ICS 33.050.99
CCS M731

团　　体　　标　　准

T/GDIOT 003—2025

基于物理层安全的物联网设备轻量级认证技术规范

Technical Specification for Lightweight Authentication of IoT Devices Based on Physical Layer Security

2025-06-10 发布　　2025-06-10 实施

广东省物联网协会　发布

目　次

前 言 2
1. 范围 3
2. 规范性引用文件 3
3. 术语和定义 3
4. 缩略语 4
5. 基本模型 5
5.1 概述 5
5.2 终端内生认证模型 5
5.3 网关代理认证模型 5
6. 基本功能 6
6.1 概述 6
6.2 物理层特征提取功能 6
6.3 认证协议功能 6
6.4 三层路由功能 6
6.5 设备管理功能 7
6.6 安全审计功能 7
6.7 与物联网应用平台通信功能 7
7. 接口要求 7
7.1 物理层特征提取接口 7
7.2 认证协议接口 7
8. 协议要求 8
9. 管理维护要求 8
9.1 本地参数配置要求 8
9.2 远程参数配置要求 8
9.3 软件升级要求 8
9.4 参数备份要求 9
9.5 恢复默认配置要求 9
9.6 系统重启要求 9
9.7 系统日志要求 9
9.8 认证服务器连接参数配置要求 9
10. 安全性要求 9
10.1 终端设备接入安全性 9
10.2 与认证服务器通信的安全性 9
10.3 认证数据安全性 10
11. 可靠性要求 10
11.1 认证机制鲁棒性 10
11.2 系统可用性保障 10

前　言

本文件依据 GB/T 1.1-2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东省物联网协会归口。

本文件由深圳大学提出。

本文件起草单位：深圳大学、鹏城实验室、南京信息工程大学、广州技象科技有限公司。

本文件主要起草人：谢宁、谭海军、苏健、张沛昌、钟世达、温文坤、刘军林、宋书山。

基于物理层安全的物联网设备轻量级认证技术规范

1. 范围

本文件规定了基于物理层安全的物联网设备轻量级认证技术的基本模型、核心功能、认证机制、算法要求、安全性要求、性能要求及互操作性要求。

本文件适用于资源受限的物联网终端设备，包括但不限于工业传感器网络、智能家居设备、智慧城市基础设施等需要实施轻量级认证的场景。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注明日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修订单）适用于本文件。

GB/T 25069	信息安全技术 术语
GB/T 33745	物联网 术语
GB/T 33474	物联网 参考体系结构
GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求
GB/T 37093-2018	信息安全技术 物联网感知层接入通信网的安全要求
GB/T 38636	信息安全技术 传输层密码协议（TLCP）
GB/T 35319	物联网系统接口要求
GB/T 36962-2018	传感数据分类与代码
GB/T 34068	物联网总体技术 智能传感器接口规范
T/TAF 062-2020	物联网设备安全平台技术要求和分级方法
ISO/IEC 27402	网络安全-物联网安全和隐私-设备基线要求
RFC 6347	数据报传输层安全协议 1.2版
RFC 8446	传输层安全协议 1.3版
RFC 7252	受限应用协议（CoAP）
ISO/IEC 20922	信息技术 消息队列遥测传输（MQTT）

3. 术语和定义

3.1 概述

以下术语和定义适用于本文件。

3.2

物联网网关 internet of things gateway

连接物联网感知层与网络层的桥接设备，具有数据转发、协议转换、设备管理等功能，能够处理物理层安全特征信息并支持轻量级认证机制的计算设备。

3.3

物联网应用平台 application platform for internet of things

通过标准接口与物联网终端设备和网关进行交互，对采集的物理层特征数据进行处理、分析和存

储，实现物联网设备认证、安全管理与控制的软件系统。

3.4

物理层安全 physical layer security

利用无线通信信道固有的物理特性（如信道状态信息、射频指纹等）建立安全机制，实现通信双方的身份认证和保密通信的技术。

3.5

轻量级认证 lightweight authentication

适用于计算资源和能源受限设备的低复杂度、低能耗的身份认证机制，通常基于物理层特征或简化密码学算法实现。

3.6

设备指纹 device fingerprint

利用物联网设备硬件、软件或通信特性产生的可唯一识别该设备的特征集合，可包括射频特征、时钟偏移、硬件不完美性等物理层参数。

4. 缩略语

下列缩略语适用于本文件。

AES 高级加密标准 (Advanced Encryption Standard)

AWGN 加性白高斯噪声 (Additive White Gaussian Noise)

CFR 信道频率响应 (Channel Frequency Response)

CIR 信道脉冲响应 (Channel Impulse Response)

CoAP 受限应用协议 (Constrained Application Protocol)

CSI 信道状态信息 (Channel State Information)

CSKG 信道秘密密钥生成 (Channel Secret Key Generation)

DTLS 数据报传输层安全 (Datagram Transport Layer Security)

ECC 椭圆曲线密码 (Elliptic Curve Cryptography)

HMAC 哈希消息认证码 (Hash-based Message Authentication Code)

IoT 物联网 (Internet of Things)

LDPC 低密度奇偶校验 (Low-Density Parity-Check)

MITM 中间人攻击 (Man-In-The-Middle)

MQTT 消息队列遥测传输 (Message Queuing Telemetry Transport)

PLA 物理层认证 (Physical Layer Authentication)

PLS 物理层安全 (Physical Layer Security)

PUF 物理不可克隆函数 (Physical Unclonable Function)

RSS 接收信号强度 (Received Signal Strength)

SKG 密钥生成 (Secret Key Generation)

SNR 信噪比 (Signal-to-Noise Ratio)

TLS 传输层安全 (Transport Layer Security)

WSN 无线传感器网络 (Wireless Sensor Network)

5. 基本模型

5.1 概述

基于物理层安全的物联网设备轻量级认证系统包含终端设备、边缘网关和认证服务器三个核心组件，构成分层认证架构。该架构利用信道特征和射频指纹等物理层特性建立设备唯一性标识，实现低计算复杂度的身份验证机制。典型系统结构见图1。

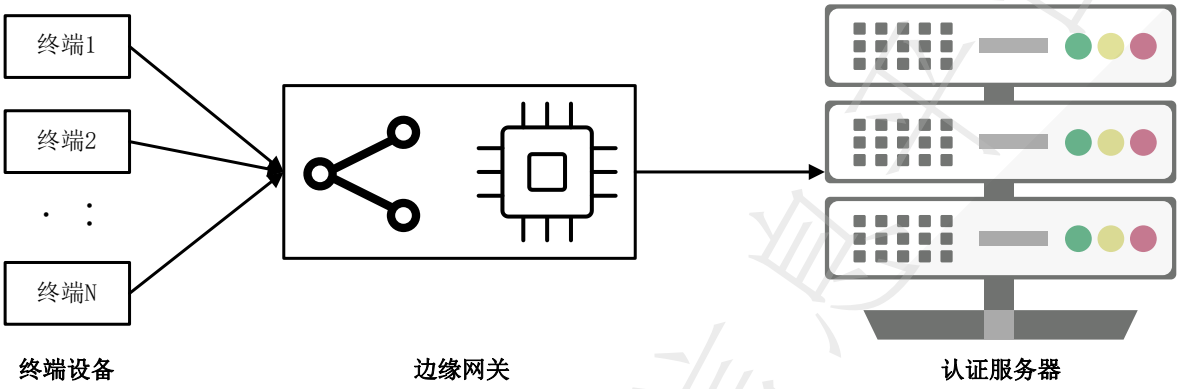

图1 基于物理层安全的物联网设备认证系统结构

根据认证功能部署位置和实现方式，划分为终端内生认证模型和网关代理认证模型两种基本模型。

5.2 终端内生认证模型

物理层特征提取与认证算法直接集成于物联网终端设备中，设备能够自主完成物理层特征采集、量化和认证协议交互。该模型适用于具备一定计算能力的终端设备，实现端到端的安全认证。基本功能结构见图2。

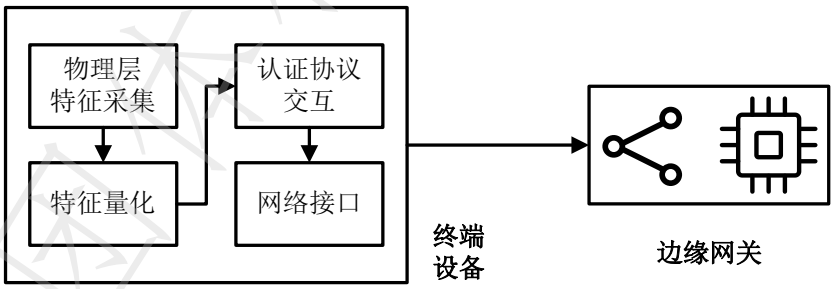

图2 终端内生认证模型功能结构

5.3 网关代理认证模型

由具备物理层特征提取能力的网关设备代理资源受限物联网终端完成认证过程。网关负责信道特征测量、射频指纹提取和认证协议执行，降低终端设备的计算负担。该模型适用于超低功耗或计算资源极度受限的物联网终端。基本功能结构见图3。

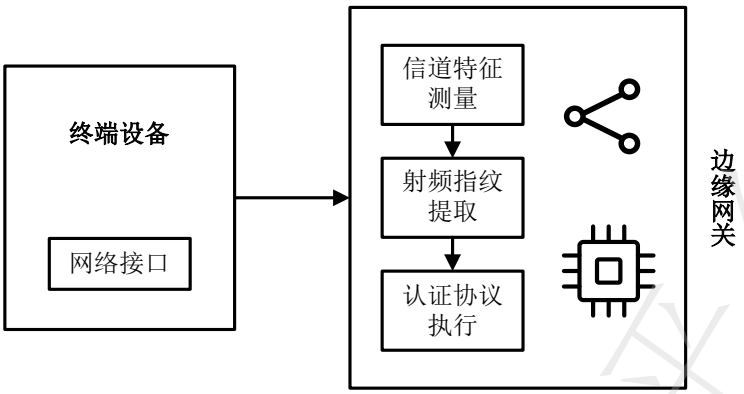

图3 网关代理认证模型功能结构

6. 基本功能

6.1 概述

认证系统应具备物理层特征提取功能、轻量级认证协议处理功能和安全密钥管理功能。应支持基于信道特征或射频指纹的设备唯一性识别，宜支持多特征融合认证。系统应具有远程和本地配置管理能力，应具有安全参数存储和更新能力。应具备与现有物联网安全框架的兼容性，能够与上层认证机制协同工作。

6.2 物理层特征提取功能

设备应支持以下至少一种物理层特征的提取与量化：

a）信道状态信息（CSI）和信道脉冲响应（CIR）提取；

b）射频指纹特征提取，包括频率偏移、I/Q不平衡、相位噪声等硬件特性；

c）信号强度（RSS）和时间特征的测量与处理。

特征提取精度应满足认证需求，信噪比应不低于15dB，特征量化误差应控制在5%以内。

6.3 认证协议功能

应支持基于挑战-响应机制的双向认证流程，并满足以下要求：

a）支持单次认证和会话持续认证模式；

b）认证时延应小于500ms（终端内生模型）或200ms（网关代理模型）；

c）支持认证结果的安全传输和验证；

d）具备防重放攻击和防中间人攻击能力。

6.4 三层路由功能

a）应支持基于物理层特征的密钥生成（SKG）功能；

b）应具备密钥动态更新机制，更新周期应与信道相干时间适配；

c）密钥熵值应不低于128比特，密钥不一致率应控制在10^-6以下；

d）宜支持密钥分发和密钥协商功能。

6.5 设备管理功能

6.5.1本地管理能力

a）应支持安全配置接口，如TLS加密的Web界面或安全命令行；

b）应具有多因素认证能力，包含物理层特征验证与传统密码认证；

c）应实行基于角色的访问控制；

d）应具备配置参数的安全存储与恢复功能。

6.5.2远程管理能力

a）应支持基于DTLS或TLS的安全远程管理；

b）应支持认证参数的远程配置与更新；

c）应具备安全远程固件升级能力，并支持固件完整性验证。

6.6 安全审计功能

a）应记录认证事件日志，包括认证成功、失败及异常事件；

b）应支持物理层特征异常监测，检测可能的欺骗攻击；

c）应具备设备行为异常分析能力，支持入侵检测。

6.7 与物联网应用平台通信功能

应支持与上层物联网平台的安全交互，包括：

a）向物联网平台提供设备认证状态和可信度评估；

b）接收物联网平台的安全策略更新；

c）支持标准安全协议（如MQTT-TLS、CoAP-DTLS）进行数据交换；

d）支持物理层认证结果与应用层认证机制的协同验证。

7. 接口要求

7.1 物理层特征提取接口

设备应具备以下物理层特征提取接口能力：

a）信道状态信息（CSI）提取接口：采样精度应不低于12比特，采样频率应与信道相干时间匹配；

b）射频特征提取接口：应支持频率偏移、相位噪声、I/Q不平衡等参数采集，特征量化分辨率应不低于16比特；

c）信号强度（RSS）监测接口：测量精度应优于±2dB，动态范围应不小于60dB。

物理层特征提取接口应支持标准化数据格式输出，便于特征处理单元进行后续处理。

7.2 认证协议接口

设备应具备以下物理层特征提取接口能力：

a）设备认证接口应支持标准化的挑战响应交互机制，接口延迟应小于30ms；

b）认证结果接口应提供标准化的认证状态指示和安全度量参数；

c）密钥管理接口应支持密钥生成、更新和分发功能，接口应提供密钥熵值和一致性指标；

d）应提供与上层安全机制的互操作接口，支持认证结果的安全传递。

8. 协议要求

8.1 物理层认证协议

物理层认证协议应具备以下特性：

a）应支持基于挑战-响应机制的双向认证流程；

b）应支持物理层特征的安全量化和传输；

c）应具备防重放攻击机制，包括时间戳或随机挑战序列；

d）应支持认证过程中的完整性保护。

8.2 轻量级密钥协商协议

a）应基于物理层信道特征实现轻量级密钥协商，协议开销应适应资源受限设备；

b）应支持密钥量化、协调和隐私放大三阶段处理；

c）应提供密钥生成速率不低于100bps（静态环境）或200bps（动态环境）的能力；

d）应支持密钥动态更新机制，更新周期应与信道变化特性适配。

8.3 与物联网平台交互协议

与物联网应用平台的交互协议应满足以下要求：

a）应支持DTLS/TLS保护的CoAP或MQTT等轻量级协议；

b）应支持认证结果与设备状态信息的安全传输；

c）应支持物理层认证与上层安全机制的协同验证；

d）通信协议应具备资源适应性，能根据设备计算能力动态调整安全强度。

9. 管理维护要求

9.1 本地参数配置要求

对于5.2所述终端内生认证模型，应能通过统一的配置界面，对物理层特征参数和认证协议参数进行配置。

对于5.3所述网关代理认证模型，应能分别配置物理层特征提取参数和认证协议参数。

9.2 远程参数配置要求

应支持通过安全通道对认证系统进行远程配置。应采用TLS或DTLS协议保护远程配置通道。当本地参数配置与远程参数配置不一致时，应优先使用远程参数配置。

9.3 软件升级要求

应具备认证系统组件的安全远程升级能力。应支持基于HTTPS或DTLS保护的CoAP等标准协议进行软件升级。

软件升级应进行版本兼容性检查，对不适用于当前设备的软件禁止进行升级操作，并返回明确的错误提示信息。

升级过程中，应通过密码学方法对升级文件进行完整性验证。当完整性验证失败时，应终止升级操作并恢复至升级前状态。

在任何软件升级失败情况下，认证系统应保持基本功能，防止设备被锁定。

9.4 参数备份要求

认证系统应具备安全参数的本地或远程备份功能。应对参数备份操作实施权限控制。宜限定仅管理员可执行参数备份操作。

应以加密格式存储导出的参数文件。

应支持参数文件的安全导入功能，并进行适当的完整性验证。

9.5 恢复默认配置要求

应提供本地和远程恢复认证系统默认参数配置的操作方法。

9.6 系统重启要求

应提供本地和远程重启认证系统组件的操作方法。

9.7 系统日志要求

应具备日志功能，记录影响认证系统的本地和远程操作的时间、类型、操作员等信息。日志应能本地保存，宜具有定期备份功能。

9.8 认证服务器连接参数配置要求

认证系统宜在出厂时，根据应用场景预置认证服务器连接参数。

应支持通过本地配置修改认证服务器连接参数，包括服务器URL和认证凭证。

对于终端内生认证模型，宜支持认证服务器参数的安全远程配置。

系统应支持MQTT-TLS或CoAP-DTLS等标准物联网安全协议与认证服务器进行安全通信。认证系统宜遵循标准化流程与认证服务器建立安全连接。

对于使用TLS/DTLS进行安全通信的系统，应实施标准的安全证书管理程序。

10. 安全性要求

10.1 终端设备接入安全性

a）物理层认证机制：应基于物理层特征（如信道状态信息、射频指纹等）建立终端设备唯一性标识，并符合GB/T 37024-2018第6.2.1节关于接入认证的要求；

b）网络访问控制：应根据物理层认证结果实施访问权限控制，限制未通过认证设备的访问范围，符合GB/T 37024-2018第6.2.2节要求；

c）传输数据保护：在无线通信环境中（如ZigBee、Wi-Fi、蓝牙等），应采用基于物理层特征的密钥生成机制或标准密码算法对传输数据进行加密，密钥熵值不低于128比特。

10.2 与认证服务器通信的安全性

a）双向认证要求：认证系统与物联网认证服务器之间应实现基于物理层特征与传统密码学相结合的双向认证机制；

b）安全协议要求：使用CoAP协议时，应使用RFC 6347规定的DTLS协议进行安全保护，确保认证信息传输的机密性和完整性；

c）安全传输保障：使用MQTT协议时，应采用RFC 8446规定的TLS 1.3或更高版本进行通信加密，支持前向安全特性；

d）Web接口保护：使用HTTP协议时，应强制采用HTTPS，并禁用不安全的密码套件，确保认证交互过程的安全性。

10.3 认证数据安全性

a）数据保护机制：物理层特征数据和认证结果应采用安全存储技术保护，实现数据加密存储与完整性验证，防止特征数据被恶意篡改或窃取；

b）访问控制：对认证参数和特征数据的访问应实施基于角色的权限控制，确保只有授权组件能够访问敏感数据；

c）物理安全防护：包含物理层特征处理功能的硬件模块应具备防物理攻击能力，包括但不限于侧信道攻击防护和篡改检测机制。

11. 可靠性要求

11.1 认证机制鲁棒性

a）特征容错处理：认证系统应具备信道特征抖动容错能力，在环境干扰下仍能保持认证准确率不低于95%；

b）冗余认证机制：应支持多特征融合认证，当某一物理层特征因干扰不可用时，可自动切换至其他特征或备用认证方式，确保认证服务的持续可用。

11.2 系统可用性保障

a）认证状态一致性：应保持物理层认证状态与上层安全机制状态的一致性，防止因层间信息不同步导致的安全隐患；

b）性能降级保护：当认证系统资源受限或遭受攻击时，应支持降级认证模式，确保关键设备的基本认证功能可用；

c）恢复机制：认证系统应具备自动恢复能力，在物理层特征暂时不可用的情况下，可采用临时替代机制并记录异常状况，待条件恢复后重新启用完整认证流程。