无线物理层认证技术：昨天、今天和明天

Wireless Physical Layer Authentication Technology: Yesterday, Today, and Tomorrow

任品毅 /REN Pinyi，徐东阳 /XU Dongyang
（西安交通大学无线通信研究所，中国 西安 710049）
(Institute of Wireless Communications, Xi'an Jiaotong University, Xi'an 710049, China)

DOI：10.12142/ZTETJ.202004013
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20200722.1043.002.html
网络出版时间：2020-07-22
收稿日期：2020-06-15

摘要：提出了物理层认证技术的未来研究方向，具体包括基于信号内生特征的无线物理层认证技术，面向5G的安全、可靠、低时延无线物理层认证协议设计，以及面向6G的无线物理层认证体系设计。物理层认证技术为无线网络中信息认证提供了灵活的安全保障。未来无线空口技术、网络架构和业务场景的新特性，使得现有研究难以为未来无线认证提供全方位的安全防护，而研发新型无线物理层认证技术在诸多方面存在挑战。

关键词：物理层安全；无线物理层认证；5G；6G

Abstract: Future research directions of physical layer authentication technology are proposed, including wireless physical layer authentication technology based on signal endogenous features, secure and reliable low-latency protocol designed for wireless physical layer authentication in 5G, and wireless physical layer authentication system designed for 6G. Physical layer authentication technology provides flexible security guarantee for information authentication in wireless networks. However, the emergence of new features of future new radio technologies, network architecture and service scenarios makes it difficult to provide all-round security protection for future wireless authentication, and there are still many challenges in developing new wireless physical layer authentication technologies.

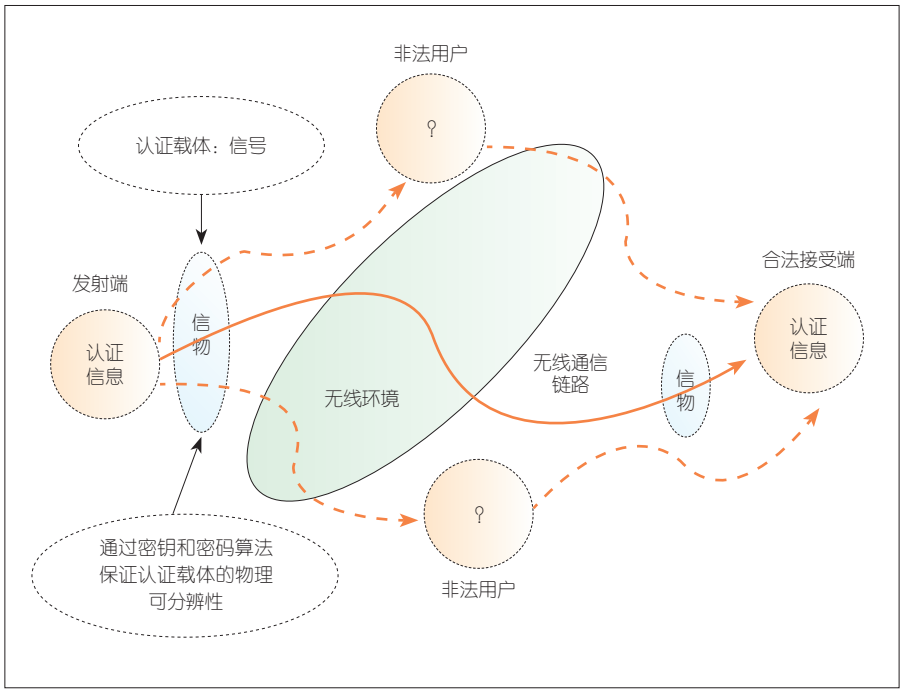
Keywords: physical layer security; wireless physical layer authentication; 5G; 6G

1 无线认证的起源与发展

认证是通过验证被认证对象的持有信物来证实该对象是否属实和有效，这些信物因人而异。数字时代来临之前，人与人之间凭关系相互识别。随着个体数量逐渐增多，陌生人也随之增多，人与人之间难以仅通过关系维持相互合作，对个体进行认证成为必然，这时承载认证信物的载体主要是语言和实物。数字时代的来临使得人与人以及人与物之间交流的方式发生变革，载体的存储和传输更多是以数字化信息为基本方式，认证则表现为虚拟化、数字化。

为了保障认证的安全性，需要对载体的存储和传输方式进行加密保护。现代密码在20世纪60年代得以推出，目的是保护私人信息免受窥探。由于密码的安全性高度依赖于个人选择，因此其安全性十分受限。20世纪70年代，一些学者提出了公开密钥体制，运用单向函数的数学原理，以实现加解密密钥的分离。其中，加密密钥是公开的，解密密钥是保密的，从而极大地提高了认证密钥的安全性。20世纪80年代初，美国科学家L. LAMPORT首次提出了利用散列函数产生一次性口令的思想，即用户每次登录系统时使用的口令是变化的，提高了加密机制的安全性。20世纪90年代，美国、加拿大等国相继开展了公钥基础设施（PKI）的研究和建设工作，为公开密钥体制提供了必要的基础设施。为了融合多种身份验证机制，多因子身份认证（MFA）于21世纪初被提出，为未来认证提供了基础性框架。

随着数字化时代的来临，认证信物载体的传播方式发生变革，并从根本上改变了安全认证的模式。1897年，意大利科学家G. MARCONI首次实现了无线电波信号的远距离传输，标志着人类进入无线通信时代。信息的无线传输导致认证无线化，特别是认证信物载体的数字化、多样化。图1给



▲图 1　无线认证的基本框架

出了无线认证的基本框架，发射端将认证信物嵌入认证载体（即无线信号）上，通过密钥和密码算法保证认证载体的物理可分辨性，从而使接收端识别发射端身份和信息，同时有效对抗非法用户的窃听和恶意篡改等行为。无线认证信物的载体表现为 4 类，包括口令特征（密码、私密密钥等）、持有特征（银行卡、密保卡等）、行为特征（语音识别、步态识别等）、生理特征（指纹识别、视网膜识别等）等。与此同时，认证无线化也引入了更多安全风险。例如，认证攻击种类繁多，包括身份假冒、数据篡改、重放攻击，以及通信抵赖。

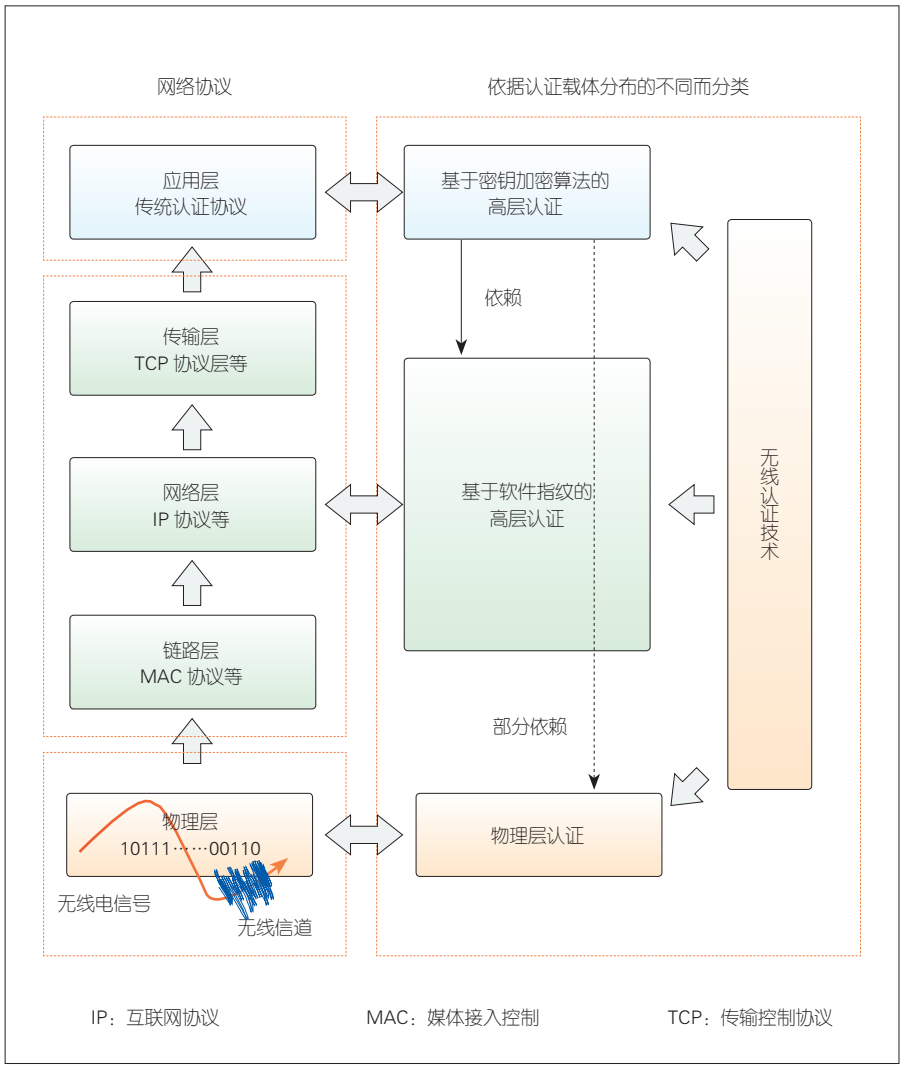
随着无线通信与密码学不断发展以及相互融合，无线认证技术得以不断发展和完善。自从 1978 年 1G 通信诞生以来，无线认证的安全性一直是首要问题。1G 几乎没有采取安全措施，移动台把其电子序列号（ESN）和网络分配的移动台识别号（MIN）以明文方式传送至网络，安全隐患极大。20 世纪 90 年代 2G 通信诞生了，但其安全机制都是基于私钥密码体制，即通过采用基于“挑战 – 响应”的共享秘密数据（私钥）的安全协议来实现对接入用户的认证和数据信息的保密。在此基础上，3G、4G 系统对该体制进行了较大改进，但仍然是基于私钥密码体制，难以实现用户数字签名。针对 4G 网络认证中存在的安全问题，5G 认证体系进行了修正，最典型的就是使用公私钥加密体制，增强了手机身份认证的安全性。由此可见，在 5G 时代，无线认证技术仍然沿用 70 年代的密码学原理。

2 无线物理层认证技术及其研究现状

2.1 无线物理层认证技术的产生

认证载体是无线认证技术中最关键的部分，认证载体既承载了认证所需信物、密钥等信息，又具有多样化的表现形式，例如印章、钥匙、签名、指纹、面部轮廓、语音声波、虹膜等。如图 2 所示，无线通信系统中的认证载体可大体分为 3 类：一类是针对密码加密算法体系的关键需求信息，主要分布于应用层面；另一类位于应用层与物理层之间，主要为协议所具备的特殊属性或部件；最后一类位于物理层，主要为与物理信号直接相关的载体，例如硬件差异（频偏、I/Q 偏移）引发的特殊信号、信道状态信息、接收信号强度指示（RSSI）等。根据认证载体的类别，移动通信的认证技术可概括为 3 类，具体包括基于密钥加密算法的高层认证机制、基于软件指纹的高层认证机制以及物理层认证。

伴随着攻击者计算能力的提升以及先进攻击方法的产生，高层认证的安全性受到极大威胁。例如，2019 年 9 月，谷歌公司宣告在全球首次实现“量子霸权”：其量子计算机仅用 200 s 就完成了世界第一超算 Summit 用 1 万年的时间才能完成的计算，计算能力提高了约 15 亿倍。根据侧信道分析攻击的原理，攻击者可以采用时序攻击的方式，基于测量一个执行单元所需的时间，获得有用信息，这些信息可以导致密钥的泄露；攻击者通过采用功耗攻击，可以对芯片电路功耗进行分析，达到攻击及非侵入性地从设备中提取加密密钥和其他机密信息的目的。此外，随着接入增加，高层认证所需的密钥分发管理更加困难，而且网络架构的复杂异构化将导致高层认证的架构兼容性更低。基于上述背景，物理层认证技术得到广泛而深入的研究。物理层认证技术通过基于物理层的特征属性来实现对身份和消息的认证，充分利用了底层信号特征属性，因而具备与高层协议透明的优良特性。除此之外，物理层认证技术还具备较高的协议架构兼容性、较高的协议灵活性以及较低的时延等特性。



▲图 2 无线认证技术研究的分类

2.2 无线物理层认证的信息论基础

最早的关于无线认证的信息论研究是以基于共享私密密钥的加密机制为基础，以实现无条件安全性为目标。C. E. SHANNON 最早在文献 [1] 中对密钥使用和私密性的性能刻画进行了理论建模。根据 SHANNON 的理论，如果密钥长度大于信息长度，合法收发端可以通过采用“一次一密”的方法使用密钥对信息进行加密，实现信息的完美私密性。然而，关于无线认证的无条件安全性研究可分为两类：一类为基于密码学的无条件安全认证；另一类为基于窃听信道模型的无条件安全认证。

对于第一类研究，G. J. SIMMONS 在文献 [2] 中最早建立了一个经典的无噪声无线认证模型：合法发射机与合法接收机共享一个密钥 K，合法发射机发射一个经过函数 f 加密的信息 M，$M=f(K,X)$，一个主动窃听者既可以窃听合法发射机的信息，又可以伪造或者篡改这些信息，并将新的错误信息发送至合法接收机，从而干扰合法接受机对信息的认证，最终合法接收机需要通过判断接收到的信息是否为 M 来识别其是否来自于合法发射机。针对该模型，J. CARTER 和 M. N. WEGAN 在文献 [3] 中证明了对于特定的信息可以实现无条件安全认证。该方案需要合法收发端根据共享私密密钥的指示，从一个大小为 B 的公共已知集合中选取双方认可的哈希函数作为加密函数 f，J. CARTER 和 WEGAN 在该文献中证明如果集合是全域的，攻击成功的概率为 $1/B$。U. M. MAURER 在文献 [4] 中证明了如果共享私密密钥不更新，非法攻击成功的概率会随着密钥使用次数的增加而提高。可以看到，以上研究并没有提及利用无线物理层信息来实现无线认证。

对于第二类研究，L. LAI 等首次在文献 [5] 中提出一个基于物理层信道的含噪无线认证模型，在 SIMMONS 提出模型的基础上，通过采用 A. WYNER 提出的基于窃听信道的信息传输方式，将无条件私密性的优势应用至无线认证中，实现了无条件安全认证 [6]。WYNER 窃听信道模型包含一个合法发射机、一个合法接收机和一个窃听端。其中，合法发射机的发送信息为 X，合法接收机端合法信道输出为 Y，窃听端窃听信道的输出 Z，系统最大私密速率可表示为 $\max I(X;Y)-I(X;Z)$。关于该模型的一个重要结论是：如果合法信道质量优于窃听信道质量，那么存在服从某一分布的 X 使得最大私密速率不为零，从而保障合法收发端的安全信息传输，并且使得窃听者从接收到的信号中获得不了任何信息。借助于该优势，LAI 等人在文中得到一个重要的结论：只要保障 $\max I(X;Y)-I(X;Z)$ 大于 0，就可以在噪声信道下实现共享私密密钥的多项式次复用，使窃听者的攻击效果不会随着密钥的使用次数增加而提升。然而，实际场景中 $\max I(X;Y)-I(X;Z)$ 大于 0 这一条件并不总是成立。因此，MAURER 在文献 [7] 中提出了一种利用合法收发端共享的

随机信息进行密钥生成的方法，弥补了对信道质量的严格要求。基于此，很多研究关注如何利用信道特征等机制进行密钥生成。

综上所述，关于无线认证的信息论研究都需要以收发端共享私密密钥为基本前提。如果研究过程中密钥的产生过程没有利用物理层信息，则可以认为该研究属于传统的高层认证；反之，该研究则为物理层认证的一个雏形。P. YU 等在文献 [8] 中通过利用哈希函数将物理层信息与共享私密密钥耦合生成一个标签或者消息认证码，之后将信息与消息认证码经由无线信道发送，合法接收端通过利用解调后的信息生成参考消息认证码，再通过对比参考消息认证码与无线接收的消息认证码，从而完成对信息的认证和提取。YU 的研究首次为物理层认证的研究提供了一个理论模型和技术框架。针对搭线窃听信道模型下的多信息认证问题，文献 [9] 提出了一种联合多信息认证和窃听信道安全传输的物理层水印信息论模型，从理论上给出了实现多信息无条件认证安全的条件，解释了物理层水印技术的性能界。上述有关无线认证信息论方面的研究工作为无线物理层认证的理论研究奠定了坚实的基础。

2.3 无线物理层认证技术的研究现状

根据采用的认证协议架构的不同，目前对无线物理层认证技术的研究可分为两大类：第一类方案以交互式协议架构为基础；第二类方案以非交互式协议架构为基础。如表 1 所示，第一类方案的综述包括物理层水印、物理层挑战响应、跨层认证以及基于物理层密钥交换的物理层认证技术。这类方案以共享私密密钥为基础，通过采用哈希函数加密和信号处理技术实现对共享私密密钥和信号内生特征的联合处理与利用，从而提升对合法设备信息认证的准确性。第二类方案的综述包括基于射频指纹的物理层认证技术和基于无线信道指纹的物理层认证技术。这类方案不依靠共享私密密钥，而是通过利用信号处理技术实现对信号内生特征的提取和利用，以提升对合法设备信息认证的准确性为目标。下面我们将分 6 个层面对这两类方案的研究现状进行综述，其中前 4 点都是关于第一类方案的综述，第 5、6 点是关于第二类方案的综述。

2.3.1 物理层水印

在各种物理层认证技术中，物理层水印是应用最为广泛的技术之一。在文献 [10] 中，合法发射端通过利用哈希函数加密共享私密密钥和目标信号形成标签，并将标签与无线信号叠加广播发送；合法接收端对接收到的信号进行估计并利用共享私密密钥得到参考标签，进一步通过对比参考标签与无线接收的标签，实现对目标信号的物理层认证。YU 等进一步推广该方法至多载波系统 [11] 并在软件无线电（SDR）平台上验证该系统 [12]。与此不同，N. GOERGEN 等在文献 [13] 中针对认知无线电系统提出了一种信号水印方案，将无线信道状态信息作为认证信号，通过利用预共享的数字签名来判定认证信号是否属于主用户信号。在文献 [10] 中，V. KUMAR 等提出了一种基于哈希算法和收发信号设计的物理层水印方法。在文献 [14] 中，KUMAR 等提出了一种基于星座旋转的物理层水印方法。在文献 [15] 中，Y. C. RAN 等针对物理层水印技术做了改进，通过使用随机的信道状态信息来替代共享私密密钥用于生成标签，形成了新的物理层认证方法。针对物联网设备，文献 [16] 提出了一种轻量级的物理层水印架构，通过设计轻便、高性能的共享私密密钥来保障标签的安全性以及标签与信息的独立性。

2.3.2 物理层挑战响应认证

关于物理层挑战响应认证技术的研究最早源于文献 [17]。该研究可以认为是高层认证在物理层面的安全增强，其基本思想为：发送方将一个随机信号（挑战）通过无线信道广播至目的端，目的端再根据密钥对接收信号变换（响应）并反向广播至发送端。发送端已知随机信号和密钥，因此可以利用信道的唯一性和互易性抵消掉随机信号并估计出密钥，并进一步根据估计的密钥是否与预期相同来判断目的端是否合法。物理层挑战响应认证本质上是一种通过联合设计密钥和信息传输方式来实现信息认证的机制。根据密钥的物理层形式和信息传输方式的不同，物理层挑战响应认证机制得到了推广和发展。文献 [18] 将传统的物理层挑战响应认证技术延伸至中继网络场景，提出了一种新型的物理层挑战响应认证机制。该机制利用不同信道的随机性和解相关特性来实现对响应分析和对目标身份的认证。针对主动感知型信息物理系统，文献 [19] 设计了基于无线信号转发的物理挑战

▼表 1 无线物理层认证技术已有研究综述分类

模型	物理层水印	物理层挑战响应	跨层认证	物理层密钥交换	射频指纹	无线信道指纹
交互式	√	√	√	√		
非交互式					√	√
基于密钥	√	√	√	√		
无密钥					√	√

响应认证机制来应对针对信息的欺骗攻击。文献 [20] 提出了一种基于多载波信道相位随机性和互易性的物理层挑战响应认证机制，该机制通过将共享私密密钥以相位的形式嵌入到收发信号来实现设备的身份认证。针对正交频分复用（OFDM）系统，文献 [21] 提出了一种基于人工噪声注入的物理层挑战响应认证机制，该机制通过人工噪声掩盖合法信道的相位信息，同时创造一种人工随机性来对抗窃听者，进而实现安全的设备身份认证。

2.3.3 跨层认证

跨层认证的基本出发点是实现物理层认证与高层认证的优势互补。文献 [22] 强调了跨层信息对于认证安全的重要性，特别是跨层认证可以利用物理层信道的富散射特性、随机性、互易性和时变性来弥补高层加密体制的不足。针对 IEEE 802.11 网络，文献 [23] 提出了一种基于媒体接入控制（MAC）层数据包和物理层接收信号强度的抗欺骗认证方案。针对异构网络中的机器类通信（MTC）设备，文献 [24] 提出了一种联合射频指纹和高层认证的跨层认证方案，通过高层认证机制保障设备的合法性，以及射频指纹来鉴别认证信息的真实性。针对移动认知无线电网络，文献 [25] 提出了一种联合信道射频指纹和高层认证的跨层认证方案。针对智能电网机器对机器（M2M）网络，文献 [26] 提出了一种双层接入认证框架，该框架通过高层认证保障无线接入过程设备的身份认证，并通过基于信道特性的物理层认证机制来保护接入信道测量，为接入数据的传输提供保障。

2.3.4 基于物理层密钥交换的物理层认证

在开放的无线接入环境中，高层认证密钥被长期多次使用因而很容易被窃听者窃取，这会导致认证的安全性丧失。虽然系统可以通过不断的密钥更新和迭代来解决这个问题，但仍然会带来不可容忍的网络开销。物理层密钥交换技术利用随机衰落信道的内生特征（随机性、唯一性和互易性）作为随机共享源来生成和分发密钥，弥补了高层密钥安全性不足的问题。物理层密钥的生成不需要消耗过多计算力，其安全性不依赖于计算的复杂度，而是与无线衰落信道的物理特性有关。除此之外，物理层密钥的分发更加简单、灵活。在文献 [7] 中，MAURER 提出了一种利用共享随机信息生成认证密钥的方法，奠定了基于物理层密钥交换技术的理论基础。一个关键问题是如何获取和选择随机源，J. E. HERSHEY 在文献 [27] 中将无线信道的唯一性、互易性等内生特征转化为双方共享的随机源。在时分双工系统中，合法信道上行和下行具有相同的信道内生特征，因而合法收发端可以共享相同的信道内生特征，通过将其作为共享随机源可以产生具备无条件安全性的物理层密钥。文献 [28–30] 分别提出了利用无线信道、预编码、空间调制等技术来实现物理层密钥交换。文献 [31] 提出了一种面向带内全双工技术的物理层密钥交换方案。针对毫米波大规模多输入多输出（MIMO）系统，文献 [32] 提出了一种基于虚拟到达角和离开角的物理层密钥交换机制。物理层密钥交换技术可以用于替代高层密钥，进而与其他基于高层密钥的物理层认证技术相结合。例如，针对 OFDM 系统，文献 [33] 提出了一种基于物理层密钥的物理层挑战响应认证机制，其中物理层密钥从合法收发端间的信道状态信息中获取。针对时分双工 OFDM 系统，文献 [34] 提出了一种基于无线信道相位信息估计的安全密钥生成机制来联合优化设计相位信息损失、安全密钥长度以及密钥的安全性。针对终端直通（D2D）中继网络，文献 [35] 则提出了一种基于社交信任和社交互易性的物理层密钥生成机制，采用博弈理论优化社交配对，从而最大化安全密钥生成速率。

2.3.5 基于射频指纹的物理层认证

上述 4 种方案合理运作的基本前提是维持合法收发端高层密钥和物理层密钥等共享私密密钥的完美私密性。与这些方案不同，基于射频指纹的物理层认证技术的核心思想是：将无线设备的硬件不完美信号特征（射频指纹）提取作为密钥，这些密钥因设备不同而不同，因而可以用于识别设备身份和检测非法用户；但是射频指纹数据库仍然可以被嗅探和学习，无法维持绝对的保密性。文献 [36] 验证了将该技术用于实际无线环境中鉴别无线设备身份的可行性。文献 [37] 从 OFDM IEEE 802.11a 无线信号的非瞬态前导码响应中提取双树复小波变换后的信号特征，在小波域建立了基于射频指纹的物理层认证机制。针对物联网设备，文献 [38] 提出了一种基于长短期记忆（LSTM）深度神经网络的射频指纹生成方法，利用无线信号的 I/Q 数据流之间的时间相关性，从大量的不完备硬件设备信号特征中训练得到可以用于识别低功率物联网设备的特征，从而保障合法设备的身份识别。针对无人机网络，文献 [39] 提出了一种基于信号能量瞬态的无人机物理层认证机制，通过能量域和时间域的信号处理技术提取无人机的信号特征，采用机器学习的方法对信号特征进行分类、识别，进而保障无人机的身份识别。文献 [40] 研究了基于频域稳态特征的射频指纹生成方法。考虑到每个设备时钟扭曲的唯一性，文

献 [41] 采用时钟扭曲测量值作为设备的特征标识并将其用于身份认证。文献[42]设计了一种物理不可克隆函数，基于该函数系统可以从无线设备的微电子芯片中利用导线和晶体管的随机时延特性来生成特征标识并将其用于身份认证。针对毫米波通信，文献 [43] 提出了一种基于波束赋形空时模式特征的物理层认证技术方案。针对物联网设备，文献 [44] 将基于射频指纹的物理层认证系统建模为一个具有解析表达式的输入输出系统，从而提供了一个通用性的设计思路，该方案不依赖数据同时具备高稳健性。针对物联网设备，文献 [45] 则提出了一种基于多采样卷积神经网络的射频信号特征提取的方法，解决了传统射频信号特征提取过程中出现不稳定兴趣域的相关问题。

2.3.6 基于无线信道指纹的物理层认证

正如文献 [8] 指出的结论：认证可以看作是一个假设检验过程。通过构建二元假设检验来判断攻击的发生或者识别设备身份是另一种研究思路。基于此，基于无线信道指纹的物理层认证技术的思想是：将不同无线信道具有的多样性、唯一性和随机性特征作为一种天然的“指纹”，通过指纹的变化或者人为的指纹特征扰动构建假设检验，进而实现设备身份认证。文献 [46] 利用两个不同地理位置上接收机频域信道解相关的特性，通过建立一个二元假设检验过程来鉴别相干时间内两条信道所承载的信息的来源。文献 [47] 通过比较相邻时刻信道频率响应的变化来判断发送方是否发生了变化，进而鉴别有无攻击威胁。文献 [48] 利用量化的时域信道冲击响应的信号幅度和相位等信息，构建二元假设检验过程。文献 [49] 通过对比无线接收信号强度的差值范围，实现移动场景中合法用户的身份认证。文献 [50] 通过将 OFDM 系统中当前时变载波偏移和偏移的预测进行对比，来实现设备身份认证。除此之外，文献 [51] 研究了二元假设检验过程中基于信道变化差值的自适应阈值优化方法。文献 [52] 通过对比不同地理位置上信号功率谱密度的差异性来实现不同位置设备的身份认证。文献 [53] 通过在不同无线帧之间注入人工噪声信号，使得不同时变信道下基于信号功率谱密度差异的二元假设检验更加高效，增强了身份认证的安全性。针对大规模 MIMO 系统，文献 [54] 提出了一种基于设备信道状态信息的二元假设检验，分析了不完美天线硬件特性对物理层认证机制的影响。文献 [55] 研究了基于极限学习机的物理层认证模型，通过联合利用无线信道的多维特征以及符合欺骗攻击模型的训练数据，提升对欺骗攻击者的安全检测性能。针对水声传感器网络，文献 [56] 提出了一种利用水声信道功率延迟谱，以区分不同传感器的物理层认证方案，该方案采用强化学习来选择身份认证参数，对网络和欺骗模型具备很高的透明性。针对车联网，文献 [57] 提出了一种用于抵御恶意边缘攻击者的物理层认证方案，该方案利用移动设备及其服务边缘共享的设备信道状态，通过强化学习、迁移学习和深度学习来达到身份认证参数选择、节省学习时间以及优化认证性能的目的。针对多用户多输入单输出 OFDM 系统，文献 [58–60] 设计了一种信号特征编码的多用户物理层认证协议，揭示了如何通过对信号内生特征进行编码来实现轻量级、低时延、高安全性的多用户导频信号物理层认证。针对车联网车辆到基础设施 OFDM 通信系统，文献 [61–62] 设计了物理层 Cover–Free 编码理论并构建了新型的多车辆物理层认证协议，揭示了如何在信号内生特征编码的环境下通过借助大规模天线的高空间分辨率来实现对攻击行为的精准检测、分离、识别和对攻击者的地理位置溯源，从而实现高安全、低时延的多车辆导频信号物理层认证。

3 未来无线物理层认证技术挑战

随着下一代空口技术、网络架构和业务场景的升级，研发新型无线物理层认证技术仍然是一个充满挑战的课题。

3.1 低时延物理层认证架构设计

传统的物理层认证协议大多基于交互式认证架构，随着网络接入架构的复杂化、异构化，在无线接入过程中不同交互式认证协议间切换开销急剧增加。除此之外，交互式架构下认证服务的等待时间参差不齐，在复杂传播环境下易引发过多的交互延迟。伴随着空口技术框架的革新，信号内生特征逐渐丰富，物理资源空间得到巨大扩充，为新型物理层认证协议架构的重新设计提供了更多的资源维度。然而，传统的物理层认证体系对这些特点鲜有关注。

3.2 高安全性物理层认证机制设计

传统的物理层认证协议机制依赖于共享私密密钥，在无线接入过程中，基于共享私密密钥的认证机制容易导致高交互延迟和弱计算安全性的问题；而基于物理资源空间的认证机制大都缺乏更为有效的资源信息，安全性能桎梏明显。随着下一代无线接入网络中信号与资源、协议特征的耦合性增强并表现出丰富的内生特征，用于认证的可用低维物理资源空间将得到极大的扩充。然而，传统的物理层认证体系对这些特点鲜有关注。

3.3 面向差异化安全保障能力的物理层认证协议设计

不同业务场景下具备不同安全保障能力的设备共存是下一代无线网络接入的一大特点，然而由于设备安全保障能力的差异化以及传统空口协议的固化，传统的无线接入物理层认证协议的安全性能控制相对僵化，难以保障具备不同安全保障能力的设备的安全性能。随着空口技术框架的革新，灵活的空口协议使得设备的安全保障能力得到显著提升，物理资源可以根据设备能力和安全需求进行灵活配置，因而赋予了物理资源使用和物理层认证协议设计更强的灵活性。然而，已有的物理层认证体系对这些特点鲜有关注。

4 未来物理层认证技术研究方向

经过 10 余年的发展，无线物理层认证技术得到了广泛研究和深入拓展。面向未来，无线物理层认证技术在如下几个研究方向存在巨大潜力。

4.1 基于信号内生特征的无线物理层认证技术

随着无线接入技术的革新、网络接入架构的复杂异构化以及用户接入设备数量和形态的急剧增多，空口技术、网络结构、设备能力都发生了巨大的变化。与此同时，信号内生特征逐渐丰富和多样化，不仅包括物理设备本身所具备和衍生的物理特性、与物理设备所连接的无线信道所具备和衍生的特征属性，还包括用户使用不同资源和协议时的模式特征等。然而，传统的信号特征处理方式难以深度挖掘和利用信号内生特征，表现为对信号内生特征的认知和处理能力不足，无法针对上述变化在架构、机制以及性能方面提供安全保障。实际中，无线信号从发射端经由无线信道传输至接收端的过程中会承载和记忆诸多来自于物理设备、无线信道和使用模式的特征，包括信号的能量特性、信道随机性和独立性等。如何通过对信号内生特征进行提取和编解码使得这些特征能安全地表征和传递信息，实现信息传递的同时保障信息的可逆认证是一个很有潜力的研究方向。

4.2 面向 5G 的安全、可靠、低时延无线物理层认证协议设计

5G 空口技术框架的革新引发了对无线物理层认证协议设计新的思考。5G 系统可根据不同的场景配置多种波形技术，实现灵活自适应的空口，增强系统对各种业务的支持能力，提高系统的灵活性和可扩展性。然而，波形的设计会直接影响信号的收发和传输，产生新的信号收发模型，为无线物理层认证设计提供新的环境和思路。

在无线接入方面，5G 引入了免调度竞争接入作为备选接入方式，通过引入免调度竞争接入机制，上行传输中设备的每次传输不再根据基站的上行授权来指示，进而设备与基站间的控制信令交互大幅度降低，极大地降低空口接入时延。然而，免调度竞争接入要求用户接入、信道训练和数据识别同时进行，引发了严重的安全问题，如何在免调度竞争接入环境中设计无线信号物理层认证协议来保障接入安全具有重要意义。

在业务场景方面，作为 5G 通信 3 大应用场景之一，超可靠低时延通信（URLLC）对应以自动驾驶、工业控制、远程医疗以及触感网络为代表的实时关键控制类业务。URLLC 的性能指标主要包括两个部分：时延和可靠性。不论是对于时延还是可靠性，无线信道状态信息的获取都起着至关重要的作用。如果无线信道状态信息的真实性被破坏，时延和可靠性必然会降低；因此如何设计无线物理层认证协议保障 URLLC 上行传输的信道状态信息是一项非常有意义的研究方向。

4.3 面向 6G 的无线物理层认证体系设计

未来 6G 将以 5G 的 3 大应用场景（大带宽、海量连接、超低延迟）为基础，实现“智慧连接”“深度连接”“全息连接”和“泛在连接”，为无线物理层认证体系的设计提供了全新的研究环境。在智慧连接方面，人工智能（AI）的安全性问题与 AI 技术本身相伴而生，特别是 AI 的安全识别机制，其直接影响和决定了 AI 技术的预期性能。因此，在 6G 的环境中，AI 问题将得到继承甚至强化，通过利用无线物理层认证技术可以充分挖掘无线信号的特征，从通信的角度来增强传输 AI 的安全性。在深度链接方面，6G 将关注触觉网络等方面的研究，通信设备及其连接对象将具备深度的感知、学习、实时的反馈与响应等功能。为此，6G 对低时延和高可靠的安全保障要求极高，如何利用无线物理层认证技术提取深度数据特征并且支持深度链接是一个潜在的研究方向。在全息连接方面，未来 6G 将媒体交互形式升级为全息信息交互，进而无线全息通信将成为现实。一方面，全息通信将提供更多的数据特征，为未来多因素无线物理层认证提供更多认证资源，提供更高的安全性水平。另一方面，全息通信对时延、可靠性、图像处理、智能化水平均有极高的要求，无线物理层认证技术未来有潜力满足这些要求。在泛在连接方面，由于大量不同类型的终端接入，有些终端设备能力强并具有一定的计算和存储能力，而有些终端设备甚至没有特定的硬件来安全存储身份标识及认证凭证。因此需要结合具体的业务场景，设计出灵

活的无线接入物理层认证协议以支持差异化的安全保障能力。

5 结束语

物理层认证技术为未来通信中的信息认证提供了高效可靠的保障。本文回顾了无线物理层认证技术研究的最新进展和成果。尽管现有的研究已经给出了多种安全认证策略，但是由于未来无线网络中空口技术、网络架构和业务场景的新特性，现有的研究尚难以为未来无线认证提供全方位的安全防护，因此还有大量的研究工作需要开展。此外，以下研究主题也值得关注：一是研究基于信号内生特征的无线物理层认证技术，提升物理层认证的安全性；二是研究面向 5G 的安全、可靠、低时延无线物理层认证协议设计；三是研究面向 6G 的无线物理层认证体系设计，充分挖掘 6G 的潜在认证资源，为未来无线接入认证提供安全保障。

参考文献

[1] SHANNON C E. Communication theory of secrecy systems [J]. Bell system technical journal, 1949, 28(4): 656–715. DOI: 10.1002/j.1538–7305.1949.tb00928.x

[2] SIMMONS G J. Authentication theory/coding theory [M]. Advances in cryptology. Berlin, Heidelberg: Springer Berlin Heidelberg. DOI: 10.1007/3–540–39568–7_32

[3] CARTER J, WEGMAN M N. Universal classes of hash functions [J]. Journal of computer and system sciences, 1979, 18(2): 143–154. DOI: 10.1016/0022–0000(79)90044–8

[4] MAURER U M. Authentication theory and hypothesis testing [J]. IEEE transactions on information theory, 2000, 46(4): 1350–1356. DOI: 10.1109/18.850674

[5] LAI L F, EL GAMAL H, POOR H V. Authentication over noisy channels [J]. IEEE transactions on information theory, 2009, 55(2): 906–916. DOI:10.1109/tit.2008.2009842

[6] WYNER A D. The wire–tap channel [J]. Bell system technical journal, 1975, 54(8): 1355–1387. DOI: 10.1002/j.1538–7305.1975.tb02040.x

[7] MAURER U M. Secret key agreement by public discussion from common information [J]. IEEE transactions on information theory, 1993, 39(3): 733–742. DOI: 10.1109/18.256484

[8] YU P L, BARAS J S, SADLER B M. Physical–layer authentication [J]. IEEE transactions on information forensics and security, 2008, 3(1): 38–51. DOI: 10.1109/tifs.2007.916273

[9] CHEN D J, ZHANG N, CHENG N, et al. Physical layer based message authentication with secure channel codes [J]. IEEE transactions on dependable and secure computing, 2019: 1. DOI: 10.1109/tdsc.2018.2846258

[10] KUMAR V, PARK J M J, BIAN K G. PHY–layer authentication using duobinary signaling for spectrum enforcement [J]. IEEE transactions on information forensics and security, 2016, 11(5): 1027–1038. DOI: 10.1109/tifs.2016.2516904

[11] YU P L, BARAS J S, SADLER B M. Multicarrier authentication at the physical layer [C]//2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks. Newport Beach, CA, USA: IEEE, 2008: 1–6. DOI: 10.1109/wowmom.2008.4594926

[12] VERMA G, YU P, SADLER B M. Physical layer authentication via fingerprint embedding using software–defined radios [J]. IEEE access, 2015, 3: 81–88. DOI: 10.1109/access.2015.2398734

[13] GOERGEN N, CLANCY T C, NEWMAN T R. Physical layer authentication watermarks through synthetic channel emulation [C]//2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN). Singapore, Singapore: IEEE, 2010: 1– 7. DOI: 10.1109/dyspan.2010.5457897

[14] KUMAR V, PARK J M J, CLANCY T C, et al. PHY–layer authentication using hierarchical modulation and duo binary signaling [C]//2014 International Conference on Computing, Networking and Communications (ICNC). Honolulu, HI, USA: IEEE, 2014: 782–786. DOI: 10.1109/iccnc.2014.6785436

[15] RAN Y C, AL–SHWAILY H, TANG C Q, et al. Physical layer authentication scheme with channel based tag padding sequence [J]. IET communications, 2019, 13(12): 1776–1780. DOI: 10.1049/iet–com.2018.5749

[16] ZHANG P C, LIU J, SHEN Y L, et al. Lightweight tag–based PHY–layer authentication for IoT devices in smart cities [J]. IEEE Internet of things journal, 2020, 7(5): 3977–3990. DOI: 10.1109/jiot.2019.2958079

[17] 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. DOI: 10.1109/jsac.2013.130914

[18] DU X R, SHAN D, ZENG K, et al. Physical layer challenge–response authentication in wireless networks with relay [C]//IEEE INFOCOM 2014–IEEE Conference on Computer Communications. Toronto, ON, Canada: IEEE, 2014: 1276–1284. DOI: 10.1109/infocom.2014.6848060

[19] SHOUKRY Y, MARTIN P, YONA Y, et al. Pycra: physical challenge–response authentication for active sensors under spoofing attacks [C]//the 22nd ACM SIGSAC Conference on Computer and Communications Security. USA: IEEE, 2015: 1004–1015. DOI: 10.1145/2810103.2813679

[20] WU X F, YANG Z. Physical–layer authentication for multi–carrier transmission [J]. IEEE communications letters, 2015, 19(1): 74–77. DOI: 10.1109/lcomm.2014.2375191

[21] WU X F, YANG Z, LING C, et al. Artificial–noise–aided physical layer phase challenge–response authentication for practical OFDM transmission [J]. IEEE transactions on wireless communications, 2016, 15(10): 6611–6625. DOI: 10.1109/twc.2016.2586472

[22] MATHUR S, REZNIK A, YE C X, et al. Exploiting the physical layer for enhanced security [J]. IEEE wireless communications, 2010, 17(5): 63–70. DOI: 10.1109/mwc.2010.5601960

[23] HAO P, WANG X B, REFAEY A. An enhanced cross–layer authentication mechanism for wireless communications based on PER and RSSI [C]//2013 13th Canadian Workshop on Information Theory. Toronto, Canada: IEEE, 2013:44–48. DOI: 10.1109/cwit.2013.6621590

[24] ZHAO C, HUANG L, ZHAO Y, et al. Secure machine–type communications toward LTE heterogeneous networks [J]. IEEE wireless communications, 2017, 24(1): 82–87. DOI: 10.1109/MWC.2017.1600141WC

[25] LE T N, CHIN W L, KAO W C. Cross–layer design for primary user emulation attacks detection in mobile cognitive radio networks [J]. IEEE communications letters, 2015, 19(5): 799–802. DOI: 10.1109/lcomm.2015.2399920

[26] CHIN W L, LIN Y H, CHEN H H. A framework of machine–to–machine authentication in smart grid: a two–layer approach [J]. IEEE communications magazine, 2016, 54(12): 102–107. DOI: 10.1109/mcom.2016.1600304cm

[27] HERSHEY J E, HASSAN A A, YARLAGADDA R. Unconventional cryptographic keying variable management [J]. IEEE transactions on communications, 1995, 43(1): 3–6. DOI: 10.1109/26.385951

[28] JORSWIECK E, TOMASIN S, SEZGIN A. Broadcasting into the uncertainty: authentication and confidentiality by physical–layer processing [J]. Proceedings of the IEEE, 2015, 103(10): 1702–1724. DOI: 10.1109/jproc.2015.2469602

[29] TAHA H S, ALSUSA E. Secret key exchange using private random precoding in MIMO FDD and TDD systems [J]. IEEE transactions on vehicular technology, 2017, 66(6): 4823–4833. DOI: 10.1109/tvt.2016.2611565

[30] TAHA H, ALSUSA E. Secret key exchange and authentication via randomized spatial modulation and phase shifting [J]. IEEE transactions on vehicular technology, 2018, 67(3): 2165–2177. DOI: 10.1109/TVT.2017.2764388

[31] VOGT H, AWAN Z H, SEZGIN A. Secret–key generation: full–duplex versus half–duplex probing [J]. IEEE transactions on communications, 2019, 67(1): 639–652. DOI: 10.1109/tcomm.2018.2868714

[32] JIAO L, TANG J, ZENG K. Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel [C]//2018 IEEE Conference on Communications and Network Security (CNS). Beijing, China. IEEE, 2018: 1–9. DOI: 10.1109/cns.2018.8433175

[33] CHOI J. A coding approach with key–channel

randomization for physical–layer authentication [J]. IEEE transactions on information forensics and security, 2019, 14(1): 175–185. DOI:10.1109/tifs.2018.2847659
[34] PENG Y X, WANG P, XIANG W, et al. Secret key generation based on estimated channel state information for TDD–OFDM systems over fading channels [J]. IEEE transactions on wireless communications, 2017, 16(8): 5176–5186. DOI: 10.1109/twc.2017.2706657
[35] WAQAS M, AHMED M, LI Y, et al. Social–aware secret key generation for secure device–to–device communication via trusted and non–trusted relays [J]. IEEE transactions on wireless communications, 2018, 17(6): 3918–3930. DOI: 10.1109/twc.2018.2817607
[36] DANEV B, CAPKUN S. Transient–based identification of wireless sensor nodes [C]//2009 International Conference on Information Processing in Sensor Networks. USA, 2009: 25–36
[37] KLEIN R W, TEMPLE M A, MENDENHALL M J. Application of wavelet–based RF fingerprinting to enhance wireless network security [J]. Journal of communications and networks, 2009, 11(6): 544–555. DOI: 10.1109/jcn.2009.6388408
[38] DAS R, GADRE A, ZHANG S H, et al. A deep learning approach to IoT authentication [C]//2018 IEEE International Conference on Communications (ICC). Kansas City, USA: IEEE, 2018: 1–6. DOI:10.1109/icc.2018.8422832
[39] EZUMA M, ERDEN F, ANJINAPPA C K, et al. Micro–UAV detection and classification from RF fingerprints using machine learning techniques [C]//2019 IEEE Aerospace Conference. Big Sky, MT, USA: IEEE, 2019: 1–13. DOI: 10.1109/aero.2019.8741970
[40] KENNEDY I O, SCANLON P, MULLANY F J, et al. Radio transmitter fingerprinting: a steady state frequency domain approach [C]//2008 IEEE 68th Vehicular Technology Conference. Calgary, Canada: IEEE, 2008: 1–5. DOI: 10.1109/vetecf.2008.291
[41] KOHNO T, BROIDO A, CLAFFY K C. Remote physical device fingerprinting [J]. IEEE transactions on dependable and secure computing, 2005, 2(2): 93–108. DOI: 10.1109/tdsc.2005.26
[42] SUH G E, DEVADAS S. Physical unclonable functions for device authentication and secret key generation [C]//2007 44th ACM/IEEE Design Automation Conference. San Diego, CA, USA: IEEE, 2007: 9–14. DOI: 10.1109/dac.2007.375043
[43] BALAKRISHNAN S, GUPTA S, BHUYAN A, et al. Physical layer identification based on spatial–temporal beam features for millimeter–wave wireless networks [J]. IEEE transactions on information forensics and security, 2020, 15: 1831–1845. DOI: 10.1109/tifs.2019.2948283
[44] ZHENG T H, SUN Z, REN K. FID: function modeling–based data–independent and channel–robust physical–layer identification [C]//IEEE INFOCOM 2019–IEEE Conference on Computer Communications. Paris, France: IEEE, 2019: 199–207. DOI: 10.1109/infocom.2019.8737597
[45] YU J B, HU A Q, LI G Y, et al. A robust RF fingerprinting approach using multisampling convolutional neural network [J]. IEEE Internet of things journal, 2019, 6(4): 6786–6799. DOI: 10.1109/jiot.2019.2911347
[46] XIAO L, GREENSTEIN L, MANDAYAM N, et al. Using the physical layer for wireless authentication in time–variant channels [J]. IEEE transactions on wireless communications, 2008, 7(7): 2571–2579. DOI: 10.1109/twc.2008.070194
[47] XIAO L, GREENSTEIN L, MANDAYAM N, et al. A physical–layer technique to enhance authentication for mobile terminals [C]//2008 IEEE International Conference on Communications. Beijing, China: IEEE, 2008: 1520–1524. DOI: 10.1109/icc.2008.294
[48] LIU F J, WANG X B, PRIMAK S L. A two dimensional quantization algorithm for CIR–based physical layer authentication [C]//2013 IEEE International Conference on Communications (ICC). Budapest, Hungary: IEEE, 2013: 4724–4728. DOI: 10.1109/icc.2013.6655319
[49] ZENG K, GOVINDAN K, MOHAPATRA P. Non–cryptographic authentication and identification in wireless networks [J]. IEEE wireless communications, 2010, 17(5): 56–62. DOI: 10.1109/mwc.2010.5601959
[50] HOU W K, WANG X B, CHOUINARD J Y, et al. Physical layer authentication for mobile systems with time–varying carrier frequency offsets [J]. IEEE transactions on communications, 2014, 62(5): 1658–1667. DOI: 10.1109/tcomm.2014.032914.120921
[51] LIU J Z, REFAEY A, WANG X B, et al. Reliability enhancement for CIR–based physical layer authentication [J]. Security and communication networks, 2015, 8(4): 661–671. DOI: 10.1002/sec.1014
[52] TUGNAIT J K. Wireless user authentication via comparison of power spectral densities [J]. IEEE journal on selected areas in communications, 2013, 31(9): 1791–1802. DOI: 10.1109/jsac.2013.130912
[53] TUGNAIT J K. Using artificial noise to improve detection performance for wireless user authentication in time–variant channels [J]. IEEE wireless communications letters, 2014, 3(4): 377–380. DOI: 10.1109/lwc.2014.2318731
[54] ZHANG P C, TALEB T, JIANG X H, et al. Physical layer authentication for massive MIMO systems with hardware impairments [J]. IEEE transactions on wireless communications, 2020, 19(3): 1563–1576. DOI: 10.1109/twc.2019.2955128
[55] WANG N, JIANG T, LV S, et al. Physical–layer authentication based on extreme learning machine [J]. IEEE communications letters, 2017, 21(7): 1557–1560. DOI: 10.1109/lcomm.2017.2690437
[56] XIAO L, SHENG G Y, WAN X Y, et al. Learning–based PHY–layer authentication for underwater sensor networks [J]. IEEE communications letters, 2019, 23(1): 60–63. DOI: 10.1109/lcomm.2018.2877317
[57] LU X Z, XIAO L, XU T W, et al. Reinforcement learning based PHY authentication for VANETs [J]. IEEE transactions on vehicular technology, 2020, 69(3): 3068–3079. DOI: 10.1109/tvt.2020.2967026
[58] XU D Y, REN P Y, RITCEY J A. Independence–checking coding for OFDM channel training authentication: protocol design, security, stability, and tradeoff analysis [J]. IEEE transactions on information forensics and security, 2019, 14(2): 387–402. DOI: 10.1109/tifs.2018.2850334
[59] XU D Y, REN P Y, RITCEY J A. Code–frequency block group coding for anti–spoofing pilot authentication in multi–antenna OFDM systems [J]. IEEE transactions on information forensics and security, 2018, 13(7): 1778–1793. DOI: 10.1109/TIFS.2018.2800696
[60] XU D Y, REN P Y, RITCEY J A. Hierarchical 2–D feature coding for secure pilot authentication in multi–user multi–antenna OFDM systems: a reliability bound contraction perspective [J]. IEEE transactions on information forensics and security, 2019, 14(3): 592–607. DOI: 10.1109/TIFS.2018.2859585
[61] XU D Y, REN P Y, RITCEY J A. PHY–layer cover–free coding for wireless pilot authentication in IoV communications: protocol design and ultra–security proof [J]. IEEE Internet of things journal, 2019, 6(1): 171–187. DOI: 10.1109/jiot.2018.2878333
[62] XU D Y, REN P Y, RITCEY J A. Reliability and accessibility of low–latency V2I channel training protocol using cover–free coding: win–win or tradeoff? [J]. IEEE transactions on vehicular technology, 2019, 68(3): 2294–2305. DOI: 10.1109/tvt.2019.2891295

作 者 简 介

任品毅，西安交通大学教授，无线通信研究所所长；主要研究领域为无线物理层安全传输、5G与网络、认知无线网络、卫星通信与组网、信号检测、分布式网络等；先后主持和参与30余项国家级课题，在“十一五”期间被聘为国家高技术研究发展计划（“863”计划）“频谱共享无线通信系统”重点项目总体专家组副组长；发表论文150余篇，出版译著10余本，以第一发明人获国家发明专利30余项，登记国家计算机软件著作权7项。

徐东阳，西安交通大学讲师；主要研究领域为无线物理层认证技术、5G、编码理论等；2017年获《China Communications》首届最佳论文奖；发表论文20余篇。