面向 6G 智能终端身份鉴别技术

夏仕达，徐瑨，陶小峰
（北京邮电大学移动互联网安全技术国家工程实验室，北京 100876）

摘　要：智能终端将极大地拓展 6G 的应用，也使 6G 面临更大的安全威胁，实现可靠的终端身份鉴别是保证 6G 网络安全的前提。针对 6G 网络架构与终端特点，归纳了身份鉴别技术在面向 6G 智能终端时的挑战与需求；进一步分析了面向 6G 智能终端身份鉴别的发展趋势；最后，探索了物理层认证在 6G 网络智能终端身份鉴别中的可能实现机制。

关键词：智能终端；6G；身份鉴别；物理层认证
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2020.00159

Intelligent terminal identification technology toward 6G

XIA Shida, XU Jin, TAO Xiaofeng
National Engineering Lab for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: The intelligent terminal will greatly expand the applications of 6G. However, it will also make 6G face with greater security threats. The reliable terminal identification technology is the premise to ensure the security of 6G networks. Firstly, based on the network architecture and terminal characteristics, the requirements and challenges of 6G intelligent terminal identification were summarized. Then, the development trend was put forward for 6G intelligent terminal identification. Finally, physical layer authentication was explored to achieve possible realization of intelligent terminal identity authentication mechanism in 6G networks.

Key words: intelligent terminal, 6G, identification, physical layer authentication

1　引言

6G 网络将成为 2030 年智能信息社会的主要推动力，太赫兹、毫米波、全息无线电、人工智能（AI, artificial intelligence）、超大规模天线阵列、区块链、可见光通信、量子通信等一系列新技术将应用于 6G 网络设计中[1]，使网络功能更加完备。卫星网络、地面蜂窝网络、海洋网络将深度融合，为移动终端提供无处不在的接入服务[2]。网络服务将不局限于个人通信业务，还将提供自动驾驶、智能工业等其他垂直行业服务[3]。6G 网络的影响力将从个人通信业务发展至各行各业。

6G 网络的网络架构和终端类型将发生质的变化。6G 网络将全面实现所有终端（包括人与物、物与物）之间的智能通信，并提供无处不在的通信支持，网络范围进一步延伸，地面网络、卫星网络、海上网络以及深海网络等网络深度融合，形成空天地海一体化的超异构网络体系[4]。6G 网络终端智能化水平不断提高，从智能手机演进至智能汽车、智能医疗器械、智能机器人、智能物联网设备、智能工业设备、智能家居设备等[5]。

随着无线网络影响力的增强，网络安全问题更加严峻，特别是无线接入终端的身份鉴别问题，异常的终端接入所带来的影响超出了通信行业本身

收稿日期：2020–02–20；**修回日期：**2020–03–08
通信作者：陶小峰，taoxf@bupt.edu.cn
基金项目：国家自然科学基金资助项目（No.61932005，No.61901051，No.61601051）
Foundation Item: The National Natural Science Foundation of China (No. 61932005, No.61901051, No.61601051)

异常的影响。如一辆不安全的智能驾驶汽车接入网络后，会上报错误的路况信息，造成严重的车祸事故[6]。因此，实现可靠的终端身份鉴别成为未来 6G 网络设计的重中之重。

6G 超异构的网络架构使得终端身份鉴别面临更大的挑战，体现在两个方面：1) 终端将在异构网络之间频繁切换，由于异构网络身份鉴别技术不同，终端在进行网络切换时，难以在不中断业务的情况下完成鉴别切换[7]；2) 随着量子计算的不断成熟，攻击者可以针对 6G 网络中的薄弱环节进行攻击，威胁密钥的安全性[8]。

异构化的智能终端拓展了 6G 网络的应用，也带来了一定的安全挑战：首先，终端的智能化水平存在差异，表现出不同的计算、存储和分析能力，一旦智能化水平低的终端被攻击者控制，会严重损害网络安全性[9]；其次，一种终端鉴别机制难以在所有类型的智能终端上执行，特别是智能化程度低的终端没有特定的存储设施来存储复杂的身份标识和认证凭证，使得传统的终端鉴别机制无法正常执行[10]。

面向 6G 智能终端身份鉴别技术的核心是自适应网络架构和终端能力，智能地为网络提供安全接入服务。为了保证终端能够在异构接入网络频繁的切换过程中保持身份鉴别的连贯性，6G 终端身份鉴别体系需要考虑不同网络的资源约束和网络需求等条件，联合优化鉴别机制的效率，以降低“木桶效应”对网络终端身份鉴别带来的影响[11]。从另一个角度看，6G 网络需要根据终端不同的智能化程度设计不同的鉴别技术，形成分级身份鉴别机制[12]，保证多种智能终端的不同鉴别机制可以联合地在 6G 网络中运行。

2 传统终端身份鉴别技术

在 2G 中，终端身份鉴别分为两大类，即全球移动通信（GSM, global system for mobile communication）系统鉴权[13]与码分多址（CDMA, code division multiple access）系统鉴权[14]。其中，GSM 鉴权是防止未授权的用户接入 GSM，基本原理是密钥协商协议。基站通过协商协议生成的鉴权响应（SRES, signed response）实现对终端的接入认证。CDMA 系统鉴权则是通过密钥和随机数计算，生成一个鉴权验证值来确定接入终端的身份。这两种终端身份鉴别技术并未充分考虑对信息篡改和伪造问题的防护，仅通过加密使攻击者无法获取明文的内容[15]。但是，攻击者可以通过最终用户实现对密钥的破解。

在此基础上，3G 采用可扩展的认证和密钥协商协议（EAP-AKA, extensible authentication protocol-authentication and key agreement）完成终端身份鉴别[16]。该协议通过加密算法和完整性密钥协商实现信令、语音和数据的完整性保护，增加了系统的灵活性。然而，该协议的复杂度较高，会产生较大的时延。此外，3G 网络没有对网络内部用户的通信链路进行保护，内部攻击者可以通过截获其他用户的认证向量进行攻击[17]。

4G 采用演进分包系统认证与密钥协商协议（EPS-AKA, evolved packet system authentication and key agreement）[18]来降低鉴权的复杂度和时延。EPS-AKA 鉴权将 4G 网络接入层和非接入层的信令分离，分别为接入网和核心网分配不同的密钥，防止内部用户攻击。然而，EPS-AKA 协议依旧存在安全隐患，如根密钥是永久性密钥，攻击者通过学习大量的鉴权参数可以对根密钥进行估计。一旦根密钥泄露，4G 网络对攻击者缺乏有效的反制措施。其次，EPS-AKA 采用对称密钥机制，在鉴权认证之前，信令以明文形式进行传输，容易导致终端信息泄露[19]。

5G 采用双向认证机制，包括 EAP-AKA'[20]协议和 5G AKA[21]协议。EAP-AKA'协议和 5G AKA 协议在整体架构设计上基本一致，只是其中的某些函数略有修改。针对 4G 网络中的安全问题，5G 鉴权协议做出了针对性修改：为了应对重放攻击，引入时间计数序列号（SQN, sequence number）用于确保质询消息的有效性；为了防止终端身份被窃听者追踪捕获，引入非对称加密技术[22]，代表真实身份的永久标识符（SUPI, subscription permanent identifier）通过公钥加密后得到密文隐藏标识符（SUCI, subscription concealed identifier）再上传至基站，从而防止终端的国际移动用户识别码（IMSI, international mobile subscriber identity）信息被截获，这也是 5G 鉴权协议的一大亮点。

基于密钥的鉴权经过不断改进，表现出良好的终端身份鉴别性能。然而，随着 6G 网络的演进，当前鉴权协议难以满足 6G 网络智能终端身份鉴别的安全要求[22]。终端身份鉴别机制的演进过程如表 1 所示，针对网络特点、网络组成和终端类型的演变，6G 网络的终端身份鉴别向智能化、分级化方向发展，以适应 6G 网络超异构的特点，实现不同网络切换下终端身份鉴别的无缝转换。

表 1　　**终端身份鉴别机制的演进过程**

	4G	5G	6G
网络特点	扁平化网络、全 IP 结构	云化、边缘化、软件化、虚拟化、切片化	智能化
网络组成	蜂窝网	地面网络、垂直行业	地面网络、太空网络、深海网络
终端类型	智能手机	智能终端	泛在、智能、轻量、共享、融合的智能终端
鉴权机制	EPS-AKA	EAP-AKA' 5G AKA	智能认证机制
特点	分级密钥 双向鉴权 明文传输身份信息	非对称密码体制 保护鉴权时间有效性 时延无法满足要求 缺乏鉴权连续性管理 缺乏统一鉴权管理	自适应安全需求 自适应鉴权算法选择 智能化鉴权切换 统一鉴权管理

3　终端身份鉴别技术展望

伴随“内生安全”理念的提出，未来 6G 网络智能终端的身份鉴别将不仅包含基于密钥的身份鉴别，还会与 6G 网络的设计结合，当前探讨 6G 网络智能终端身份鉴别是有必要的。近年来，已有学者研究物理层认证技术[23-25]和区块链认证技术[26-28]实现智能终端身份鉴别的可能性，终端身份鉴别技术对比如表 2 所示。

物理层认证技术充分利用了无线通信中的物理信道和终端硬件特征的随机性，构造基于物理层特征的身份标识鉴别终端身份，由于攻击者难以预测并伪造信号的物理层特征，物理层认证具有较强的安全性[23]。物理层认证核心是将对数据和信令的认证转移到对无线信道的认证。物理层认证的实现分为两种：1) 将接收信号的物理层特征作为身份标识符，利用合法用户和攻击者之间的物理层特征差异，实现对终端身份的鉴别[24]；2) 与传统的密钥认证方式结合，在密钥生成的过程中，引入无线信道的随机性，密钥会随着无线信道的变化而更新，从而实现高安全性的身份鉴别[25]。

虽然物理层认证表现出安全性高、复杂度低、通用性强的优势，但是其可靠性低、稳健性差以及无法保证数据完整性的缺点限制了其大规模部署。因此，提高物理层认证的可靠性和稳健性是面向 6G 网络的终端身份鉴别亟待解决的问题，特别是智能汽车、智能工业等 6G 垂直行业。此外，数据完整性保护对于面向 6G 网络的智慧医疗等垂直行业至关重要，将成为物理层认证中与 6G 网络结合的研究重点之一。

区块链认证技术是一种多个终端的群组鉴别方式，各个节点通过共识机制和竞争计算更新区块链，如果一个节点的信息受到篡改，则该节点不能继续参与更新，而其他节点间的通信不会受到影响[26]。区块链认证的核心是通过非对称加密算法保证接入终端应用数据的安全性[27]。区块链的数据层包含哈希、时间戳等函数，保证信息不可篡改，网络层定义了终端的鉴别机制，共识层为区块链中的所有终端提前约定好一种鉴别共识，激励层激励区块链中的所有终端积极参与鉴别工作，合约层主要包含各种智能鉴别的算法和智能合约[28]。在智能合约中，系统预先设定了响应条件和触发条件，一旦存

表 2　　**终端身份鉴别技术对比**

	密钥鉴权	物理层认证	区块链认证
原理	密钥协商协议	物理层特征认证	非对称加密和智能合约
主要作用	终端接入保护、数据完整性保护	终端接入保护	数据完整性保护
优势	稳定性强 可靠性高	安全度高 复杂度低 通用性强	信息无法篡改 隐私保护
挑战	复杂度高 通用性差	可靠性差 稳健性低 无法保护数据完整性	保证节点可信度 大规模部署下时延高

在异常终端的数据接入网络，终端检测机制会自动激活，并定位到具体的终端。

区块链认证技术能够有效鉴别接入终端中的异常用户，提供数据完整性保护。在面向 6G 网络的智能家居、智能机器人等相关产业中，不可信终端的参与会极大地破坏区块链认证的执行效率，实现所有参与用户的可信管理是区块链认证技术在 6G 网络中应用的前提。此外，超高密度的终端接入是面向 6G 网络应用的一大特点，但大规模的终端接入使得区块链认证的时延显著提高。因此，提高执行效率、降低计算复杂度成为区块链认证技术未来的研究热点之一。

4　面向 6G 智能终端的物理层认证技术

本节围绕物理层认证技术展开，探索其在 6G 网络中的应用。由于安全性较高、复杂度较低的特点，物理层认证技术近年来成为无线网络身份安全的一个重要发展方向，是 6G 网络智能终端身份鉴别的一个可行方案。相较于传统基于密钥的认证协议，物理层认证的优势体现在：1) 安全性高，物理层认证的本质是认证时变性和随机性较强的无线信道，具有量子计算能力的攻击者也难以实时破解并追踪合法用户的物理层特征；2) 计算和通信开销低，通信双方不需要进行额外的信令交互即可完成认证，适用于 6G 网络超低时延的通信需求；3) 通用性强，其认证机制对通信协议交互的依赖程度小，适用于 6G 网络的超异构架构；4) 可以实现密集终端的群组认证，符合 6G 网络超密集终端接入的特点。

首先，研究了物理层认证的两种基本模型：基于物理层特征的加密认证和基于物理层特征的比较认证。其次，针对 6G 网络智能化的特点，探索了未来 6G 网络中的物理层认证增强技术。

4.1　基于物理层特征的加密认证

基于物理层特征的加密认证的基本原理为：发送端通过物理层特征对信号进行加密，接收端利用信道互异性完成信号解密，从而完成认证过程[29-30]。基于物理层特征的加密认证流程如图 1 所示，该认证加密的核心在于通过物理层特征对鉴权信号进行加密，可表示为

$$S(t)=f_H(\boldsymbol{x}(t)) \tag{1}$$

其中，$\boldsymbol{x}(t)$ 为核心网向基站响应的鉴权向量，$f_H(\cdot)$ 为与信道特征关联的加密函数，$S(t)$ 为鉴权信息的密文形式。可以看出，只有合法用户可以生成解密函数 $f_H^{-1}(\cdot)$ 完成身份的认证过程。该认证机制的核心在于将物理层特征作为密钥，完成认证过程。由于物理层特征与用户位置以及发送设备直接相关，具有时变性，因此，难以被攻击者破解。

基于物理层特征的加密认证充分利用无线信道的时变性，实现了动态密钥更新，可有效抵御 6G 网络中计算能力强的攻击者，增强了 6G 网络终端身份鉴别的可靠性。由于太赫兹被认为是 6G 网络可能的通信频段之一，其信道衰减更强，信道估计误差更大，收发双方的信道互异性难以得到满足，该机制需要进一步提升稳健性，消除信道估计误差对认证性能的影响。其次，实时更新物理层特征密钥会给 6G 网络引入较大的计算开销和通信开销，在面向 6G 网络应用时，基于物理层特征的密钥认证技术需要建立一个统一资源、性能和安全需求的

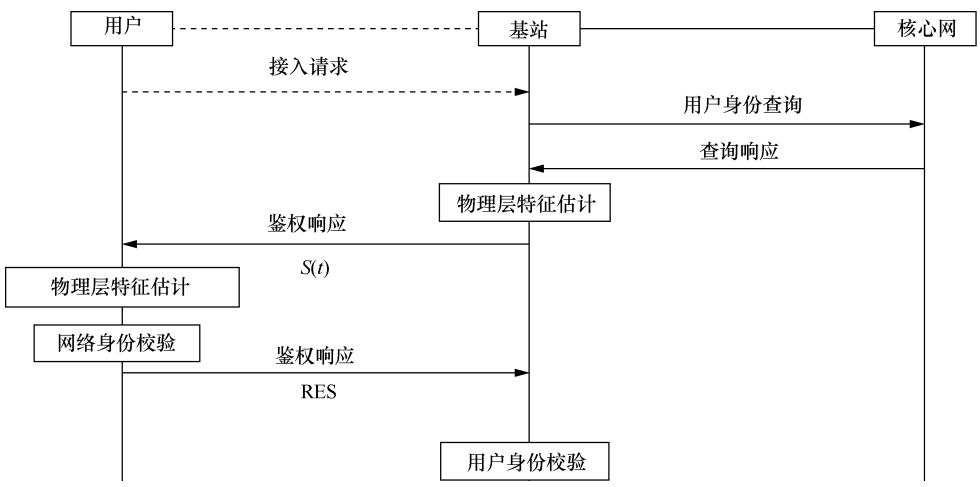

图 1　基于物理层特征的加密认证流程

管理体系。基于上述特点，基于物理层特征的加密认证在 6G 网络中将主要应用于计算资源丰富、安全需求较高的通信场景，如智慧医疗、智能工业等。

4.2　基于物理层特征的比较认证

基于物理层特征的加密认证需要精确估计信道来保证加密函数和解密函数的互反性，该过程会引入较大的计算复杂度，不适用于时延敏感场景[31]。因此，本节研究了一种轻量级的基于物理层特征的比较认证。

基于物理层特征的比较认证的基本原理为：以物理层特征作为接收信号的身份标识符，通过比较接收信号的身份标识符与参考向量，认证接收信号的身份[32-33]。基于物理层特征的比较认证流程如图 2 所示，该认证方式的核心是比较接收信号的物理层特征与参考特征的相似度

$$d(H(t),\boldsymbol{H}_r)=|H(t)-\boldsymbol{H}_r| \tag{2}$$

其中，$H(t)$ 表示当前接收信号的物理层特征，$\boldsymbol{H}_r$ 表示参考向量。$d(H(t),\boldsymbol{H}_r)$ 越小表示相似度越大，即当前时刻信号来自合法用户的概率更大。基于物理层特征的比较认证具有较低的复杂度和通信开销，但该机制没有对信息隐私性和完整性进行保护。

基于物理层特征的比较认证通过比较接收信号的物理层特征与参考向量完成对接入终端的身份认证，由于该机制具有较低的通信和计算开销，适用于 6G 网络终端在多种网络切换时的无缝鉴别转换。物理层特征的随机性为终端提供了丰富的识别空间，但其波动性较强的特点使得认证的可靠性和稳健性差，特别是高速移动的通信场景，移动性管理是该认证的研究重点。其次，基于物理层特征的比较认证缺少隐私性保护和数据完整性保护，该机制需要与传统的密码学认证方式结合，实现 6G 网络可靠的终端身份鉴别。因此，基于物理层特征的比较认证在 6G 网络中将主要应用于计算资源受限、终端接入密度较高的通信场景，如高密度感知网络、物联网等。

4.3　物理层认证增强技术

物理层认证的局限性主要体现在：1) 信道的随机性使得物理层特征表现出较强的波动性，物理层认证难以在时变性强的信道环境中执行；2) 物理层特征相对固定的取值范围，使其难以在密集终端场景下部署。为了满足 6G 网络的智能终端身份鉴别性能需求，物理层认证技术需进一步增强其可靠性和稳健性。

机器学习是物理层认证中常见的可靠性增强技术，通过训练样本对终端的物理层特征进行精确建模，克服物理层特征波动性带来的影响。6G 网络峰值速率将提升至 1 Tbit/s，是 5G 网络的 100 倍，6G 网络的基站和终端的数据处理能力也将提升 100 倍，为机器学习算法的部署提供了有力支撑[5]。

基于机器学习的物理层认证增强如表 3 所示，文献[34-36]提出了基于深度学习思想的物理层认证增强技术，通过学习合法终端和攻击终端的样本，建立样本分类模型，实现高可靠的物理层认证。类似的基于模型训练的认证方法包括强化学习[37]、回归学习等[38-39]。然而，信道的时变性导致学习模型难以始终符合实际通信场景。基于此，文献[40]通过核机器学习将物理层属性映射至线性可分离空间，增强物理层认证的可靠性。该物

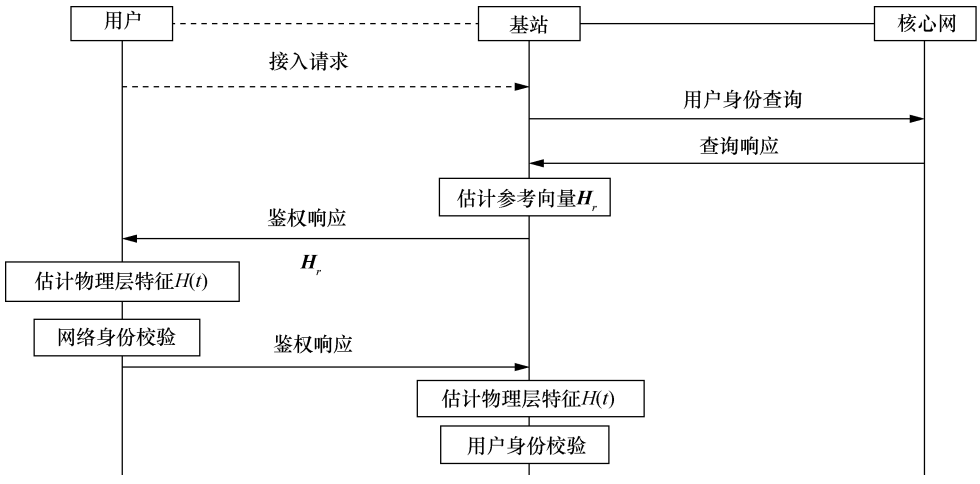

图 2　基于物理层特征的比较认证流程

理层认证增强技术的性能取决于核函数的选择。文献[41-43]提出了基于聚类学习的物理层认证增强技术，通过聚类物理层特征进行分类，提高物理层认证可靠性，由于缺少攻击者数据模型，该方法对具有稀疏异常的终端不够敏感。

随着 6G 网络智能化水平的不断提高，基于机器学习的物理层认证增强技术有望得到大规模部署。由于无线信道固有的开放性，基于模型训练的物理层认证增强方法需要自适应调整模型参数，以适应无线信道的变化。对于无法获得训练样本的通信场景，物理层认证增强方法需要进一步提高对攻击样本的敏感程度，提高物理层认证的精度，降低学习的复杂度。机器学习算法将从有监督的学习策略逐步向半监督甚至无监督的学习策略转换，并综合考虑 6G 网络的计算能力和安全需求，实现精度可调、复杂度可调的认证机制，以适应 6G 网络超异构和终端超异构的特点。

针对物理层认证稳健性较低的特点，多物理层属性和多观测节点可以用于增强终端的辨识度。基于多物理层属性认证的本质是通过增加身份标识的维度来提高终端的可辨识度。在终端密集场景下，通信系统中一旦存在恶意用户，多物理层属性和多观测节点也为不同终端提供了额外的差距，从而增强身份鉴别的可靠性。

基于多属性或多观测点的物理层认证增强如表 4 所示，文献[34,44]提出了利用双互补属性提高物理层认证的辨识度，在此基础上，文献[40,45]提出利用多个物理层属性进一步增强物理层认证的稳健性。在多属性认证中，属性的选择对可靠性和稳健性有着质的影响。由于多属性的提取会带来较大的计算复杂度，文献[38]提出联合感知节点的数据进行统一认证，从而增强终端的可辨识度。该机制需要额外的辅助感知节点。文献[46]提出利用终端所在无线环境中的多个信号的物理层特征作为身份标识，以防止中间人攻击，但环境信号稳定的假设限制了其通用性。

6G 网络密集的接入终端为基于多观测节点的物理层认证增强技术提供了可能性，环境中的无线终端可以作为潜在的观测节点，为终端身份鉴别提供额外的辨识度。参与认证的观测节点的可信管理是物理层认证增强技术的一个重要研究方向。其次，对于多属性物理层认证增强技术，属性的选择直接影响认证性能，为了符合 6G 智能化的特点，需要设计智能属性选择机制，以自适应不同的通信场景。最后，多属性或多观测节点的物理层认证增强技术中存在时间维度和属性维度的样本关联性，合理的关联性分析能够有效增强物理层认证的可靠性和稳健性，并进一步降低复杂度。

4.4 物理层认证技术展望

物理层认证以其高安全性和低复杂性成为无线网络终端身份鉴别的一个重要发展方向。然而，当前物理层认证的研究还存在一些亟待解决的问题。首先，为了实现物理层认证在 6G 网络中的大规模部署，提高物理层认证的可靠性和稳健性势在必行，特别是在高速移动场景下的认证。其次，当前的物理层认证研究主要针对具体通信场景和攻击模型，为了适应 6G 网络广泛的应用场景，一个智能的、参数可调的物理层认证框架是其大规模部

表 3 基于机器学习的物理层认证增强

学习类型	学习方法	特点	参考文献
有参数学习	深度学习	基于攻击样本学习分类模型，实现可靠认证	[34-36]
	强化学习	基于攻击者样本学习判决阈值，最大化认证精度	[37]
	回归学习	学习属性可靠性评估模型，增强认证可靠性	[38-39]
无参数学习	基于核函数学习	通过核函数将非线性可分样本映射至线性可分子空间，增强认证可靠性	[40]
	聚类学习	基于样本结构对合法样本和攻击样本自适应分类，提高认证可靠性	[41-43]

表 4 基于多属性或多观测点的物理层认证增强

样本类型	方式	特点	参考文献
多属性	互补双属性 多独立属性	同一信号的多个物理层属性作为身份标识	[34,44] [40,45]
多观测节点	接收信号自身观测 环境信号观测	不同感知节点对同一信号的联合感知作为身份标识	[38] [46]

署的前提。最后，为了保证 6G 网络的隐私性和数据完整性，物理层认证需要与传统的密钥认证机制结合。总的来说，面向 6G 网络超异构特征，物理层认证以其部署灵活和智能化的特点将成为未来 6G 网络智能终端身份鉴别的一个可行方案。

5　结束语

本文围绕 6G 网络中的智能终端身份鉴别问题展开了分析和研究，并探索了物理层认证对于 6G 智能终端身份鉴别的可行性。相较于之前的移动网络，6G 网络将在系统架构、接入终端类型等方面发生本质变化。智能终端的身份鉴别机制也将随着网络的演进而发生本质变化，鉴别过程将不仅通过某一层的协议来完成，而需要在整个通信过程中执行。随着 6G 接入网络和服务终端的多样化和智能化，单一的终端鉴别机制难以满足整个网络的安全需求。因此，统一且自适应的认证机制将在 6G 网络中得以实现，以满足 6G 网络对超低时延、超可靠通信和用户隐私性的需求。

参考文献：

[1] ZHANG Z, XIAO Y, MA Z, et al. 6G wireless networks: vision, requirements, architecture, and key technologies[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 28-41.

[2] STRINATI E C, BARBAROSSA S, GONZALEZ-JIMENEZ J L, et al. 6G: the next frontier from holographic messaging to artificial intelligence using sub terahertz and visible light communication[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 42-50.

[3] LETAIEF K B, CHEN W, SHI Y, et al. The roadmap to 6G: AI empowered wireless networks[J]. IEEE Communications Magazine, 2019, 57(8): 84-90.

[4] YANG P, XIAO Y, XIAO M, et al. 6G wireless communications: vision and potential techniques[J]. IEEE Network, 2019, 33(4): 70-75.

[5] ZONG B, FAN C, WANG X, et al. 6G technologies: key drivers, core requirements, system architectures, and enabling technologies[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 18-27.

[6] CHEN C M, XIANG B, LIU Y, et al. A secure authentication protocol for Internet of vehicles[J]. IEEE Access, 2019, 7: 12047-12057.

[7] NARMADHA R. Heterogeneous network security management[J]. International Journal of Intelligent Enterprise, 2019, 6(1): 32-52.

[8] DENNING D E. Is quantum computing a cybersecurity threat?[J]. American Scientist, 2019, 107(2): 83-85.

[9] CHENG X, ZHANG Z, CHEN F, et al. Secure identity authentication of community medical Internet of things[J]. IEEE Access, 2019, 7: 115966-115977.

[10] ZHOU L, LI X, YEH K H, et al. Lightweight IoT-based authentication scheme in cloud computing circumstance[J]. Future Generation Computer Systems, 2019, 91: 244-251.

[11] CHEN Y, SHEN Q, SUN P, et al. Reliable migration module in trusted cloud based on security level-design and implementation[C]//2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PHD Forum. IEEE, 2012: 2230-2236.

[12] LI X, HAN Y, GAO J, et al. Secure hierarchical authentication protocol in VANET[J]. IET Information Security, 2019, 14(1): 99-110.

[13] 牛静媛. 移动通信系统安全性分析[D]. 北京: 北京邮电大学, 2008.
NIU J Y. Analysis of the security mechanism in mobile communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2008.

[14] 张磊. GSM/UMTS 混合网络安全若干关键技术研究[D]. 北京: 北京邮电大学, 2011.
ZHANG L. Key technology research on GSM/UMTS hybrid network security[D]. Beijing: Beijing University of Posts and Telecommunications, 2011.

[15] CHANG C C, LEE J S, CHANG Y F. Efficient authentication protocols of GSM[J]. Computer Communications, 2005, 28(8): 921-928.

[16] NTANTOGIAN C, XENAKIS C. One-pass EAP-AKA authentication in 3G-WLAN integrated networks[J]. Wireless personal communications, 2009, 48(4): 569-584.

[17] MUN H, HAN K, KIM K. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA[C]// 2009 Wireless Telecommunications Symposium. IEEE, 2009: 1-8.

[18] 向东南, 毛文俊. LTE 系统 EPS-AKA 过程安全性研究与改进[J]. 无线电通信技术, 2016, 42(5):60-63.
XIANG D N, MAO W J. Research and improvement of LTE EPS-AKA procedure security[J]. Radio Communication Technology, 2016, 42(5): 60-63.

[19] FERRAG M A, MAGLARAS L, ARGYRIOU A, et al. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes[J]. Journal of Network and Computer Applications, 2018, 101: 55-82.

[20] 胡鑫鑫, 刘彩霞, 刘树新, 等. 移动通信网鉴权认证综述[J]. 网络与信息安全学报, 2018, 4(12): 5-19.
HU X X, LIU C X, LIU S X, et al. Overview of mobile communication network authentication[J]. Chinese Journal of Network and Information Security, 2018, 4(12): 5-19.

[21] PRASAD A R, ARUMUGAM S, SHEEBA B, et al. 3GPP 5G security[J]. Journal of ICT Standardization, 2018, 6(1): 137-158.

[22] BASIN D, DREIER J, HIRSCHI L, et al. A formal analysis of 5G authentication[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM: 2018: 1383-1396.

[23] 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.

[24] PAUL L Y, BARAS J S, SADLER B M. Physical-layer authentication[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 38-51.

[25] WANG X, HAO P, HANZO L. Physical-layer authentication for wireless security enhancement: current challenges and future developments[J]. IEEE Communications Magazine, 2016, 54(6): 152-158.

[26] 杨惠杰, 周天祺, 桂梓原. 区块链技术在物联网中的身份认证研究[J]. 中兴通讯技术, 2018, 24(6): 39-44.
YANG H J, ZHOU T Q, GUI Z Y. Blockchain technology for identity

authentication in Internet of things[J]. ZTE Technology Journal, 2018, 24(6): 39-44.

[27] HAMMI M T, HAMMI B, BELLOT P, et al. Bubbles of trust: a decentralized blockchain-based authentication system for IoT[J]. Computers & Security, 2018, 78: 126-142.

[28] LIN C, HE D, HUANG X, et al. BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0[J]. Journal of Network and Computer Applications, 2018, 116: 42-52.

[29] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.

[30] ZHANG J, RAJENDRAN S, SUN Z, et al. Physical layer security for the Internet of things: authentication and key generation[J]. IEEE Wireless Communications, 2019, 26(5): 92-98.

[31] ZENG K, GOVINDAN K, MOHAPATRA P. Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks][J]. IEEE Wireless Communications, 2010, 17(5): 56-62.

[32] GAO N, NI Q, FENG D, et al. Physical layer authentication under intelligent spoofing in wireless sensor networks[J]. Signal Processing, 2020, 166: 107272.

[33] ZHAO C, HUANG M, HUANG L, et al. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks[J]. Computer networks, 2017, 128: 164-171.

[34] WANG N, JIANG T, LYU S, et al. Physical-layer authentication based on extreme learning machine[J]. IEEE Communications Letters, 2017, 21(7): 1557-1560.

[35] LIAO R F, WEN H, WU J, et al. Deep-learning-based physical layer authentication for industrial wireless sensor networks[J]. Sensors, 2019, 19(11): 2440.

[36] BALDINI G, GIULIANI R, DIMC F. Physical layer authentication of Internet of things wireless devices using convolutional neural networks and recurrence plots[J]. Internet Technology Letters, 2019, 2(2): e81.

[37] XIAO L, LI Y, HAN G, et al. PHY-layer spoofing detection with reinforcement learning in wireless networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 10037-10047.

[38] XIAO L, WAN X, HAN Z. PHY-layer authentication with multiple landmarks with reduced overhead[J]. IEEE Transactions on Wireless Communications, 2017, 17(3): 1676-1687.

[39] QIU X, JIANG T, WU S, et al. Physical layer authentication enhancement using a Gaussian mixture model[J]. IEEE Access, 2018, 6: 53583-53592.

[40] FANG H, WANG X, HANZO L. Learning-aided physical layer authentication as an intelligent process[J]. IEEE Transactions on Communications, 2018, 67(3): 2260-2273.

[41] YANG J, CHEN Y, TRAPPE W, et al. Detection and localization of multiple spoofing attackers in wireless networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 24(1): 44-58.

[42] XIA S, LI N, TAO X F, et al. Multiple attributes based spoofing detection using an improved clustering algorithm in mobile edge network[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 242-243.

[43] CHEN Y, WEN H, WU J, et al. Clustering based physical-layer authentication in edge computing systems with asymmetric resources[J]. Sensors, 2019, 19(8): 1926.

[44] LIU J, WANG X. Physical layer authentication enhancement using two-dimensional channel quantization[J]. IEEE Transactions on Wireless Communications, 2016, 15(6): 4171-4182.

[45] FANG H, WANG X, HANZO L. Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes[J]. IEEE Transactions on Communications, 2020.

[46] XIAO L, YAN Q, LOU W, et al. Proximity-based security techniques for mobile users in wireless networks[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 2089-2100.

[作者简介]

夏仕达（1993− ），男，北京邮电大学博士生，主要研究方向为基于物理层安全的终端身份安全接入和异常用户检测。

徐瑨（1981− ），女，博士，北京邮电大学副教授，主要研究方向为宽带移动通信、无线网络安全等。

陶小峰（1970− ），男，博士，北京邮电大学教授、博士生导师，主要研究方向为无线通信、移动通信安全等。