



中华人民共和国国家标准

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

Information technology—Sensor network—
Part 601: Information security: General technical specifications

2016-04-25 发布

2016-08-01 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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	4
5 概述	4
5.1 传感器网络资产	4
5.2 安全模型	4
5.3 安全环境假设	5
5.4 安全威胁	5
5.5 安全策略	6
5.6 传感器网络安全目标	8
6 安全机制	8
6.1 密钥管理机制	8
6.2 访问控制	9
6.3 鉴别机制	9
6.4 路由安全	9
6.5 安全数据融合	9
6.6 加密机制	9
6.7 安全审计机制	9
6.8 帧安全机制	10
6.9 协调器变换的安全机制	10
7 安全等级划分	10
7.1 安全等级划分概述	10
7.2 安全等级划分方法	10
7.3 安全等级划分要求	11
附录 A (资料性附录) 密钥管理	18
附录 B (资料性附录) 访问控制机制	22
附录 C (资料性附录) 路由安全	28
附录 D (资料性附录) 安全数据融合机制	33
附录 E (资料性附录) 帧安全机制	35
附录 F (资料性附录) 协调器变换安全机制	39
参考文献	42

前 言

GB/T 30269《信息技术 传感器网络》拟分为以下几部分：

- 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：面向高可靠性应用的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 的网络层规范；
- 第 304 部分：通信与信息交换：面向视频的媒体访问控制层和物理层规范；
- 第 305 部分：通信与信息交换：超声波通信协议规范；
- 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：传感节点解析和管理规范；
- 第 503 部分：标识：传感节点标识符注册规程；
- 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 603 部分：信息安全：密钥管理技术规范；
- 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：网络传输安全测评规范；
- 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测评规范；
- 第 809 部分：测试：传感网系统安全测评规范；
- 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：传感器网络结点数据交互规范。

本部分是 GB/T 30269 的第 601 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。

本部分凡涉及密码相关内容，按国家有关法规实施。

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：中国电子技术标准化研究院、重庆邮电大学、深圳市海思半导体有限公司、山东省计算中心、中国科学院软件研究所、西安西电捷通无线网络通信有限公司。

本部分起草人：陈星、王浩、赵华伟、张立武、张向东、徐静、董挺、汪付强、杜志强。

信息技术 传感器网络

第 601 部分:信息安全:通用技术规范

1 范围

GB/T 30269 的本部分针对传感器网络传输的安全威胁和安全目标,提出了传感器网络的安全模型,描述了传感器网络安全策略、机制、等级。

本部分适用于传感器网络的安全设计、开发、运营和维护,可为传感器网络安全评估提供参考。

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 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第 1 部分:简介和一般模型

GB/T 30269.2—2013 信息技术 传感器网络 第 2 部分:术语

3 术语和定义

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

传感器网络 sensor network

利用传感器网络结点及其他网络基础设施,对物理世界进行信息采集并对采集的信息进行传输和处理,并为用户提供服务的网络化信息系统。

3.2

结点鉴别 node authentication

证实结点是其所声称的结点。

3.3

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

[GB/T 20984—2007,定义 3.18]

3.4

可信第三方 trusted third party

在同安全相关的活动方面,被其他实体信任的安全机构或其代理。

[GB/T 25069—2010,定义 2.2.4.6]

3.5

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)。

[GB/T 25069—2010,定义 2.2.2.108]