



中华人民共和国国家标准

GB/T XXXXX—XXXX

可持续流动与交通 基于 5G 通信的自组网 网导则

Sustainable mobility and transportation — Guidelines for mesh
networks based on 5G communication

(ISO 37184:2023, MOD)

(征求意见稿)

(本草案完成时间：2026-08-03)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

国家市场监督管理总局
国家标准化管理委员会 发布

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 总则 1

 4.1 概述 1

 4.2 自组网的创建及与5G骨干网的连接 2

 4.3 目标城市问题及自组网提升交通服务的效果 2

5 自组网的应用 2

 5.1 概述 2

 5.2 交通服务的推广 3

6 安全性 3

 6.1 数据传输性能 3

 6.2 数据传输安全性 3

7 个人隐私保护 5

8 运行观测 5

 8.1 概述 5

 8.2 观察参数 5

 8.3 服务优化 5

参考文献 6

前 言

本文件按照 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。

本文件修改采用 ISO 37184:2023《可持续流动与交通 为5G通信提供自组网的交通服务框架》。

本文件与 ISO 37184:2023的技术差异及其原因如下：

- a) 更改了标准名称由“为5G通信提供自组网的交通服务框架”调整为“基于5G通信的自组网导则”，更改后的名称更符合标准内容，并易于理解；
- b) 增加了三项“规范性引用文件”（见第2章），原因是按照标准内容有直接引用这些引用文件；
- c) 增加了“术语和定义”中“自组网”术语（见3.1），便于使用者理解；
- d) 修改了“总则”中关于3GPP TS 38.104的5G通信频段的标准引用，调整为引用国内标准（见4.1），原因是已有国内标准对5G工作频段做了规范，采标后应按照国内标准进行调整；
- e) 删除了“自组网的应用”中关于3GPP TR 38.874的引用（见5.1），原因是“集成接入与回程”是通用术语，不需要引用白皮书文件进行说明；
- f) 增加了“数据传输安全性”中增加了“宜使用国产自主、高安全低成本易维护的密钥技术”相关推荐性要求（见6.2.1），让标准匹配国家安全技术规范。
- g) 修改了“个人隐私保护”中关于IEEE Std 802.11aq:2018的标准引用，调整为引用国内标准（见第7章），原因是已有国内标准对做了规范，采标后应按照国内标准进行调整。

本文件做了下列编辑性改动：

- 6.2.2.1 概述章节中，国际标准编号替换为对应的国家标准编号；
- 8.2 观察阐述章节中，国际标准编号替换为对应的国家标准编号；
- 参考文献中，国际标准编号替换为对应的国家标准编号；
- 调整了格式和标点符号，以符合 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》的要求）。

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。

本文件由全国城市可持续发展标准化技术委员会（SAC/TC 567）提出并归口。

本文件起草单位：中城智慧科技有限公司、中国标准化研究院、上海象形通讯科技股份有限公司、中国世界贸易组织研究会数字经济和数字贸易专业委员会、中城智慧（北京）城市规划设计研究院有限公司、河南交通职业技术学院、河南中天高新智能科技股份有限公司、中汽信息科技（天津）有限公司、广东省电信规划设计院有限公司、临泉县中原牧场供应链管理有限公司、上海信诚智享数字科技有限公司、国网思极位置服务有限公司、中移（成都）信息通信科技有限公司、中铁二十一局集团第五工程有限公司、中咨数据有限公司、中车青岛四方车辆研究所有限公司。

本文件主要起草人：聂明、赵飞、杨勇、李超、阎伟、李小强、周文帅、李玲玲、彭桂林、杨锋、曹喆喆、汤飞飞、吴龙照、甘斌斌、阎毛毛、郑承夏、叶丽云、胡全贵、陈春雷、宋湘君、戴瑶、成维明、张蕴灵、邵景干、王雪虹、舒畅、张红芬、赵明喆、朱叶、钱振宇、任鹏远、胡淼。

引 言

5G 是新一代蜂窝移动通信服务，可连接个人计算机、智能手机等各种终端设备。当通过二维码、人脸识别等方法将非电子物品的图像转换成电子数据进行识别后，这些物品也能接入 5G 网络参与通信。因此，任何物品均可在 5G 网络中实现互联。5G 通信具有高速、低时延、大容量数据传输的特点，并可结合边缘计算技术以提升性能。

5G 通信使用高频段载波，该频段内此前存在许多空闲信道。然而，高频波在传播过程中极易受物体干扰而产生散射。这一缺陷导致 5G 通信需要建设大量基站，才能成功接收和转发信号。

交通服务是最广泛的网络，通过公路、铁路、河流或运河将人、配送物品及货物连接到村庄、城镇、城市和大型城区。这些公路、铁路、河流或运河都配备有路灯、交通信号、标志牌、公共汽车站、铁路仪器、车站、港口等交通设施。在人类活动的地方，私人和商业车辆也都会很活跃。因此，交通设施和车辆是安装载波收发节点的理想场所。这些设施与车辆静态或动态地构成局部自组网络，可以与 5G 通信的骨干网有机重叠。从而间接且有效地补充了目前使用 5G 通信服务的交通服务。

本文阐述了如何利用交通设施和车辆提供尽可能多大型并稳定的自组网，作为当前 5G 骨干网的补充，为使用 5G 通信服务的交通服务做出贡献。

可持续流动与交通 基于 5G 通信的自组网导则

1 范围

本文件提供了基于 5G 通信的自组网导则，规范了自组网的应用、安全性、个人隐私保护和运行观测。

本文件适用于智慧交通及相关服务的运营商，用于通过自组网扩展 5G 通信网络，以提升交通服务的 5G 通信网络稳定性和性能。

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（包括所有的修改单）适用于本文件。

GB/T 36625.3-2021 智慧城市 数据融合 第 3 部分：数据采集规范

YD/T 3929-2024 5G 数字蜂窝移动通信网 6GHz 以下频段基站设备技术要求（第一阶段）

YD/T 4249-2023 5G 数据安全总体技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

自组网 mesh network

一种去中心化的无线网络拓扑结构，网络中的每个节点都可以发送和接收数据，每个节点都可以与一个或者多个对等节点进行直接通信。

4 总则

4.1 概述

5G 通信服务已逐步在全国普及，通过增加载波信道数量实现更多数据传输。3G 和 4G 通信主要使用低频信道，5G 通信则采用高频段，根据 YD/T 3929-2024 5G 数字蜂窝移动通信网 6GHz 以下频段基站设备技术要求（第一阶段），我国 5G 通信载波带宽大于 100MHz 的工作频段为 2515MHz 至 2675MHz、3300MHz 至 3400MHz、3400MHz 至 3600MHz、4800MHz 至 4900MHz、4900MHz 至 5000MHz。由于 5G 通信高频载波波长较短，传播过程中易散射并大幅衰减。为了在更远距离传输中获得足够的信号幅度或功率，并扩大服务覆盖范围，需建设更多基站，但这需要充足的电力供应和较大的运营场地，导致成本增加。由于这些原因，5G 骨干网的通信服务区域未能实现全区域覆盖。

交通系统已形成密集且庞大的网络，交通设施可以作为自组网的小基站安装地点，以扩大 5G 通信覆盖范围。小基站体积小、重量轻，可简单部署于多个地点并进行本地通信信号处理。这样的小基站

称为自组网节点，并形成一個自组网。多个小自组网相互重叠可以形成大自组网，并可与现有 5G 骨干网进一步融合。

每个城市都配备有交通车辆和交通设施（如公交站、火车站、港口、机场、公路、铁路、服务设施及相关商业建筑），其具体规模取决于人口数量和人口密度。公路和铁路沿线的路灯、交通信号灯、标志牌及电力和信号杆等交通设施，其网络覆盖整个城市或大型城区。因此，交通车辆和交通设施是安装自组网节点的理想地点。自组网节点具有体积小、重量轻、功耗低、维护成本低的特点，其信号覆盖半径约 150 米，但大量自组网节点形成的网络可构成大型网络。车辆通过移动有效地帮助动态形成自组网；智能手机如果有足够路由功率，也可参与自组网的构建，这样行人携带手机在城市中移动时，也能为自组网形成提供支持。

4.2 自组网的创建及与 5G 骨干网的连接

在交通设施和车辆中部署大量自组网节点形成的自组网，可实现自组网内及自组网间通信信号的自动路由。在自组网中，自组网节点发射的信号通过节点间跳传，寻找到达 5G 骨干网网关的最短路径。

自组网的通信服务是对现有 5G 通信服务的补充和适配，不会对 5G 通信技术和服务产生负面影响。自组网宜具备适应性和灵活性，以实现网络配置的动态高效调整与优化。

通过提供自组网实现的智慧交通旨在支持现有 5G 骨干网，为基于 5G 通信的交通服务提供支撑。未来随着通信技术（如 6G、7G）的发展，通过提供自组网实现的智慧交通则可随之做相应的调整。

4.3 目标城市问题及自组网提升交通服务的效果

城市居民和访客在使用交通服务时，需要稳定的通信及高速、大容量的数据传输。5G 通信可满足这一需求，但目前无法实现全区域的稳定服务覆盖。通过提供自组网，可加速覆盖区域扩展，提升用户对通信服务的访问能力。除通信和交通业务的基本需求外，以下示例展示了基于自组网的智慧交通服务应用：

示例 1：汽车通过获取障碍物和实时定位信息实现自主行驶。通过为 5G 通信提供自组网，智慧交通服务可提供可靠的交通和延误信息，覆盖所有道路及车辆，扩大自动驾驶的运营范围。

示例 2：在站点间运行的公交和卡车服务，因安装和维护路边监控成本高，难以实现跟踪。但通过 5G 通信中的智能手机实时收集车队信息，可实现对公交和卡车调度的跟踪和控制，确保准点运营，满足用户出行和货物运输的计划需求。而该服务需 5G 通信对服务路线的充分覆盖。

5 自组网的应用

5.1 概述

基于 5G 的通信的自组网实现的目标是通过大量自组网节点形成自组网，自组网相互有机重叠，形成大自组网，并与 5G 骨干网连接，从而为智慧交通提供稳定的、全面覆盖的通信服务。在自组网中，交通设施和车辆作为自组网内自动路由及与 5G 骨干网连接的节点。所有自组网节点和网关在加入或离开自组网时，不影响通过自组网的端到端通信，也不得受其影响。由于自组网需连接已建成并运行的骨干网，自组网应设计为高健壮性，该功能为“集成接入与回程”。

即便是在小型村镇，公交车、站点、路灯、路标、摩托车以及各类汽车，也都能接入自组网节点并充当路由点。若自组网节点配备协议转换软件，这些交通设施与车辆还可作为网关，实现与 5G 骨干

网之间的信号传输。在中大型城市，交通服务更为丰富，火车、火车站及其他运营设施的数量也更多，由此形成规模更大的交通网络。可见，交通网络的规模取决于当地人口，交通网络可直接根据 5G 通信市场的需求，直接用于自组网的构建。

5.2 交通服务的推广

为扩展智慧交通服务，可由电信用户和企业向交通运营商提供收入支持，激励运营商利用其交通设施参与自组网建设。此外，鼓励市民和交通用户作为服务支持者（而非仅作为用户）参与，例如在私人车辆上安装自组网节点，同样也是有效举措。政府可通过财政和税收激励措施，鼓励智慧交通服务发展，推动该类通信作为公共基础设施的可行性。

6 安全性

6.1 数据传输性能

为确保交通设施和车辆提供的自组网中 5G 通信的安全性，需满足特定条件。在自组网内部以及多个自组网之间（包括动态创建的自组网），需实现海量数据的高速、实时、无故障传输。由于 5G 通信用于自动驾驶等高度安全的运营场景（其目标是通过与其他车辆及障碍物实时通信，在公共道路上实现零碰撞或零事故），因此数据传输需防范网络攻击。

当自组网节点、自组网及网关发生故障或损坏时，途经这些节点和网络的通信将受到干扰或中断。为避免此类情况（非小型基站本身出现的机械故障），需定期更换电池为新电池，或者使用供电时间超过小基站运行时间的电池。

由于智慧交通设施与车辆所构建的自组网会参与 5G 通信，自组网中的数据传输宜满足以下要求：

- a) 采用非集中式的端到端传输模式；
- b) 具备大容量传输能力（下行链路超过 10GB，上行链路超过 1GB）；
- c) 高速传输（速率超过 1GB/s）；
- d) 支持在线或离线传输；
- e) 低时延（例如车对车服务时延小于 5ms）；
- f) 高效率（注：公钥加密技术通过动态使用公钥、私钥及匹配字段，实现高效且低时延的数据传输）；
- g) 不可篡改且不可否认；
- h) 信息收集、传输和发布易于操作；
- i) 低成本。

6.2 数据传输安全性

6.2.1 概述

确保安全是智能交通服务中最重要的一环，因其关系到系统韧性——即在面临 4.1 与 6.1 节所述网络攻击风险时，仍能执行核心任务或关键功能的能力。

自组网通信需防范出现故障或遭受恐怖袭击。因此，安全性宜满足：

- a) 实时性；
- b) 动态性；
- c) 适用于任何终端（包括移动终端）；

- d) 防伪造;
- e) 防重复传输;
- f) 不可否认;
- g) 设备(如传感和定位设备)无损坏。

为确保自组网通信的高安全性,同时保持高速、低时延的数据传输性能,数据应通过快速切换握手、认证和加密机制进行加密。同时还需考虑降低安全机制的搭建、运营及维护成本。自组网中数据传输的安全技术宜使用国产自主、高安全低成本易维护的密钥技术,宜按 GB/T36625.3-2021 中 9.2 对组合诚信密钥系统(CCKS)中的技术安全规定执行,实现:

- a) 非对称公钥;
- b) 大容量密钥;
- c) 认证程序简单快捷;
- d) 无需第三方认证;
- e) 支持在线和离线通信。

6.2.2 安全流程

6.2.2.1 概述

在 GB/T 46142-2025 定义的数字化支付智慧交通服务中,对金融交易实施了最高的安全流程。对于数字化支付,传输的数据使用公钥和私钥进行加密,公钥和私钥每次创建一次,且只使用一次,并在同样动态创建的匹配字段中进行匹配。对于 GB/T 46141-2025 指定的 QR 码识别/认证,也以相同方式使用这些密钥和匹配字段,以实现高安全级别。

6.2.2.2 安全原则

在智能交通设施及车辆构建的自组网中,公钥与私钥由数据发送方与接收方临时创建。为确认公私钥匹配,需临时创建匹配字段。接收方临时创建匹配字段,整合发送方创建的发送方私钥和接收方通过通用算法创建的发送方公钥;同理,发送方临时创建匹配字段,整合接收方创建的接收方私钥和发送方通过相同算法创建的接收方公钥。当两组密钥在各自对应的字段中成功匹配后,即可实现高精度的相互识别。为实现高安全性,所有个人对象数据、公钥、私钥和匹配字段均宜临时创建并仅使用一次。为提升流程处理效率,不依赖第三方认证中心,而是由自组网内的数据传输参与者预先约定通用算法,来临时生成和使用密钥与字段。

在智慧交通服务中,为确保通信的安全性和可管理性,所有设备(如检测和定位设备、传输设备、计算机、无线路由器、智能终端)均需分配唯一特定数字身份标识。设备信息经公钥加密后,与管理中心预先分配的加密标签(作为设备数据集的标识,包含位置、功能和特性等)关联,存储于数据库中。

设备间传输和交换数据时,采用双向点对点认证,通过匹配公钥和私钥验证设备身份标识的合法性。双方私钥成功匹配后,设备被识别并开始传输或交换数据。

该认证通过边缘计算实现,无需第三方认证中心。虽为最高安全级别,但处理时间可控制在 10ms 内,该时延基本可忽略不计,适用于自动驾驶等不允许通信延迟的场景。

6.2.3 与 5G 骨干网之间的网关安全性

自组网的安全性按 6.2.2 实现，5G 骨干网的安全性则通常通过基于公钥基础设施的加密标准实现。因此，自组网与 5G 骨干网之间的网关或接口两侧的安全算法不同。通信信号通过网关时，需实现两种安全系统算法的转换，且保持安全级别不变。

7 个人隐私保护

交通设施和车辆提供的自组网中，个人隐私保护的性能和质量应与现有 5G 骨干网一致。YD/T 4249—2023 的第 10 章节规定了个人隐私保护的要求。因此，通过提供 5G 通信自组网实现的交通服务应遵循该条款，确保智慧交通服务中的个人隐私保护。

8 运行观测

8.1 概述

为推行智慧交通服务及维持其预期性能，并确认其有效性，应定期观察 8.2 中的参数。

8.2 观察参数

- a) 智慧交通服务中使用的应用程序数量；
- b) 用户使用智慧交通服务的次数；
- c) 使用智慧交通服务的机构和业务活动数量（如每月统计）；
- d) 目标城市/区域通过智慧交通服务实现的自组网通信次数；
- e) 目标城市/区域通过智慧交通服务实现的自组网通信时长；
- f) 目标城市/区域通过智慧交通服务实现的自组网通信数据量；
- g) 智慧交通服务的运行故障数量和类型；
- h) 智慧交通服务的通信中断时长。

用于比较和观察智慧交通性能的参数包括：GB/T 36749-2018 和 ISO 37122 中定义的智慧交通普及率指标。

8.3 服务优化

若 8.2 中的参数值无变化，应改变交通服务条件。改变交通服务条件不是改变原则，而是改变流程，包括技术参数值。为修正智慧交通服务条件，需确认服务实施区域在规划中是否存在未预见的情况或因当地特定条件导致的异常，并通过修改智慧交通服务系统的当前条件解决这些异常。

参 考 文 献

- [1] GB/T 36749-2018 城市可持续发展 城市服务和生活品质的指标
 - [2] GB/T 46141-2025 智慧城市基础设施 智慧交通快速响应矩阵码应用指南
 - [3] GB/T 46142-2025 智慧城市基础设施 智慧交通数字化应用支付指南
 - [4] ISO Guide 82, Guidelines for addressing sustainability in standards
 - [5] ISO 37122, Sustainable cities and communities — Indicators for smart cities
 - [6] ISO 37154:2017, Smart community infrastructures — Best practice guidelines for transportation
-