ICS 33.050.99
CCS M731

团　　体　　标　　准

T/GDIOT 004—2025

物联网多源数据融合与安全定位技术标准

Technical Standard for Multi-Source Data Fusion and Secure Positioning in Internet of Things

2025-06-10 发布　　2025-06-10 实施

广东省物联网协会　发布

目　次

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、南京信息工程大学、鹏城实验室、广州技象科技有限公司。

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

物联网多源数据融合与安全定位技术标准

1. 范围

本文件规定了物联网多源数据融合与安全定位系统的基本架构、融合算法、定位机制、接口规范、安全要求及性能指标。

本文件适用于需要高精度定位及多源数据融合能力的物联网应用场景，包括但不限于智慧城市、智能交通、室内外混合定位、工业物联网及公共安全等领域。

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 33474　物联网参考体系结构

GB/T 33745　物联网术语

GB/T 37025-2018　信息安全技术 物联网数据传输安全技术要求

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 38624.1　物联网 网关 第1部分：面向感知设备接入的网关技术要求

GB/T 40778.1　物联网 面向Web开放服务的系统实现 第1部分：参考架构

GB/T 40778.2　物联网 面向Web开放服务的系统实现 第2部分：物体描述方法

GB/T 37024-2018　信息安全技术 物联网感知层网关安全技术要求

GB/T 41479-2022　信息安全技术 网络数据处理安全要求

GB/T 36478.4　信息交换和共享 第4部分：数据接口

RFC 7252　受限应用协议(CoAP)

RFC 8446　传输层安全协议1.3版本

ISO/IEC 20924　信息技术-物联网(IoT)-定义和词汇

ISO/IEC 30141　物联网(IoT)-参考架构

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 internet of things

通过各类信息传感设备，实时采集任何需要监控、连接和交互的物理对象的信息，通过各类网络接入，实现物与物、物与人的泛在连接，实现对物理世界的智能感知、识别和管理。

3.3

多源数据融合 multi-source data fusion

将不同来源、不同时空特性、不同表达形式的多种异构数据进行汇聚、关联、分析和集成，以提高信息利用价值和决策准确性的处理过程。

3.4

安全定位 secure positioning

采用多重验证机制和抗干扰技术的定位方法，能够有效抵御欺骗、重放等攻击，并保证位置数据的完整性和真实性。

3.5

物联网感知层 perception layer of IoT

由各类传感节点、射频标签、二维码、智能终端等构成，实现对物理世界的感知和信息采集功能的层级。

3.6

物联网网关 internet of things gateway

具有计算和数据处理能力，连接感知层设备与网络层的功能实体，可实现协议转换、数据预处理、边缘计算和安全隔离等功能。

3.7

物联网平台 IoT platform

提供设备连接、数据存储、业务规则处理、应用开发等核心功能的软件系统，支持物联网应用的快速构建和运行。

3.8

数据层融合 data-level fusion

对来自不同传感器的原始数据直接进行融合处理，获取更准确完整的感知信息的过程。

3.9

特征层融合 feature-level fusion

对从多源数据中提取的特征信息进行集成处理，形成更高层次特征表达的过程。

3.10

决策层融合 decision-level fusion

对各子系统独立处理后形成的初步判断结果进行综合，得出最终决策的过程。

3.11

异构数据处理 heterogeneous data processing

对结构化、半结构化和非结构化等不同类型数据进行统一标准化处理的方法。

3.12

定位指纹 positioning fingerprint

利用环境特征（如WiFi信号强度、地磁场分布等）形成的空间位置特征映射。

3.13

多源定位 multi-source positioning

同时利用GNSS、蜂窝网络、WiFi、蓝牙等多种定位技术获取位置信息的方法。

3.14

位置验证 location verification

通过物理层信号特征、时间延迟测量等方法对申报位置进行真实性验证的技术。

3.15

定位隐私保护 location privacy protection

在保证定位服务质量的前提下，防止位置信息泄露的技术措施和管理规范。

4. 缩略语

下列缩略语适用于本文件。

AI　　人工智能(Artificial Intelligence)

AP 无线访问接入点(Wireless Access Point)
BLE 低功耗蓝牙(Bluetooth Low Energy)
CoAP 受限应用协议(Constrained Application Protocol)
CSI 信道状态信息(Channel State Information)
DL 深度学习(Deep Learning)
DDoS 分布式拒绝服务(Distributed Denial of Service)
GNSS 全球导航卫星系统(Global Navigation Satellite System)
GPS 全球定位系统(Global Positioning System)
HTTP 超文本传输协议(Hyper Text Transfer Protocol)
HTTPS 超文本安全传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)
IoT 物联网(Internet of Things)
IPv4 互联网协议第4版(Internet Protocol Version 4)
IPv6 互联网协议第6版(Internet Protocol Version 6)
LBS 基于位置的服务(Location Based Service)
LPWAN 低功耗广域网(Low Power Wide Area Network)
ML 机器学习(Machine Learning)
MQTT 消息队列遥测传输协议(Message Queuing Telemetry Transport)
NB-IoT 窄带物联网(Narrowband Internet of Things)
NFC 近场通信(Near Field Communication)
PaaS 平台即服务(Platform as a Service)
PDR 行人航位推算(Pedestrian Dead Reckoning)
QoS 服务质量(Quality of Service)
RFID 射频识别(Radio Frequency Identification)
RSSI 接收信号强度指示(Received Signal Strength Indicator)
RTK 实时动态定位(Real-Time Kinematic)
SaaS 软件即服务(Software as a Service)
SSH 安全外壳(Secure Shell)
TDoA 到达时间差(Time Difference of Arrival)
TLS 传输层安全协议(Transport Layer Security)
UWB 超宽带(Ultra-Wideband)
VPN 虚拟专用网络(Virtual Private Network)
WSN 无线传感器网络(Wireless Sensor Network)

5. 基本模型

5.1 概述

物联网多源数据融合与安全定位系统具备多种数据获取能力、融合处理能力和安全定位功能，满足GB/T 35319所描述的系统接口要求和GB/T 40778.1所描述的参考架构。系统基于层次化数据处理框架，实现感知数据的采集、预处理、融合分析与安全定位。系统首先在终端层采集多源数

据，可包括单比特探测数据、UWB 数据、IMU 数据、里程计数据、被动式信道指纹和主动式安全等，并通过时空校正、可信度评估与多模态融合算法实现数据融合处理，随后依据 GB/T 35319 系统接口规范和 GB/T 40778.1 参考架构对融合结果进行安全定位，最终输出高可信度的安全定位与认证结果。典型系统结构见图1。

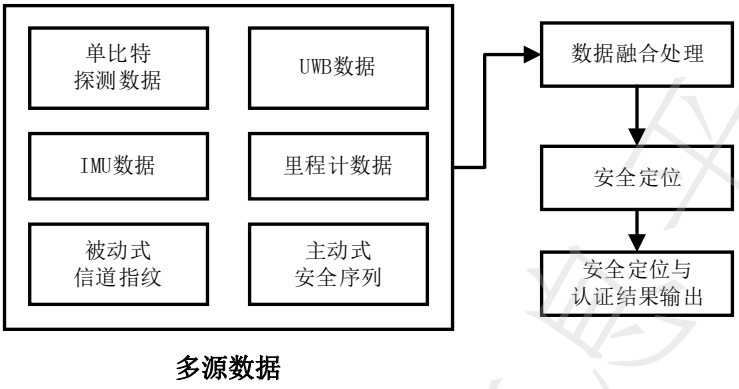

图1 物联网多源数融合与安全定位系统典型结构

根据系统集成度和部署方式的不同，划分为集中式融合模型和分布式融合模型两种基本架构。

5.2 集中式融合模型

终端设备端针对多源感知数据分别执行原始数据采集与初步滤波，然后经网络接口将预处理后的多源信息集中上报至边缘网关 / 云端；在边缘网关上，首先对各路预滤波数据进行时空校准与多模态数据融合处理，然后在融合结果基础上完成抗攻击的安全定位，最终由输出高可信度的定位与认证结果。集中式融合模型基本功能结构见图2。

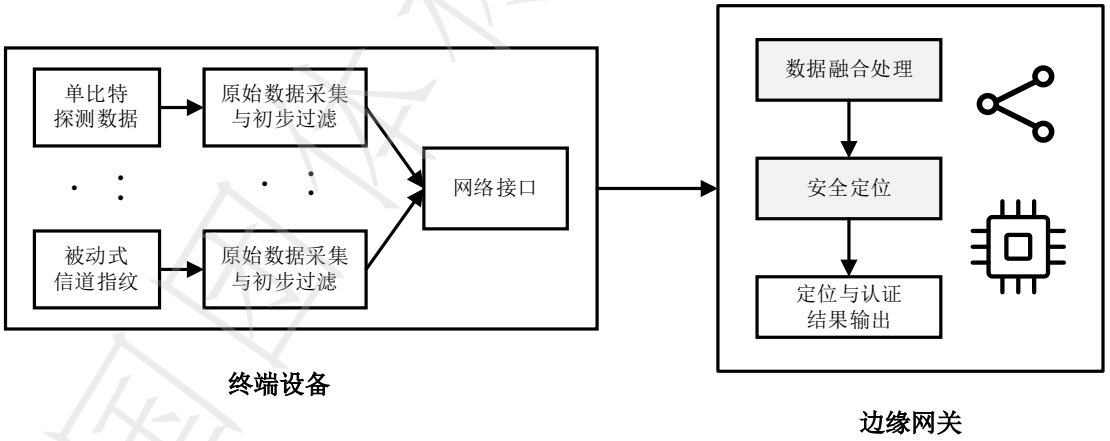

图2 集中式融合模型基本功能结构

5.3 分布式融合模型

终端设备对多源信息分别完成原始数据采集与初步滤波，并进行初步数据融合与定位，随后通过网络接口将初步融合定位结果上报至边缘网关；在边缘网关侧，先对上报的初步融合数据执行多模态深度数据融合处理，再进行抗攻击的高精度安全定位解算，最后输出定位与认证结果。分布式融合模型基本功能结构见图3。

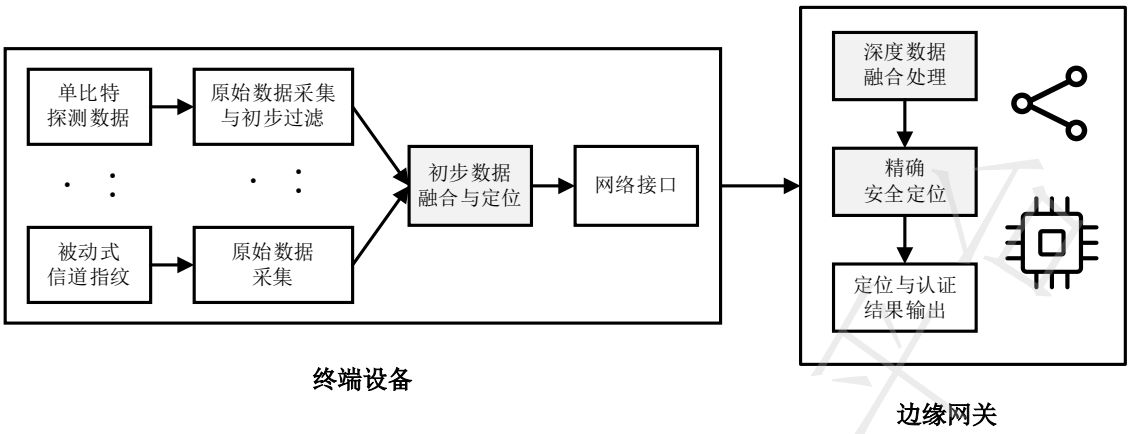

图3 分布式融合模本功能结构

6. 基本功能

6.1 概述

系统应具备多源数据采集功能、数据预处理功能、数据融合功能、安全定位功能、系统管理功能和平台交互功能。应支持标准化数据接口，宜采用开放式架构设计。系统应具备远程和本地管理能力，应支持配置参数持久化存储。应具备对异构数据源的统一接入与管理能力，实现数据标准化处理与安全传输。

6.2 数据采集功能

应支持以下数据源的接入与采集：

a） 支持GNSS定位数据采集，包括但不限于GPS、北斗、伽利略等系统；

b） 支持无线网络定位信号采集，包括WiFi、蓝牙、NB-IoT、UWB等；

c） 支持惯性传感器数据采集，包括加速度、角速度、地磁等；

d） 支持环境感知数据采集，包括温度、湿度、光照、气压等；

e） 宜支持视觉、声学等辅助定位数据采集。

6.3 数据预处理功能

应提供以下数据预处理能力：

a） 应支持数据过滤，去除异常值和冗余数据；

b） 应支持时间同步与数据对齐，建立统一的时间基准；

c） 应支持数据格式标准化转换；

d） 宜支持边缘侧数据降维与特征提取；

e） 应提供数据质量评估机制，对数据可靠性进行量化评估。

6.4 数据融合功能

应提供以下数据融合能力：

a） 应支持基于卡尔曼滤波的数据融合算法；

b） 应支持多级融合架构，包括数据层、特征层和决策层融合；

c） 应支持异构数据源的适配性融合处理；

d） 宜支持基于机器学习的智能融合算法；

e） 应提供融合结果可信度评估机制。

6.5 安全定位功能

应提供以下安全定位能力：

a） 应支持多源定位数据交叉验证机制；

b） 应具备抗欺骗、抗干扰定位能力；

c） 应支持位置认证与验证功能；

d） 应提供定位精度与可靠性评估指标；

e） 宜支持位置隐私保护机制。

6.6 本地管理能力

a） 应支持Web界面、命令行或API等至少一种本地管理方式；

b） 应具备身份认证机制，当连续认证失败超过预设次数时，应具有自动锁定功能；

c） 应实现基于角色的权限分级管理；

d） 应支持配置参数备份与恢复功能；

e） 应支持系统日志记录与审计功能。

6.7 远程管理能力

a） 应支持基于TLS/SSL的安全远程管理；

b） 应支持远程配置参数更新；

c） 应支持远程固件升级与版本管理；

d） 应支持远程系统状态监控；

e） 宜支持基于策略的自动化管理。

6.8 平台交互功能

f） 应支持标准化数据交换格式，包括JSON、XML等；

g） 应支持主流物联网通信协议，包括MQTT、CoAP、HTTP等至少一种；

h） 应具备数据加密传输能力；

i） 应提供标准化API接口，支持第三方系统集成；

j） 应支持数据分级授权访问机制。

7. 接口要求

7.1 数据采集接口要求

系统应支持多源数据采集接口，包括：

a) 应支持GNSS数据采集接口，接收灵敏度应不低于-160dBm，定位精度应优于10米；

b) 应支持无线网络信号采集接口，支持WiFi(IEEE 802.11)、蓝牙(BLE)、UWB等至少一种技术，采集RSSI/CSI信息；

c) 应支持惯性传感单元接口，支持加速度、陀螺仪、磁力计等数据采集；

d) 应支持环境感知接口，采集用于位置特征识别的环境参数；

e) 宜支持标准化传感器接口规范，参见GB/T 34068所述。

7.2 数据交换接口要求

a) 应支持标准化数据交换格式，如JSON、XML等；

b) 应支持统一数据模型，遵循GB/T 40778.2信息描述方法；

c) 应提供实时数据流接口与批量数据接口；

d) 应支持数据融合引擎的输入/输出接口规范；

e) 应提供定位结果标准化输出接口。

7.3 系统集成接口要求

a) 应提供标准化API接口，支持RESTful或WebSocket等方式；

b) 应支持与第三方平台的安全数据交换接口；

c) 应提供位置信息验证接口，支持外部系统进行位置认证；

d) 宜支持开放式插件接口，便于扩展新的数据源和算法模块；

e) 应支持标准化的数据访问控制接口。

8. 协议要求

8.1 通信协议要求

系统组件间通信应采用标准化协议，包括但不限于：

a) 设备数据采集层：应支持CoAP、MQTT、HTTP等至少一种协议；

b) 数据传输层：应支持TLS 1.3及以上版本进行安全传输；

c) 应用交互层：应支持标准化的API调用协议；

2. 无线通信应支持以下协议之一或多种组合：

a) IEEE 802.11 (WiFi)系列协议；

b) 蓝牙5.0及以上版本；

c) IEEE 802.15.4 (ZigBee/Thread)；

d) NB-IoT/eMTC等LPWAN协议；

e） UWB通信协议。

8.2 数据融合与定位协议要求

a） 数据融合算法应遵循标准化处理流程，支持多层次融合架构；

b） 定位数据交换应采用标准化位置表达格式，包括坐标系定义、精度表示和可信度指标；

c） 系统架构应参照GB/T 40778.1相关内容设计；

d） 数据标识与描述应符合GB/T 40778.2相关规范；

e） 应支持定位认证协议，实现位置信息的可信验证。

8.3 安全协议要求

a） 应支持数据加密传输协议，保护敏感位置信息；

b） 应实现基于PKI体系的身份认证协议；

c） 应支持安全密钥协商与更新协议；

d） 应支持防重放攻击协议机制；

e） 宜支持位置隐私保护协议，提供位置信息的可控分享机制。

9. 系统管理维护要求

9.1 系统参数配置要求

系统应提供统一的配置管理界面，支持对多源数据采集模块、数据融合引擎和安全定位模块的参数进行配置。

对于分布式融合模型，应支持边缘节点和云端节点的协同配置管理，确保参数一致性。

9.2 远程参数配置要求

系统应支持基于TLS/HTTPS的安全远程配置协议，实现对设备参数的远程配置。应支持基于角色的访问控制机制，确保仅授权用户能修改关键参数。当本地配置与远程配置参数冲突时，应优先采用安全等级更高的配置源。

9.3 软件升级要求

系统应支持远程升级功能，包括感知模块固件、融合算法和安全组件的更新。升级过程应符合以下要求：

a） 应对升级包进行数字签名验证，确保来源可信；

b） 应进行版本兼容性检查，防止安装不兼容组件；

c） 应实施升级文件完整性校验，发现异常时终止升级并回滚；

d） 应支持差分升级机制，减少传输数据量；

e） 升级过程中基本定位功能应保持可用。

9.4 数据与参数备份要求

系统应具备以下备份能力：

a） 应支持关键配置参数的本地与远程备份；

b） 应支持融合算法模型参数的定期备份；

c） 备份数据应采用加密存储方式，密钥管理应符合GB/T 37025-2018要求；

d） 应对备份和恢复操作实施严格的权限控制；

e） 应支持定时自动备份和手动备份功能。

9.5 恢复默认配置要求

系统应提供选择性配置恢复机制，支持以下功能：

a） 支持全局参数恢复与模块级参数恢复；

b） 提供本地与远程恢复操作接口；

c） 恢复操作前应创建当前配置快照，便于必要时回退；

d） 恢复过程应记录详细的操作日志。

9.6 系统重启要求

系统应提供安全受控的重启机制：

a） 支持本地与远程系统重启功能；

b） 重启前应完成挂起任务处理与数据保存；

c） 重启操作应具备多级授权验证；

d） 支持模块级重启与全系统重启选项；

e） 重启过程应保留核心定位能力，满足最低安全定位需求。

9.7 系统日志要求

系统应建立完整的日志管理机制：

a） 记录系统运行状态、参数变更、访问控制、定位过程、异常事件等关键信息；

b） 日志应包含时间戳、操作类型、操作者身份、操作结果等要素；

c） 日志应采用加密存储，防止非授权访问与篡改；

d） 应支持日志分级管理与自动归档功能；

e） 应实现日志远程备份与安全审计功能。

9.8 数据融合与定位服务配置要求

a） 系统应支持多源数据融合策略的配置，包括数据权重、融合算法选择、特征提取参数等；

b） 应支持定位安全策略配置，包括位置验证阈值、防欺骗参数、隐私保护级别等；

c） 应支持对接第三方数据源与应用系统的参数配置；

d） 系统宜支持根据环境变化自适应调整融合算法参数；

e） 应支持云端与边缘侧的融合策略协同，确保一致性与互操作性。

9.9 安全审计要求

a） 系统应建立安全审计机制，对定位请求、数据访问和系统操作进行全程跟踪；

b） 应提供多维度安全审计报告，支持按时间、用户、操作类型等条件检索；

c） 安全事件应按风险等级分类，并触发相应的告警机制；

d） 应支持审计数据的加密存储与安全传输；

e） 审计结果应符合GB/T 41479-2022要求，保障数据处理安全。

10. 安全性要求

10.1 数据源安全

a） 多源数据接入安全：

●应建立严格的多源感知设备接入认证机制，符合GB/T 37024-2018第6.2.1节要求；

●应实施基于角色的网络访问控制策略，符合GB/T 37024-2018第6.2.2节要求；

●应对WiFi、蓝牙、UWB、RFID等无线通信数据采用强密码加密保护，防止数据截获与篡改。

b） 数据采集安全：

●应采取措施防止物理感知数据的欺骗与仿冒；

●应建立数据来源可信验证机制，确保感知数据真实性；

●终端硬件应具备抗篡改能力，保障数据采集过程安全。

10.2 数据融合与处理安全

a） 应对数据融合过程实施访问控制和安全审计；

b） 应采用安全隔离机制防止恶意数据污染融合结果；

c） 应采取措施防范融合算法受到旁路攻击；

d） 应建立异常数据识别机制，及时隔离可疑数据源。

10.3 定位结果安全

a） 应建立定位结果完整性保护机制，防止结果被篡改；

b） 应实施定位数据分级保护，对敏感位置信息实施严格访问控制；

c） 应建立位置数据脱敏与匿名化机制，保护用户隐私；

d） 应支持基于加密协议的安全位置验证技术。

10.4 通信安全

a） 系统组件间通信安全：

● 应对所有系统内部通信进行身份认证；

● 使用CoAP协议时，应采用DTLS 1.2及以上版本进行加密保护；

● 使用MQTT协议时，应采用TLS 1.3及以上版本进行加密保护；

● 使用HTTP协议时，应强制使用HTTPS，并禁用不安全的加密套件。

b） 与外部系统通信安全：

● 应采用加密通道保护外部数据交换接口；

- 应实施严格的API访问控制与调用审计；
- 应建立防重放攻击机制，避免定位数据被非法重用。

10.5 数据源安全

a) 多源感知数据与融合结果应采用加密存储，保证存储数据的机密性；

b) 应建立数据完整性校验机制，防止存储数据被篡改；

c) 数据访问应实施严格的身份认证与权限控制，采用多级授权机制；

d) 敏感定位数据应支持安全删除功能，防止数据恢复。

11. 可靠性要求

11.1 数据源可靠性

a) 应建立多源数据质量评估机制，识别并剔除低可靠性数据源；

b) 系统应能容忍部分数据源失效，保持基本定位功能；

c) 应建立数据源冗余策略，关键场景下至少具备三种以上独立定位数据源；

d) 应支持动态数据源优选机制，根据环境变化自适应选择最可靠数据源。

11.2 融合算法可靠性

a) 融合算法应具备异常数据识别与处理能力；

b) 应建立算法降级运行机制，在计算资源受限情况下保障基本功能；

c) 应实施融合算法性能监控，及时发现并处理性能异常；

d) 关键算法模块应支持冗余部署，防止单点故障。

11.3 系统韧性设计

a) 系统应具备软件双备份能力，实现在主要软件模块故障时自动切换至备份模块；

b) 关键处理节点应支持冗余部署，实现故障自动转移；

c) 系统应具备自我诊断与恢复能力，能够识别并隔离故障组件；

d) 应建立完整的系统状态回滚机制，支持配置与数据的快速恢复。

11.4 服务持续性保障

a) 系统应支持不间断服务机制，确保核心定位功能24小时可用；

b) 应建立定位服务质量监控体系，包括精度、可用性、响应时间等指标；

c) 应提供服务降级策略，在极端条件下保障基本定位能力；

d) 应建立完善的故障转移机制，实现在组件失效时的无缝切换。