



中华人民共和国国家标准

GB/T 30269.808—2018

信息技术 传感器网络 第 808 部分： 测试：低速率无线传感器网络 网络层和应用支持子层安全

Information technology—Sensor network—Part 808: Testing: Network layer and application support sublayer security for low-rate wireless sensor network

2018-12-28 发布

2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 传感器网络 第 808 部分：
测试：低速率无线传感器网络
网络层和应用支持子层安全
GB/T 30269.808—2018

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)

网址：www.spc.org.cn

服务热线：400-168-0010

2018 年 12 月第一版

*

书号：155066·1-61819

版权专有 侵权必究

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总体描述	3
6 NWK 安全测试	5
6.1 环境配置	5
6.2 测试过程	5
6.3 测试判决	6
6.4 说明	7
7 APS 安全测试	7
7.1 TC_APS_SE01 信任中心配置分发初始化密钥材料到终端设备	7
7.2 TC_APS_SE02 信任中心配置分发初始化值到终端设备	8
7.3 TC_APS_SE03 手持设备分发初始化密钥材料到终端设备	10
7.4 TC_APS_SE04 手持设备分发初始化值到终端设备	11
7.5 TC_APS_SE05 基于随机密钥池的方法建立直接密钥	13
7.6 TC_APS_SE06 基于多项式池的方法建立直接密钥	15
7.7 TC_APS_SE07 基于同一簇内路径密钥建立的方法建立路径密钥	17
7.8 TC_APS_SE08 基于不同簇内路径密钥建立的方法建立路径密钥	20
7.9 TC_APS_SE09 更新初始化密钥材料	23
7.10 TC_APS_SE10 更新初始化值	24
7.11 TC_APS_SE11 更新共享密钥	26
7.12 TC_APS_SE12 更新会话密钥	28
7.13 TC_APS_SE13 撤销密钥	29
7.14 TC_APS_SE14 在网关处对数据资源采用自主访问方法启动访问控制过程	31
7.15 TC_APS_SE15 在网关处对节点资源采用自主访问方法启动访问控制过程	33
7.16 TC_APS_SE16 在网关处对数据资源采用强制访问方法启动访问控制过程	35
7.17 TC_APS_SE17 在网关处对节点资源采用强制访问方法启动访问控制过程	37
7.18 TC_APS_SE18 在节点处对节点资源采用强制访问方法启动访问控制过程	38
7.19 TC_APS_SE19 基于异或算法的身份鉴别	40
7.20 TC_APS_SE20 基于哈希运算的身份鉴别	43

7.21	TC_APS_SE21 基于分组密码算法的身份鉴别	45
7.22	TC_APS_SE22 基于非对称密码算法的身份鉴别	48
7.23	TC_APS_SE23 启动广播消息鉴别	50
7.24	TC_APS_SE24 启动安全数据融合服务	52
7.25	TC_APS_SE25 安全数据融合撤销	55
附录 A (规范性附录)	协议实现一致性声明	58

前 言

GB/T 30269《信息技术 传感器网络》拟分为以下部分：

- 第 1 部分：参考体系结构和通用技术要求；
- 第 2 部分：术语；
- 第 301 部分：通信与信息交换：低速无线传感器网络网络层和应用支持子层规范；
- 第 302 部分：通信与信息交换：高可靠性无线传感器网络媒体访问控制和物理层规范；
- 第 303 部分：通信与信息交换：基于 IP 的无线传感器网络网络层规范；
- 第 304 部分：通信与信息交换：声波通信系统技术要求；
- 第 401 部分：协同信息处理：支撑协同信息处理的服务及接口；
- 第 501 部分：标识：传感节点标识符编制规则；
- 第 502 部分：标识：传感节点标识符解析；
- 第 503 部分：标识：传感节点标识符注册规程；
- 第 504 部分：标识：传感节点标识符管理规范；
- 第 601 部分：信息安全：通用技术规范；
- 第 602 部分：信息安全：低速率无线传感器网络网络层和应用支持子层安全规范；
- 第 701 部分：传感器接口：信号接口；
- 第 702 部分：传感器接口：数据接口；
- 第 801 部分：测试：通用要求；
- 第 802 部分：测试：低速无线传感器网络媒体访问控制和物理层；
- 第 803 部分：测试：低速无线传感器网络网络层和应用支持子层；
- 第 804 部分：测试：传感器接口；
- 第 805 部分：测试：传感器网关；
- 第 806 部分：测试：传感节点标识符解析；
- 第 807 部分：测试：网络传输安全；
- 第 808 部分：测试：低速率无线传感器网络网络层和应用支持子层安全；
- 第 809 部分：测试：基于 IP 的无线传感器网络网络层协议；
- 第 901 部分：网关：通用技术要求；
- 第 902 部分：网关：远程管理技术要求；
- 第 903 部分：网关：逻辑接口；
- 第 1001 部分：中间件：传感器网络节点接口。

本部分为 GB/T 30269 的第 808 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分主要起草单位：中国信息安全认证中心、山东省标准化研究院、中国电子技术标准化研究院、无锡物联网产业研究院、山东省计算中心(国家超级计算济南中心)、重庆邮电大学、中国传媒大学。

本部分主要起草人：甘杰夫、公伟、王曙光、王庆升、陈书义、苏静茹、寇春晓、邢涛、李昭、郑潇潇、汪付强、吴晓明、谢昊飞、李红胜、刘剑波、田佳音、杨成。

引 言

GB/T 30269 的本部分针对 GB/T 30269.602—2017《信息技术 传感器网络 第 602 部分:信息安全:低速率无线传感器网络网络层和应用支持子层安全规范》描述了低速率无线传感器网络网络层和应用支持子层安全的测试例。鉴于某一测试例可能涉及若干协议要求,某一协议要求可能对应若干测试例,因此本部分描述的测试例未与 GB/T 30269.602—2017 的条款一一对照。

信息技术 传感器网络 第 808 部分： 测试：低速率无线传感器网络 网络层和应用支持子层安全

1 范围

GB/T 30269 的本部分针对 GB/T 30269.602—2017 规定了低速率无线传感器网络网络层和应用支持子层安全的测试例。

本部分适用于声称符合 GB/T 30269.602—2017 的产品一致性测试和针对特定产品的特定测试例设计。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

- GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第 1 部分：基本概念
 GB/T 30269.301—2014 信息技术 传感器网络 第 301 部分：通信与信息交换：低速无线传感器网络网络层和应用支持子层规范
 GB/T 30269.601—2016 信息技术 传感器网络 第 601 部分：信息安全：通用技术规范
 GB/T 30269.602—2017 信息技术 传感器网络 第 602 部分：信息安全：低速率无线传感器网络网络层和应用支持子层传输安全规范
 GB/T 30269.801—2017 信息技术 传感器网络 第 801 部分：测试：通用要求

3 术语和定义

GB/T 17178.1—1997、GB/T 30269.301—2014、GB/T 30269.601—2016 界定的以及下列术语和定义适用于本文件。

3.1

被测设备 device under test; DUT

被测实现所位于的设备。

[GB/T 30269.803—2017, 定义 3.4]

3.2

密钥材料 keying material

确立和维持密码密钥关系所必需的数据。

3.3

共享密钥 shared key

两个或多个节点之间在初始密钥材料的基础上建立的长期共同使用的密钥。

3.4

会话密钥 session key

为保证一对节点之间的保密通信或消息鉴别而随机产生的密钥。