ICS 35.110
L 79

中华人民共和国国家标准

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

Information technology—Sensor network—Part 602：Information security：Network layer and application support sublayer security specification for low-rate wireless sensor networks

2017-12-29 发布　　2017-12-29 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

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规范；

——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：传感器接口测试规范；

——第805部分：测试：传感器网关测试规范；

——第806部分：测试：传感节点标识符解析一致性测试技术规范；

——第807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测评规范；

——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：逻辑功能接口技术规范；

——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602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。

本部分起草单位：重庆邮电大学、中国电子技术标准化研究院、无锡物联网产业研究院、成都秦川科技发展有限公司、中国信息安全认证中心、山东省计算中心(国家超级计算济南中心)。

本部分主要起草人：王浩、魏旻、陈书义、苏静茹、吴岳飞、甘杰夫、王平、卓兰、汪付强。

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

1　范围

GB/T 30269的本部分规定了低速率无线传感器网络网络层和应用支持子层的原语、命令帧格式以及安全交互规程。

本部分适用于低速率传感器网络传输安全的开发设计。

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 15629.15—2010　信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第15部分:低速无线个域网(WPAN)媒体访问控制和物理层规范

GB/T 25069—2010　信息安全技术　术语

GB/T 30269.2—2013　信息技术　传感器网络　第2部分:术语

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

3　术语和定义

GB/T 25069—2010、GB/T 30269.2—2013界定的以及下列术语和定义适用于本文件。

3.1

直接密钥　direct key

邻居节点之间建立的共享的对密钥。

3.2

密钥建立　key establishment

为一个或多个实体产生一个可用的、共享的秘密密钥的过程。

3.3

密钥管理　key management

根据安全策略,实施对密钥材料进行产生、登记、认证、注销、分发、安装、存储、归档、撤销、衍生、销毁和恢复的服务。

3.4

密钥材料　keying material

确立和维持密码密钥关系所必需的数据(如密钥,初始化值)。