, transmission control protocol/ internet protocol）栈中各层的功能和安全机制[11]。该5层模型包括应用层、传输层、网络层、链路层和物理层，每个协议层都有其相对应的安全威胁和漏洞，然而除了物理层以外的其他上层都有相应的安全保护机制。物理层信号在无线信道传输过程中处于开放状态，因此存在信息泄露、易遭受攻击等问题，这种典型的“木桶效应”严重影响了系统的安全通信。此外，随着信号窃听技术、截获攻击手段的高速发展，“木桶效应”的物理层传输面临的安全威胁越来越明显。

无线通信物理层是指无线通信系统中负责处理无线信号传输的最底层协议，其主要任务是将数字信息转换为适合在无线媒介上传输的模拟信号，并通过天线将信号发送出去，同时，它还负责接收和解码来自其他设备的无线信号，并将其转换回数字信息。内生安全是基于网络空间的安全威胁所提出的新理论[12]，目前网络空间内生安全理论与技术已得到有效验证。在网络空间内生安全理论的基础上，针对无线通信中电磁波传播的开放性引发的特殊安全问题，无线通信物理层内生安全的概念被提出[13]。无线通信物理层内生安全通过挖掘无线内生安全属性，创新内生安全机制，在工程实现上和各类通信技术进行较好的兼容，在未来无线通信系统具有广阔的应用价值。无线通信物理层内生安全通过挖掘无线内生安全属性，创新内生安全机制，设计内生安全功能，同时与传统安全技术和新兴赋能技术相融合，在工程实现上和各类通信技术进行较好的兼容，提供应对安全威胁的内生安全能力。

无线通信物理层内生安全与传统安全机制相结合还能够进一步拓展安全维度，在不同场景中的鉴权认证、数据完整性保护和物联网轻量级加密等方面提供特色增量。与传统的安全方案相比，无线通信物理层内生安全技术具有低计算复杂度的优势，对通信资源和硬件设施需求较少，可应用于低功耗、轻量级的通信场景，如无线局域网（WLAN, wireless local area network）、无线个域网（WPAN, wireless personal area network）、物联网（IoT, Internet of things）等，实现不同场景中安全与通信的灵活可调控设计，在未来无线通信系统具有广阔的应用价值。

2　无线通信物理层内生安全关键技术

无线通信物理层内生安全旨在通过无线信道的不可预测和随机特性，实现信息理论上的安全。香农[14]从信息论角度证明了当密钥的信息熵大于或等于明文的信息熵时，系统能够达到完全保密。目前物理层安全技术的研究发展分为2个思路展开，如图3所示，分别是以Wyner[15]为代表的无密钥的物理层安全以及以Maurer[16]为代表的有密钥的物理层安全。

图3　无线物理层安全基本分类

Wyner[15]提出了含噪窃听信道模型，在该模型中窃听信道是合法信道的退化信道，且发送用户需获得信道状态信息（CSI, channel state information），从而设计安全编码算法或者信号处理技术完成信息的安全传输。然而在实际系统中，由于各种电磁干扰、参数量化误差、信号反馈时延等因素的影响，如何获得精确的窃听信道状态信息限制了这些无密钥物理层安全策略的实用化进程。

Maurer[16]指出在现实系统中，理想的退化窃听信道几乎不存在，并提出可采用合法通信信道提取安全密钥完成安全通信，此时即使窃听信道条件优于合法信道时，仍然可以进行安全传输。自此，以Maurer[16]为代表的基于密钥的无线物理层安全机制逐渐引起广大学者的关注和研究。

本文重点讨论基于密钥的无线物理层安全中无线密钥生成、无线身份认证以及无线加密传输3个关键技术。

2.1 无线密钥生成技术

现有文献关于无线密钥生成理论已经具有初步进展，利用无线信道特征生成密钥是一个替代公钥密码的轻量化技术，目前已被用于各种复杂环境及通信场景中[17-22]。对这些系统的密钥提取进行分析，能够更加客观地揭露密钥提取的本质，为后续的密钥提取策略提供基础。

文献[17]提出了广义信道探测方法和广义预处理方法，有效提高了多输入多输出（MIMO, multiple-input multiple-output）通信场景中的信道探测效率。文献[18]研究了高度可重置的散射环境中物理层密钥生成的安全性，并推导了密钥容量表达式，仿真结果表明，窃听者通过对周围环境和传播规律的准确了解可以显著降低密钥容量。智能反射面（IRS, intelligent reflecting surface）由于其能实时动态改变无线信道环境，提高不同场景下的通信质量，被认为是极具前景的革命性技术[23]。由于IRS具有控制无线环境的能力，因此可以利用它来辅助基于无线信道的物理层密钥生成[19-20]。在高移动性场景中，较短的信道相干时间给密钥生成增加了复杂性和挑战性。文献[21]提出一种用于正交时频空（OTFS, orthogonal time frequency space）调制技术系统中的密钥生成方法，该方法利用交映傅里叶变换将快速变化的时频域信号转换为慢速变化的延迟多普勒域信号，并利用延迟多普勒域的无线信道表示生成共享密钥。文献[22]研究了在存在相关窃听信道的情况下，2个节点在中继器协助下生成密钥的性能，利用合作干扰方案对中继器和窃听器施加叠加信道测量，对密钥和私钥生成的密钥容量的下限和上限进行了评估，但未给出具体的密钥提取策略。

在无线密钥生成技术中，利用无线信道的随机性和不可预测性来生成密钥，提供了一种新颖的安全解决方案。然而，这一技术也面临着一些挑战。首先，信道条件的快速变化可能导致密钥生成的不稳定性，这在高动态环境下尤为明显。其次，如何确保从信道特征中提取的密钥具有足够的熵，以抵抗潜在的攻击，是设计中的关键问题。尽管存在这些挑战，无线密钥生成技术在IoT设备中显示出巨大潜力，尤其是在资源受限的环境中。例如，一项针对智能城市传感器网络的研究中，利用无线信道的多路径效应生成密钥，成功提高了数据传输的安全性，同时保持了系统的低复杂性和低能耗。

2.2 无线身份认证技术

由于无线介质的开放性，非法用户冒充合法用户进行非法访问、节点克隆、数据篡改等欺骗攻击的情况屡见不鲜[24-25]。作为通信系统底层守护者，无线物理层身份认证（PLA, physical layer authentication）利用信道或设备的独特属性来识别攻击者，为安全通信提供了第一道保护线[26-27]。结合高层接入认证方案，物理层安全认证方案可以进一步加强认证性能，提高通信网络的信息安全性。

目前关于无线物理层身份认证的研究主要有3类。第一类是基于射频（RF, radio frequency）指纹[28-29]。其利用通信设备存在的硬件差异来完成双方的身份认证。然而，认证性能与设备的特性密切相关，特别容易受到外部干扰和噪声的影响。第二类是基于物理层信号水印[30]。该方法通过将标签信息嵌入传输信号中来生成水印，由于标签信息的保密性，攻击者很难获取信息。但是，这种认证机制需要单独地设计认证标签，实现起来可能比较复杂。第三类是基于无线信道机制[31-32]，其又可细分为有密钥和无密钥2种方法，无密钥的信道机制主要是利用合法信道与窃听信道的CSI进行用户身份确认，但这对被认证方的所处位置要求较高，并且容易受到模仿攻击，有密钥的信道机制可看作一种主动认证方式，其将密钥隐藏在信道衰落中，利用

信息交互完成身份认证。假设检验方法[33-34]常用于基于密钥的物理层认证，以区分合法用户和窃听者，然而认证技术中假设检验的基础理论研究仍处于起步阶段。基于密钥的物理层认证技术的研究起源于文献[33]，其利用无线信道的空时唯一性和短时互易性来保护探测和响应信号从而完成身份认证。文献[34]提出了基于多载波信道相位响应的物理层认证方案，其通过在接收和发送信号的阶段嵌入共享密钥来进行认证，进一步提高了认证性能。

无线身份认证技术通过将认证参数与信号的物理层特征绑定，提供了一种有效的安全认证手段。这种方法的优点在于，它能够利用无线信道的固有特性，增强系统的安全性。然而，这种方法也存在一些缺点，比如对CSI的准确性要求较高，且在信道条件变化频繁的环境中，认证过程可能会受到影响。此外，如何防止认证参数被窃听者模拟或篡改，也是需要解决的问题。在实际应用中，例如在车联网通信中，无线身份认证技术被用来确保车辆间通信的安全性。通过将车辆的物理层信号特征与其身份绑定，即使在高速移动的场景下，也能实现高效的车辆身份认证。

2.3　无线加密传输技术

无线通信体系的不断发展以及各种新兴技术的出现给未来无线通信传输性能和安全架构带来全新挑战。无线物理层加密（PLE, physical layer encryption）传输技术可充分利用无线通信自身底层属性，从通信信号以及无线信道的特征出发，利用物理层特性完成保密通信，还可结合无线密钥对编码、调制、扩跳频等物理层传输技术进行加密设计从而实现安全传输[35-36]。作为一种新型安全机制，无线加密传输技术具有底层机动调控、节约通信资源、多场景适用以及与无线通信共生等显著优势。

作为一种新型安全机制，PLE可充分利用无线通信本身的信号格式和无线信道的物理特征，与多载波[37-39]、多天线[40]、新型信道编码[41-42]等技术结合实现对物理层信息的保护。在通信系统中，信息比特在物理层会经过多个阶段如编译码、调制解调等。在这些阶段进行安全传输一体化PLE设计，可在不影响系统可靠性的前提下，进一步提升系统的安全性。文献[35]提出基于polar码冻结位物理层加密算法，其利用混沌序列代替polar冻结位的固定比特，在保证系统可靠性的基础上提高码字的安全性。在此基础上进一步进行polar码结构分析，设计自适应码长的polar码安全技术[36]，既能实现码长可灵活调控又能实现编码安全性。此外，还可将PLE应用于调制技术中，通过对星座图进行旋转、幅相变换以及符号子块间置乱[37-38]，以隐蔽调制信息，保护调制过程中调制方式、码本信息以及调制信息的安全，并减少信息泄露，从而进一步增大窃听者的解密难度。可见，经过加密与调制的一体化设计后，若窃听者采用穷举攻击的方式需遍历所有可能的调制参数，在每种可能的参数下经历解调、译码才能判断出是否破译成功。因此，无线物理层加密作为一种底层的加密方式，能够有效提高通信系统的安全性。

无线加密传输技术通过在物理层对信号进行加密处理，增强了无线通信的安全性。这种方法的优点在于，它能够在不牺牲系统性能的前提下，提供额外的安全保障。然而，加密处理可能会增加系统的复杂性和计算负担，特别是在需要实时处理的场合。此外，加密算法的选择和密钥管理也是设计中需要考虑的重要因素。在实际应用中，例如在军事通信系统中，无线加密传输技术被用来保护敏感信息的安全。通过采用先进的编码和调制技术，结合动态密钥管理策略，即使在敌方试图进行窃听或干扰的情况下，也可确保通信内容的安全和可靠。

3　无线通信物理层内生安全的优势

物理层安全设计是否与网络层安全设计重叠？例如，在网络层已经对传输的信号设计了足够复杂的加密算法，在物理层进行二次加密，在安全上叠加安全，以追求安全冗余是否还有必要？针对这一问题，必须指出的是，无线通信物理层内生安全理念不是一种在网络层安全上纯粹的叠加，而是对无线通信构架中物理层内生属性的充分利用，具有以下独特优势。

1) 唯一性。物理层自带一些网络层不具有的内生安全属性如硬件设备射频指纹、无线信道特征参数等，这些独特的内生安全属性可以被充分利用。一方面，硬件设备的特殊性，使得其射频指纹具有唯一性。例如，功率放大器在开机时产生的暂态特性或者非线性的稳态特征、混频器引入的信号频率漂移测量值等都可用于对发射机进行身份识别和认证，从而区分不同的硬件发射机以及辨别假冒

攻击者。另一方面，无线环境的变化会带来信道特征的变化，这些变化往往是随机的、时变的且无法预测的。在时分双工（TDD, time division duplexing）系统中，无线信道的上下行链路若采用相同频率，则具有短时互易性，这使得收发节点在相干时间内可以获得一致的无线信道特征。此外，不同时间和空间的信道环境不同，这带来的空时唯一性保证了窃听者无法通过窃听信道获得合法信道特征。

2) 兼容性。物理层内生安全设计能够与已有的无线通信传输技术兼容，减少系统冗余。未来的通信体系将会选择采用大规模天线、高频段、大带宽等技术，这使得无线通信内生安全元素更加丰富。利用这些丰富的内生安全元素，物理层内生安全设计将加密、解密模块与已有的无线通信模块如编码、调制、扩跳频等进行有机结合，在保证通信KPI的同时，提供一种灵活可控、通信共生的一体化新型安全机制。例如，在编码设计方案中，可根据编码属性进行加密设计从而构造安全码字，在保证系统可靠性的基础上提升安全性；在多载波调制方案中，经典的降低峰均比模块需要独立设置随机密钥生成器并存储密钥，若能够将物理层安全加密模块与这些模块相结合，将有效减少密钥生成、存储的代价，在拓展系统安全性的同时降低系统冗余；在跳频通信方案中，可以利用无线密钥对跳频图案、调制符号等进行置乱、旋转，以实现通信抗干扰与安全传输的双重目的。

3) 异构性。物理层内生安全设计能够使得窃听者难以具有与合法通信方完全相同的物理层通信架构，这使得窃听者难以获取完整的密文。如图4所示，传统网络层安全设计中，构建了一套明文-密文-明文的加解密流程，使得具有密钥的合法通信方能够通过“密文-明文”环节，而窃听者难以实现这个逆过程。在该过程中，往往密文是完全能够被获取的，窃听者可进行已知明文穷举攻击，即获取一部分密文和明文帮助破译，从而获得有效信息。不同于网络层安全设计，物理层内生安全设计能够从底层出发，使密钥参与编码、调制、抗干扰等物理层通信架构，使得无密钥的窃听者难以具有与合法通信方相同的结构，导致窃听者无法获取完整的密文，更难以完成“密文-明文”的破解。若窃听者希望参与到破译过程，则需要对物理层的内

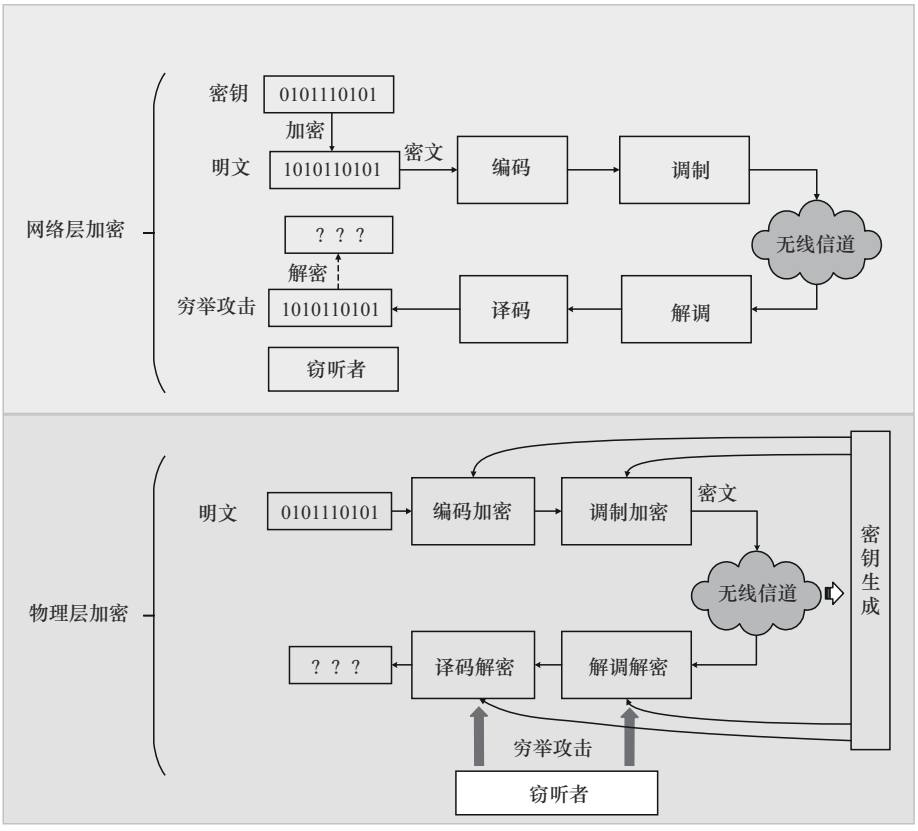


图4　网络层和物理层加密流程

生特性进行模仿，对独特的物理层编码、调制、扩跳频等方法进行设计，这时需要在物理层完成复杂的硬件调试和参数匹配，这将付出更昂贵的代价。

4) 可再生性。物理层内生安全设计适用于不同场景下的轻量级加密，且其密钥具有可再生性。在当下万物互联的5G场景以及未来的6G场景，大量低成本传感器形成的无线传感网络中，各个通信节点不仅受到计算资源、体积、功耗的约束，还将不断动态接入或退出。若均采取网络层的加密手段，这些海量通信终端和节点则需要复杂的加密成本和密钥存储空间。而利用无线物理层内生属性进行安全设计能够为这些场景提供网络层安全设计不具有的轻量化优势，从而保护高速业务数据传输的完整性，更加符合这些场景的安全需求。由于无线信道的动态性，信道特性随时间是动态变化的，这提供了网络层不具有的再生属性。收发双方利用信道估计获取时变的随机密钥，能够解决密钥分发的问题。基于物理层信道动态内生属性可以产生足够安全的新密钥，避免了重复使用同一密钥带来的安全隐患。此外，密钥速率与信息传输速率的相互适配，可进一步达成“一次一密”的安全要求。

4　无线通信物理层内生安全的挑战

尽管物理层内生安全设计具有上述优势，然而仍然存在大量的现实问题需要解决。其中最为关键的问题是，利用物理层内生属性加密时，不可避免地带来额外的硬件成本和计算成本，这些设计甚至可能会带来通信过程中额外的时延、误码和通信协同问题。在通信中，往往需要考虑的第一要务是通信质量，若安全设计带来显著的通信质量风险，则是不可接受的。因此，如何进行物理层内生安全设计，利用好内生安全属性实现安全设计的同时尽可能降低对通信质量的影响，做到物理层构架去冗余和理层功能再利用的效果，是一个亟待解决的关键问题。

1) 物理层构架去冗余

物理层内生安全设计中，加密、解密的环节涉及密钥生成、密钥存储等过程，其中，有些过程在通信过程中是冗余的。若能够在原有通信环节中加入、延伸出加密、解密架构，则避免了这些重复的设计过程和额外的冗余模块，这将带来系统复杂度的降低和可靠性的提升。

例如，在正交频分复用（OFDM, orthogonal frequency division multiplexing）系统中，常常需要降低峰均比的设计，可采用一系列随机数生成多组信号，再选择峰均比较低的一组发送，即选择性映射方法。在该方法中，若将随机数生成器采用无线信道生成的密钥，则避免了降低峰均比模块中的密钥生成或存储的过程。此外，选择性映射方法中的随机数采用密钥而非固定值可完成加密，有效实现了构架上的去冗余。

同样，在跳频抗干扰通信中常使用伪随机序列生成器生成或者保护跳频图案。若利用无线信道生成的密钥序列代替伪随机生成器生成的序列，将跳频和加密控制进行联合设计，则可增强跳频图案的抗破译性能，并减少加密与跳频图案设计中随机序列生成的冗余。

此外，在某些轻量化加密设计中，无线信道生成的密钥参与已有的无线通信传输技术加密甚至可以替代传统的信息加密，因为密钥加密后的动态参数取代了传统通信过程中的固定参数，使得窃听者难以接收、破译信号。例如，在某些低成本的传感器网络中，可以采用无线信道密钥对信息、载波块进行交织置乱，以代替简单的加密，可以低冗余地实现安全与通信质量提升等多种功能，有效降低传感器的功耗。

2) 物理层功能再利用

在实现可靠通信过程中，往往需要多个环节设计保证通信质量，如信道估计、信道编码、调制解调等。当网络层能够为传输信源提供安全保证时，再进行物理层的密钥生成、加密会带来额外的加密功能设计和实现环节，因此，纯粹将无线信道内生属性用于密钥生成，再利用这些密钥对信源进行常规的异或加密运算并未充分利用无线物理层内生属性。因此，在物理层内生安全设计中，应尽量考虑将物理层的加密同通信、认证结合，实现功能上的融合与再利用。一方面，这将使得无线信道产生有限的密钥被充分利用；另一方面，这些融合和再利用能够加大窃听者攻击的难度和成本。

例如，将物理层中调制技术进行内生安全设计，利用无线信道获取的密钥用于调制符号的星座旋转，这将使得窃听者必须采用额外的星座旋转体制和同步设计才能获取密文；否则，窃听者的错误采样位置将直接导致密文丢失。因此，功能模块上

的有效结合和利用提高了窃听者的攻击门槛，提升了安全性。

同样，根据物理层信道编码技术的内生属性，将无线信道提取的密钥用于编码步骤中，并设计加密方案以适应于不同的窃听信道模型，从而降低误码率，提高系统可靠性。例如，对新型编码技术极化码进行凿孔删余设计，既能实现码长的灵活调控，又能实现编码的安全性。

此外，还可将物理层内生安全与认证技术相结合，将无线信道特征作为物理层内生安全元素，利用无线信道的“位置标签”实现合法用户间的身份认证。该方案可与现有的认证机制相补充，从而扩展认证维度，增强无线内生安全认证防御体系，有效抵御异地伪装和攻击。

5 未来研究展望

电磁波的传播特性使得无线信道成为自然界中一种天然的随机源，并且无线信道具有第三方无法测量、无法重构、无法复制的特点，这些科学规律反映出无线信道具有内生安全属性。作为通信安全的颠覆性革命技术，无线内生安全可充分利用无线信道的内在属性，健全无线通信新型安全机制，实现不同场景中安全与通信的灵活可调控设计。现阶段关于无线通信物理层内生安全的研究具有一定进展，未来可深入挖掘和研究的地方包括以下几点。

1) 无线密钥生成技术。一直以来，密钥生成都是基于信道互易性、半双工模式下进行的，可进一步研究信道互易性不理想以及全双工通信模式下的密钥提取。其次在高速移动场景下，由于信道相关时间会随着通信节点移动速度的增加而变短，这对信道探测、信道互易性等都会有新的挑战。此外，目前考虑的大多数窃听模型中为单一的被动窃听者，若窃听者数量多，或者窃听者可以进行主动攻击以及干涉合法通信节点的密钥提取过程，如何在该强大窃听场景下进行密钥提取是具有实际研究意义的方向。

2) 无线身份认证技术。多用户场景下如何基于无线信道进行准确的身份认证，以及如何利用无线衰落信道的随机性和位置互异性保护网络中用户的身份认证信息可进一步深入探索。其次，可尝试将收发机射频指纹机制进行结合，采用机器学习的手段进行训练和识别，利用硬件射频的差异性来完成不同的无线设备。此外，还可进一步研究如何结合物理层信号水印机制，利用身份认证信息与主传输信息的相叠加，在不需要增加额外的带宽的基础上，设计对信号星座图的低功率扰动的广义信号水印方案完成身份认证。

3) 无线加密传输技术。将上层安全技术进行结合，实现跨层安全设计，将物理层内生安全通信算法加入现有通信系统中，进一步设计上层的控制信息，完成多层联合的信息保护和安全增强。其次，可进一步研究大规模天线阵列系统的物理层加密传输方法，通过保护天线组合和映射模式以及调制方式，达到安全通信的目的。此外，可深入挖掘物理层传输技术的内在属性，如信源编码、信道编码调制技术、扩频技术、多址接入技术等，实现物理层多功能安全一体化设计。

6 结束语

作为一种新型安全机制，无线通信物理层内生安全具有底层机动调控、节约通信资源、多场景适用以及与无线通信共生等显著优势。现阶段关于无线通信物理层内生安全的研究具有一定进展，未来可进一步深入挖掘和研究物理层内生安全关键技术，充分利用无线信道的内在属性，实现不同场景中安全与通信的灵活可调控设计。

参考文献：

[1] NOSOUHI M R, SOOD K, GROBLER M, et al. Towards spoofing resistant next generation IoT networks[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 1669-1683.

[2] YAN W F, SHU Q, GAO P. Security risk prevention and control deployment for 5G private industrial networks[J]. China Communications, 2021, 18(9): 167-174.

[3] 强奇, 武刚, 黄开枝, 等. 5G安全技术研究与标准进展[J]. 中国科学: 信息科学, 2021, 51(3): 347-366.
QIANG Q, WU G, HUANG K Z, et al. Survey on research and standardization of 5G security technology[J]. Scientia Sinica (Informationis), 2021, 51(3): 347-366.

[4] 张平, 牛凯, 田辉, 等. 6G移动通信技术展望[J]. 通信学报, 2019, 40(1): 141-148.
ZHANG P, NIU K, TIAN H, et al. Technology prospect of 6G mobile communications[J]. Journal on Communications, 2019, 40(1): 141-148.

[5] 刘国荣, 沈军, 白景鹏. 可定义的6G安全架构[J]. 移动通信, 2021, 45(4): 54-57.
LIU G R, SHEN J, BAI J P. A definable 6G security architecture[J]. Mobile Communications, 2021, 45(4): 54-57.

[6] MAO B M, LIU J J, WU Y Y, et al. Security and privacy on 6G network

edge: a survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25 (2): 1095-1127.

[7] 鲁信金, 黄璐莹, 陈继林, 等. 6G卫星互联网通信安全抗干扰技术研究[J]. 无线电通信技术, 2023, 49(1): 1-9.
LU X J, HUANG L Y, CHEN J L, et al. Research on security anti-interference technology in 6G satellite Internet[J]. Radio Communications Technology, 2023, 49(1): 1-9.

[8] CHEN H S, HAN X T, ZHANG Y Y. Endogenous security formal definition, innovation mechanisms, and experiment research in industrial Internet[J]. Tsinghua Science and Technology, 2024, 29(2): 492-505.

[9] LI H Q, LI X D, ZHANG Z T, et al. ESUAV-NI: endogenous security framework for UAV perception system based on neural immunity[J]. IEEE Transactions on Industrial Informatics, 2024, 20(1): 732-743.

[10] 黄开枝, 金梁, 钟州. 5G物理层安全技术: 以通信促安全[J]. 中兴通讯技术, 2019, 25(4): 43-49.
HUANG K Z, JIN L, ZHONG Z. 5G physical layer security technology: enhancing security by communication[J]. ZTE Technology Journal, 2019, 25(4): 43-49.

[11] HARRIS B, HUNT R. TCP/IP security threats and attack methods[J]. Computer Communications, 1999, 22(10): 885-897.

[12] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189-204.
WU J X. Development paradigms of cyberspace endogenous safety and security[J]. Scientia Sinica (Informationis), 2022, 52(2): 189-204.

[13] 金梁, 楼洋明, 孙小丽, 等. 6G无线内生安全理念与构想[J]. 中国科学: 信息科学, 2023, 53(2): 344-364.
JIN L, LOU Y M, SUN X L, et al. Concept and vision of 6G wireless endogenous safety and security[J]. Scientia Sinica (Informationis), 2023, 53(2): 344-364.

[14] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[15] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8): 1355-1387.

[16] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.

[17] HUA Y B. Generalized channel probing and generalized preprocessing for secret key generation[J]. IEEE Transactions on Signal Processing, 2023, 71: 1067-1082.

[18] JI Z J, ZHANG Y, HE Z W, et al. Vulnerabilities of physical layer secret key generation against environment reconstruction based attacks[J]. IEEE Wireless Communications Letters, 2020, 9(5): 693-697.

[19] HU L, LI G Y, HU A Q, et al. Exploiting malicious RIS for secret key acquisition in physical-layer key generation[J]. IEEE Wireless Communications Letters, 2024, 13(2): 417-421.

[20] LU X J, LEI J, SHI Y X, et al. Intelligent reflecting surface assisted secret key generation[J]. IEEE Signal Processing Letters, 2021, 28: 1036-1040.

[21] SOLAIJA M S J, ZEGRAR S E, ARSLAN H. Delay-Doppler-based key generation using OTFS[J]. IEEE Wireless Communications Letters, 2023, 12(8): 1474-1478.

[22] DIAMANT R, TOMASIN S, ARDIZZON F, et al. Secret key generation from route propagation delays for underwater acoustic networks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3318-3333.

[23] ZHANG Z J, DAI L L, CHEN X B, et al. Active RIS vs. passive RIS: which will prevail in 6G?[J]. IEEE Transactions on Communications, 2023, 71(3): 1707-1725.

[24] AHUJA B, MISHRA D, BOSE R. Fair subcarrier allocation for securing OFDMA in IoT against full-duplex hybrid attacker[J]. IEEE Transactions on Information Forensics and Security, 2898, 16: 2898-2911.

[25] JIANG X Y, LIU X Y, CHEN R Q, et al. Efficient receive beamformers for secure spatial modulation against a malicious full-duplex attacker with eavesdropping ability[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1962-1966.

[26] XIE N, SHA M R, HU T X, et al. Multi-user physical-layer authentication and classification[J]. IEEE Transactions on Wireless Communications, 2023, 22(9): 6171-6184.

[27] WU Y M, WEI D, GUO C L, et al. Physical layer authentication based on channel polarization response in dual-polarized antenna communication systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2144-2159.

[28] SOLTANIEH N, NOROUZI Y, YANG Y, et al. A review of radio frequency fingerprinting techniques[J]. IEEE Journal of Radio Frequency Identification, 2020, 4(3): 222-233.

[29] HE Y L, PODLESNY M. Dielectric waveguide filled with particulate media for ultrahigh frequency (UHF) radio frequency identification (RFID) applications[J]. IEEE Journal of Radio Frequency Identification, 2022, 7: 27-37.

[30] KAMILI A, HURRAH N N, PARAH S A, et al. DWFCAT: dual watermarking framework for industrial image authentication and tamper localization[J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5108-5117.

[31] XIE N, CHEN J J, HUANG L. Physical-layer authentication using multiple channel-based features[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2356-2366.

[32] XIE N, LI Z Y, TAN H J. A survey of physical-layer authentication in wireless communications[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 282-310.

[33] SHAN D, ZENG K, XIANG W D, et al. PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1817-1827.

[34] WU X F, YANG Z. Physical-layer authentication for multi-carrier transmission[J]. IEEE Communications Letters, 2015, 19(1): 74-77.

[35] LU X J, LEI J, LI W, et al. Physical layer encryption algorithm based on polar codes and chaotic sequences[J]. IEEE Access, 2019, 7: 4380-4390.

[36] LU X J, LEI J, LI W. A physical layer encryption algorithm based on length-compatible polar codes[C]//Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall). Piscataway: IEEE Press, 2020: 1-7.

[37] 鲁信金, 雷菁, 施育鑫. 基于旋转置乱的索引跳频抗干扰加密方法[J]. 通信学报, 2021, 42(12): 27-34.

LU X J, LEI J, SHI Y X. Index modulation aided frequency hopping anti-jamming and encryption method based on rotation scrambling[J]. Journal on Communications, 2021, 42(12): 27-34.

[38] LU X J, LEI J, LI W, et al. A joint scheme for PAPR reduction of OFDM signals based on 3-D constellation rotation encryption[C]//Proceedings of the 2020 International Conference on Wireless Communications and Signal Processing (WCSP). Piscataway: IEEE Press, 2020: 766-770.

[39] KEBEDE T, WONDIE Y, STEINBRUNN J, et al. Multi-carrier waveforms and multiple access strategies in wireless networks: performance, applications, and challenges[J]. IEEE Access, 2022, 10: 21120-21140.

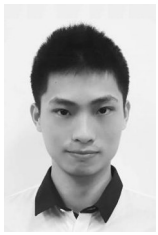
[40] LI H Y, YANG N, HUANG Y H, et al. A multi-antenna pilot predistortion scheme and channel estimation algorithm for LTE-based terrestrial broadcast system[J]. IEEE Transactions on Broadcasting, 2023, 69(1): 215-223.

[41] HAMA Y, OCHIAI H. Binary-input ternary-output turbo codes forternary PSK transmission[J]. IEEE Communications Letters, 2022, 26(9): 1974-1978.

[42] LI Y X, QU D M. Modified SC decoding for BDPSK modulated polar codes[J]. IEEE Communications Letters, 2023, 27(1): 46-49.

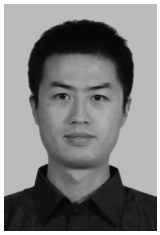
[作者简介]

鲁信金（1994– ），女，安徽滁州人，博士，电子信息系统复杂电磁环境效应国家重点实验室助理研究员，主要研究方向为无线通信技术、无线内生安全、通信抗干扰等。



施育鑫（1995– ），男，福建泉州人，博士，国防科技大学第六十三研究所助理研究员，主要研究方向为无线通信、通信抗干扰等。

雷菁（1968– ），女，陕西西安人，国防科技大学教授、博士生导师，主要研究方向为信息论、LDPC码、空时编码、先进的多址技术、物理层安全、无线通信技术等。



杨志飞（1984– ），男，河南安阳人，国防科技大学副研究员，主要研究方向为认知无线电、信道编码、通信抗干扰等。

杨小军（1986– ），男，江西宜春人，国防科技大学助理研究员，主要研究方向为建模与仿真、评估与决策、人工智能等。