报 告

2024-12

IMT-2020(5G)推进组

Ambient IoT 核心网关键技术研究

目 录

第一章　Ambient IoT应用场景与标准进展

1.1 Ambient IoT 应用场景

物联网随着 5G 网络的部署和终端类型及数量的增加在很多行业得到广泛应用，其中的无源或环境物联网(Ambient IoT，AIoT)对终端功耗、终端尺寸和成本提出极致的要求；例如功耗可以低到数微瓦级别，成本降到 1 元甚至更低。相对于其他类型物联网技术，Ambient IoT 终端能够从环境采集能量、使用反向散射通信模式，再加上终端低成本的优势，使得 Ambient IoT 在如物流、仓储、交通、工业、农业、智慧城市、智能家居等领域已经或者未来会有广泛的应用。

物流：Ambient IoT 技术可以应用在物流行业的全流程中，如货物跟踪与监控，即在货物运输过程中，使用 Ambient IoT 标签、GPS 定位和传感器等技术实时跟踪货物位置和状态，如温度、湿度等，可以及时发现异常情况，如货物丢失、温度超标等并做出快速响应。Ambient IoT 还可应用于物流的运输路径优化，结合 GPS、交通信息等数据，优化车辆行驶路径，降低运输成本和时间，实时监控车辆状态以提高运输安全性。借助 Ambient IoT 技术还可以跟踪产品使用情况，提供个性化的售后服务，可预测产品故障，提前安排维修保养等。Ambient IoT 技术具备识别准确度高、性能可靠、存储信息量大、适用于严苛环境等特点，且 Ambient IoT 标签功耗低、体积小、成本低，适用于物流货物的全流程、精细化管理。

仓储：Ambient IoT 技术应用在仓储行业的多个方面，包括智能库存管理，在仓库内部署各种具有通信功能的传感器，实时监测并上报库存数量、货品状态(温度、湿度等)，通过数据分析预测需求，自动调节库存水平，降低库存成本，及时发现库存异常并快速做出响应。Ambient IoT 可以助力自动化入库出库，自动识别仓库货品，实现无人值守的入库出库操作，与 AGV、机器人等无人搬运设备联动提高搬运效率和准确性。Ambient IoT 技术还能实现智能仓储货架管理，在货架上安装重量传感器，实时监测货架载重情况，结合标签信息，优化货物摆放以提高仓储空间利用率。Ambient IoT 标签具有极小的尺寸与极低的成本，在大型仓储等货物吞吐量巨大的场景下极具竞争力，且得益于标签及读写器性能的提升，新型无源物联将支持货物大批量自动化读取，具备更高效的盘存效率。

交通：对于交通行业，Ambient IoT 技术可应用于智能交通管理，如车载传感器、路边单元可以收集车辆运行、道路等数据，实现对交通状况的实时监控、车辆调度优化、信号灯控制等功能，提高城市道路的通行效率。Ambient IoT 技术还可应用于智能停车管理，在停车场部署带通讯功能的车位检测传感器，可以实现车位检测、引导、预约等功能，让停车更加便捷高效。在车联网应用中，通过在汽车上安装 IoT 传感器和通信模块，可以实时监控车辆状态、位置信息，并通过车载终端提供故障诊断、远程控制等功能。另外在城市交通电动自行车监管方面，Ambient IoT 标签具有准确度高、性能可靠、低成本、易部署等特点，可粘贴在电动自行车车牌上，协助交通部门监控电动自行车行驶、停放状态；或者借助环境能量收集技术，新型无源标签可与温、湿度等传感器结合，附着在电动自行车电池模组上，监控其温、湿度状态等。

工业：Ambient IoT 技术在工业制造中有广泛的应用场景，可以帮助提升工厂的智能化水平和运营效率。以下是一些主要的应用场景：生产过程监控和优化，在生产线上部署各种有传感器功能的 Ambient IoT 标签，实时监测设备运行状态、产品质量、能源消耗等关键数据，通过远程监控和自动控制，实现生产过程的智能化管理和优化。还可用于设备管理和维护，在关键设备上安装 Ambient IoT 标签，实时监测设备运行参数和异常情况，利用远程诊断和维护功能，缩短设备故障响应时间，提高设备可用性。Ambient IoT 技术还可应用于工厂环境中的协作机器人和无人作业，在生产线上部署协作机器人，通过 Ambient IoT 标签进行信息采集和传送实现人机协作，提高作业灵活性和效率；利用无人驾驶小车、AGV 等实现仓储、搬运等无人作业,降低人工成本，通过 IoT 标签监控和控制协作机器人及无人作业设备，保障作业安全性。现代化工厂环境中存在大量的传感器节点，用于温度、湿度、振动监测、生产线监测、危险事件监测等方面。同时，在某些应用中，可能要求传感器节点部署在恶劣的环境、特殊的位置空间，甚至是极端危险环境中以完成对制造流程数据的智能感测。工业场景具有作业环境特殊，时延敏感等特点，一般要求网络通信时延为十毫秒至百毫秒级，Ambient IoT 标签可支持多种传感，且具备耐高/低温、抗腐蚀能力；Ambient IoT 标签因其免电源、免维护的特性，可部署在以上工厂特殊环境中，同时基于环境能量采集技术，实现传感器标签的自供能。

农业：Ambient IoT 具有的低成本、低功耗、无需电源的特点，非常适合在农业生产的各个环节进行应用。例如，用于对农作物生长环境监控，对水分、土壤、空气等植物所生长的环境进行监控分析，及时了解环境变化，保证植物成长和农作物质量达到合适生长的水准。用于对农畜产品安全生产监控，Ambient IoT 技术可以加强人们对农畜

产品安全生产的管理，通过 IoT 标签对农畜产品进行生产过程的全称识别与跟踪，例如在饲养动物的耳朵上植入 IoT 标签，作为身份标识，可以同时绑定这些动物的详细资料，后续这些动物从农场到加工厂的全过程都可以利用 IoT 标签来进行追踪管理，以判断该农畜产品的安全生产状态信息。在比如用于农产品流通管理，在农产品上粘贴无源物联标签，会大大提高产品信息在流通过程中的采集速率，提高农产品供应链中信息集成和共享程度，提高了整个供应链的效益。

智慧城市：Ambient IoT 技术凭借其低成本、免维护的优势，在智慧城市的各个领域都有广泛应用前景，实现城市基础设施及资源的动态感知、集中监控、智能报警、诊断分析、远程运维等。对于智能路灯系统，Ambient IoT 传感器可以被安装在路灯上,自主检测周围的光照、人流等情况，实现智能调节路灯亮度，从而提高能源利用效率；这些传感器无需外部电源供给，可以长期工作。应用于垃圾监测和收运优化，IoT 标签可以贴附在垃圾桶上，检测垃圾填充程度，并通过蜂窝网络把数据传输给管理中心；这样可以优化垃圾收运路线和提高效率。应用于城市停车场的停车位监测，Ambient IoT 传感器可以安装在停车位上，检测车辆进出情况，并把信息发送给停车管理系统；这可以帮助驾驶员快速找到空余车位。应用于城市家庭的水电气表远程抄表，Ambient IoT 技术可以实现水电气表的远程自动抄表，摆脱了传统的人工巡检，提高了抄表效率和数据准确性。应用于城市环境监测，Ambient IoT 传感器标签可以被部署在城市各个角落，监测空气质量、噪音水平等环境指标，为城市管理和规划提供重要依据。

智能家居：Ambient IoT 技术在智能家居中的应用，能够提高家居自动化水平，同时也更加节能环保和方便用户使用。智能家居利用家电的自动控制、照明控制、温度控制、防盗和报警控制等多种功能和手段，使家居环境更加安全、便利、舒适。Ambient IoT 传感器可以贴附在墙壁、家具、家电等位置，无需外部电源供给。这些传感器可以实时监测温度、湿度、光照、门窗状态等家居环境数据，并将数据无线传输给智能家居控制系统，可以根据收集的数据,自动调节空调、灯光、窗帘等设备，提升家居的智能化水平。Ambient IoT 技术还可应用于家用物品定位与寻找，家庭生活用品存储类似于小型仓库，基于 Ambient IoT 技术可以快速记录家庭储物信息，以及确定遗忘物品的位置。 可采用 Ambient IoT 标签附着在用户需要定位的家庭物件上，可以实现非接触式快速自动识别与定位，便于家庭内部使用。

Ambient IoT 技术除了在上述领域的应用外，还可在如可穿戴设备、医疗健康、电

力、铁路运行、公共安全等诸多领域或行业使用。Ambient IoT 的技术优势，结合行业已有的基础设施，能够满足这些领域的特定需求并助力它们更好地为人类社会服务。

1.2 拓扑形态

根据 AIoT 设备与作为读写器的基站或者 UE 的连接方式，3GPP 定义了四种 AIoT 拓扑形态（Topology）。

以下图示中带箭头实线表示 AIoT 数据/信令的传输，箭头方向(单向或双向)表示传输的方向。

1) 拓扑形态 1：基站与 AIoT 设备直连

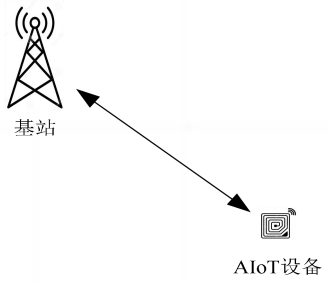

图 1 拓扑形态 1

拓扑形态 1 如图 1 所示。在拓扑形态 1 中，作为读写器的基站与 AIoT 设备直连并与其进行双向通讯。基站与 AIoT 设备之间的通讯包括了数据传输和信令交互。在此拓扑形态中，向 AIoT 设备传送数据/信令的基站可能不同于从 AIoT 设备接收数据/信令的基站。

2) 拓扑形态 2：基站通过中间节点与 AIoT 设备连接

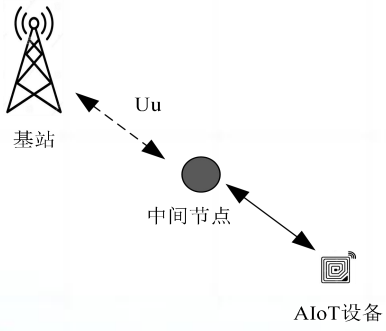

图 2 拓扑形态 2

拓扑形态 2 如图 2 所示。在拓扑形态 2 中，基站与位于 AIoT 设备和基站之间的中间节点进行双向通讯。在此拓扑形态中，中间节点可以是支持 AIoT 功能的中继(Relay)、融合接入与回传(IAB)节点、UE、转发器(Repeater)等。中间节点转发基站与 AIoT 设备之间的数据/信令。

3) 拓扑形态 3：基站通过辅助节点与 AIoT 设备连接

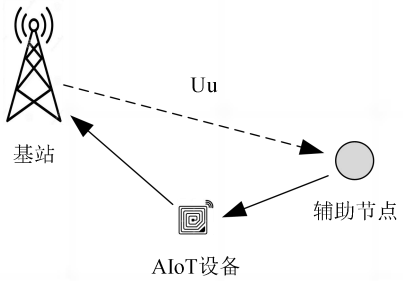

图 3 拓扑形态 3-1

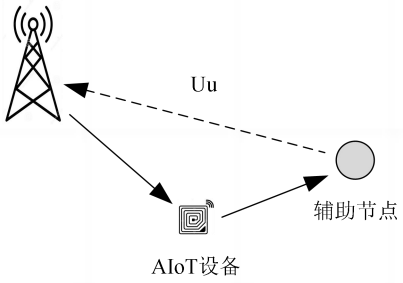

图 4 拓扑形态 3-2

拓扑形态 3 有两种方式，分别如图 3 和图 4 所示。在拓扑形态 3-1 中，AIoT 设备直接传送数据/信令到基站，而从辅助节点接收 AIoT 数据/信令，即下行辅助的方式；在拓扑形态 3-2 中，AIoT 设备从基站接收数据/信令，而传送 AIoT 数据/信令到辅助节点，即上行辅助的方式。

4) 拓扑形态 4：UE 与 AIoT 设备直连

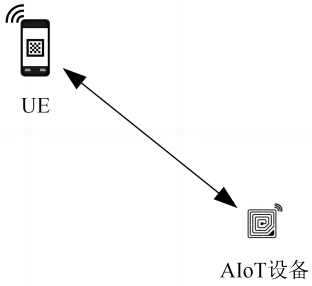

图 5 拓扑形态 4

拓扑形态 4 如图 5 所示。在拓扑形态 4 中，AIoT 设备与作为读写器的 UE 直连并与其进行双向通讯。UE 与 AIoT 设备之间的通讯包括数据传输和信令交互。

以上四种拓扑形态中：拓扑形态 1 适用于基站作为读写器的情形，基站与 AIoT 设备之间距离足够近并且没有遮挡能够实现直接通讯。拓扑形态 2 适用于基站与 AIoT 设备间因为距离或者遮挡原因需要由中间节点转发两者之间的数据或信令；中间节点如前所述可以是中继(Relay)、融合接入与回传(IAB)节点、UE、转发器(Repeater)，对于中间节点是 UE 的情形以 UE 作为读写器，负责与 AIoT 设备的通讯。拓扑形态 3 有两种类型：分别是对于从基站到 AIoT 设备的下行数据/信令需要由辅助节点转发(图 3.1)，以及从 AIoT 设备到基站的上行数据/信令需要由辅助节点转发(图 3.2)；拓扑形态 3 适用于基站和 AIoT 设备间单向(下行或上行)需要由辅助节点转发的情形，辅助节点与基站之间使用传统 Uu 口进行通讯。拓扑形态 4 类似于 RFID 手持读写器的场景，UE 作为读写器与 AIoT 设备通讯，至于 UE 如何与网络连接及传送数据并不做限定。

3GPP 针对上述拓扑形态，明确在 Release 19 阶段首先针对拓扑形态 1 和 2 两类进行研究，并对拓扑形态 2 限定中间节点为 UE 读写器的情形。

1.3 标准进展

3GPP 从 2022 年 Release 18 开始启动对 Ambient IoT 的研究，主要涉及 3GPP SA 和 RAN 若干工作组的工作。

在 3GPP SA 的几个工作组中，SA1 工作组已经完成 Release 19 的研究报告和规范工作，对 Ambient IoT 的应用场景和需求进行了定义，相关输出见 TR22.840 和 TS22.369。SA2 工作组于 2023 年 12 月通过 Release 19 Ambient IoT 的研究立项，对端到端解决方案

进行研究，包括 Ambient IoT 的架构，认证授权及设备标识；以及 Ambient IoT 的签约、注册和连接管理，支持的 Ambient IoT 服务等。目前已完成研究阶段的大部分工作，相关输出见 TR23.700-13。SA3 也正在开展 Ambient IoT 的 Device 认证和授权、AIoT 业务操作安全等相关的研究。

在 3GPP RAN 工作组，首先在 Release 18 对 Ambient IoT 进行了初步研究，对满足 Ambient IoT 用例的设计目标进行了探讨，相关输出见 TR38.848。在此基础上，RAN1~RAN4 工作组对 Ambient IoT 无线技术进行深入研究，相关结论写入研究报告 TR 38.769，包括：代表性用例、部署场景、连接拓扑、环境物联网设备、详细设计目标和所需功能。RAN 工作组研究了多个 Ambient IoT 无线技术和候选方案，基于现有技术无法满足目标用例的所有要求，建议 3GPP RAN 工作组开展新的 Ambient IoT 物联网技术的标准化工作。

ITU 也正在对无源物联进行研究，在 2023 年 ITU-T SG20 工作会议上启动对无源物联的需求和用例进行分析的工作，目前正在讨论阶段，相关输出见[ITU SG20-TD1510 YSTR.Ambient-IoT]。

AMbient Power（AMP）作为 IEEE 802.11 工作组中的一种新的 TIG/SG 于 2022 年成立，致力于解决 802.11 网络中无源物联通信的支持问题；目前工作正在进行中。

国内标准组织 CCSA 也在推进 Ambient IoT 的研究和标准化工作。前期已经完成《基于蜂窝通信的无源物联网应用需求研究》报告，主要研究基于蜂窝无源物联相关的应用场景和业务需求。2024 年 4 月，在 CCSA TC5 WG12 第 35 次会议上，经讨论同意对《支持无源物联网的核心网架构及增强技术研究》进行立项。该项目主要研究支持无源物联技术的 5GC 核心网架构及关键技术，明确所需的架构及网元增强功能，涉及无源物联设备识别与管理、签约管理、连接管理、寻呼及可达性管理、数据传输及服务开放等，预计 2026 年 4 月结项。在 2022 年的 TC10 WG2 第 40 次工作组会议上立项了《基于蜂窝通信技术的无源物联服务 第 1 部分：应用场景及需求》，制定蜂窝网络的无源物联应用场景及需求相关标准，目前已经进入送审阶段。此外，在 2023 年的 TC10 WG2 第 42 次工作组会议上立项了《基于蜂窝通信技术的无源物联服务 第 2 部分：总体技术要求》，拟规定基于蜂窝网络的无源物联总体技术要求，目前正在起草阶段。

第二章　Ambient IoT关键技术

2.1 概述

Ambient IoT 关键技术涉及核心网主要包括几个方面：适用于蜂窝网络的设备标识(Device ID)的设计与使用，对 Ambient IoT 设备的管理；需要支持的 Ambient IoT 的业务类别，如盘点(Inventory)、命令(Command)及具体的读、写等操作；以及支持 Ambient IoT 的网络架构，包括在核心网需要增加或改造的网元，对基站(支持 AIoT Reader 能力的 RAN)的影响等；在特定网络架构下 Ambient IoT 设备的盘点、读、写等业务流程；另外在 Ambient IoT 安全方面，包括对设备和读写器的认证和授权，业务流程中的数据安全等。

2.2 Device ID 设计与 Device 管理

本章节介绍 AIoT 设备标识 Device ID 的设计，以及设备的签约管理等方面的内容。

2.2.1 Device ID 设计

运营商或第三方企业为 AIoT 设备设置永久 AIoT 设备标识（AIoT Device ID），用于识别 AIoT 设备并定位相应的数据管理服务器 （例如新数据管理功能、5G 核心网已有的 UDM 或 UDR）、身份鉴权服务器（Authentication Server）（若执行安全认证）。

永久 AIoT 设备标识包括两部分信息（以下分别称为 Part1 信息和 Part2 信息）；其中，每一部分包含的信息列举如下：

1) Part1 信息：

- ID 类型（ID Type），包括：
  - 指示是否包含网络标识符的信息
  - 指示是否包含用于识别第三方的信息
  - Part2 类型，用于指示 EPC 或其他格式
- 网络标识符（即 MCC+MNC 和/或 NID），当 ID 包括网络标识符时。
- 用于标识第三方的信息，当 ID 包括用于标识第三方的信息时。

2) Part2 信息：

- 在 Part1 信息标识范围内，用于区分不同 AIoT 设备的信息（例如 EPC 或其他格式）。

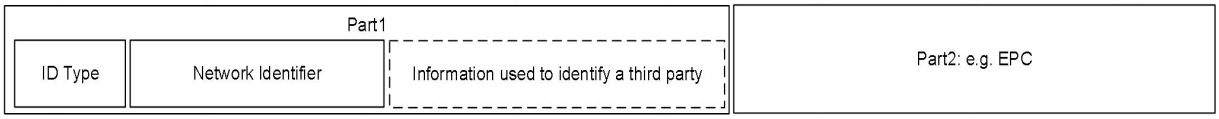

图6：运营商分配的ID示例

对于运营商分配的 AIoT 设备标识符，网络标识符是必需的，该网络标识符或该网络标识符与用于标识第三方的信息的结合可用于选择数据管理服务器、身份鉴权服务器（若执行安全认证）。运营商分配的 AIoT 设备标识符如图 6 所示。

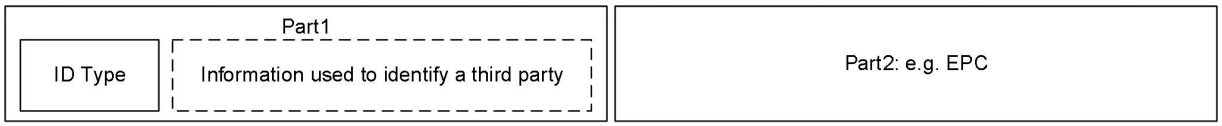

图7：第三方分配的ID示例

对于第三方企业分配的 Part 1 信息，不需要网络标识符。第三方可能是证书持有者（credential holder），也可能不是证书持有者。如果第三方不是证书持有者，则应为网络提供第三方相关上下文，包括用于选择数据管理服务器的信息。第三方分配的 AIoT 设备标识符如图 7 所示。

标识的长度是固定的或动态的在标准上还没有确定，但需要确保 AIoT 设备标识是全局唯一的。

2.2.2 Ambient IoT Device 签约管理

Ambient IoT Device 的签约数据与普通 5G 终端的签约数据不同，它包含 Ambient IoT Device 的永久标识和必要的安全参数。

Ambient IoT Device 的永久标识如果由运营商分配，则由运营商保存 Ambient IoT Device 的签约数据。运营商可以用独立的数据库存储 Ambient IoT Device 的签约数据，隔离 Ambient IoT Device 和普通终端的签约数据。

Ambient IoT Device 的永久标识如果由第三方企业分配，可以由第三方企业管理 Ambient IoT Device 的签约数据，也可以由运营商保存。

当网络收到 Ambient IoT Device 上报的数据，如果网络中保存有 Ambient IoT Device 的签约数据，根据签约数据对 Ambient IoT Device 上报的数据进行校验，从而保障数据隐私和避免越权执行业务操作，提供了高安全管控。如果 Ambient IoT Device 的签约数据由第三方企业保管，Ambient IoT Device 数据安全保障由第三方企业负责。

2.3 Ambient IoT 网络架构

在 1.2 节所述的几种拓扑形态中，3GPP 首先对拓扑 1 和拓扑 2 进行研究；并分别提出支持拓扑 1 的 Ambient IoT 架构和支持拓扑 2 的 Ambient IoT 架构。其中拓扑 1 按照 AIoT 功能与 RAN 读写器的连接分为直连和非直连（通过 AMF）两种方式，拓扑 2 分为基于用户面和基于 RRC 控制面两种方式。

随着未来 Ambient IoT 应用场景的丰富，一方面需进一步研究 1.2 节新所述的其它几种拓扑形态，另一方面考虑可能出现其它新的拓扑形态；这些拓扑形态对应的网络架构也会出现更多的变种。

2.3.1 拓扑 1 的网络架构

支持拓扑 1 的 Ambient IoT 网络架构有两种选项：（1）AIOT RAN 直连 AIOTF；（2）AIOT RAN 通过 AMF 连接 AIOTF。下面具体介绍这两种选项。

2.3.1.1 架构选项 1：AIOT RAN 直连 AIOTF

架构选项 1 即 AIOT RAN 直连 AIOTF 方式，如图 8 所示。

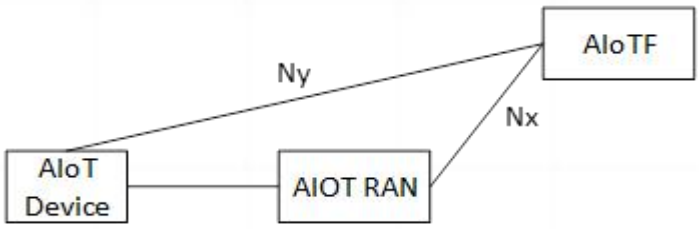

图 8：AIOT RAN 直连 AIOTF

1) AIOTF 是新定义的核心网网络功能，它负责管理 Ambient IoT Device 和执行 Ambient IoT 业务。

a) AIOTF 的主要功能包括：

- 授权 AF 发起的 Ambient IoT 业务请求
- 管理 AIOT RAN / BS reader（比如：根据服务区域）
- 根据 AF 请求的业务区域选择 AIOT RAN / BS reader
- 发送 Ambient IoT 业务指令到 AIOT RAN / BS reader
- 接收 Ambient IoT Device 发送的 Device 标识或 Device 数据

b) AIOTF 支持以下网络接口：

- AIOTF - Ambient IoT Device：接口协议是 AIoT NAS，AIoT NAS 协议用于 Ambient IoT Device 上报 Device 的永久设备标识和数据，并可以加密上报的内容。
- AIOTF - AIOT RAN：AIOTF 负责 AIOT RAN/ BS reader 的选择，向 AIOT RAN 发送 Ambient IoT 业务指令，并接收 AIOT RAN 上报的 Ambient IoT 业务结果。
- AIOTF 与其他核心网网元（比如 UDM，NEF）之间采用服务化接口协议通信。

2) AIOT RAN 可以包含一个或者多个 BS reader，它的功能主要包括：

- 接收核心网下发的 Ambient IoT 业务指令
- 在 Ambient IoT 空口上和 Ambient IoT Device 通信
- 转发 Ambient IoT Device 上报的 Device 标识到核心网

3) Ambient IoT Device 的功能主要包括：

- 接收 BS reader 或者核心网下发的盘存或读写指令
- 上报 Device 标识或者数据
- 支持 Ambient IoT 安全能力

架构选项 1 的协议栈如图 9 所示。

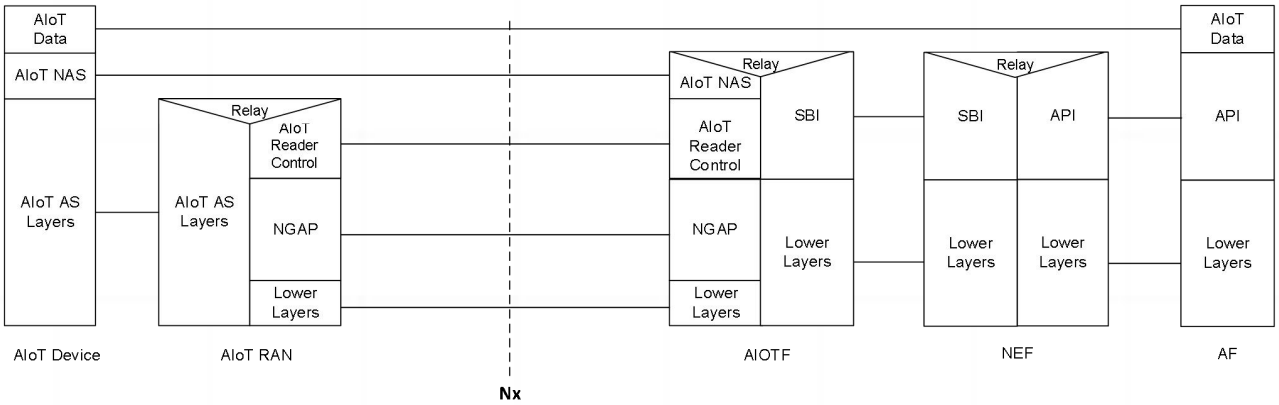

图 9：架构选项 1 协议栈

2.3.1.2 架构选项 2：AIOT RAN 通过 AMF 连接 AIOTF

架构选项 2 即 AIOT RAN 通过 AMF 连接 AIOTF 方式，如图 10 所示。

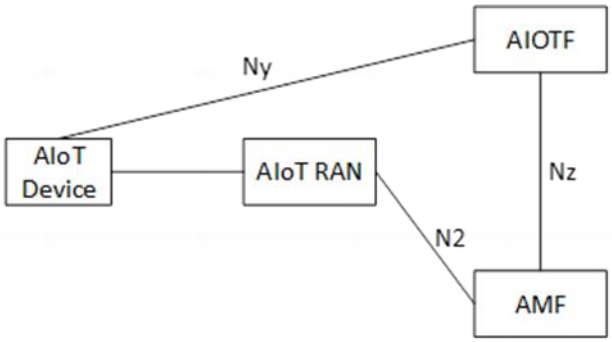

图 10：AIOT RAN 通过 AMF 连接 AIOTF

架构选项 2 相比于选项 1 的区别在于：AIOTF 和 AIOT RAN 之间的传输路径不是直连接口而是需要经过 AMF 的路由转发。

AIOT RAN 和 AMF 之间采用 N2 接口，支持 NG-AP 协议。AIOTF 和 AMF 之间采用服务化接口协议通信。

架构选项 2 的协议栈如图 11 所示。

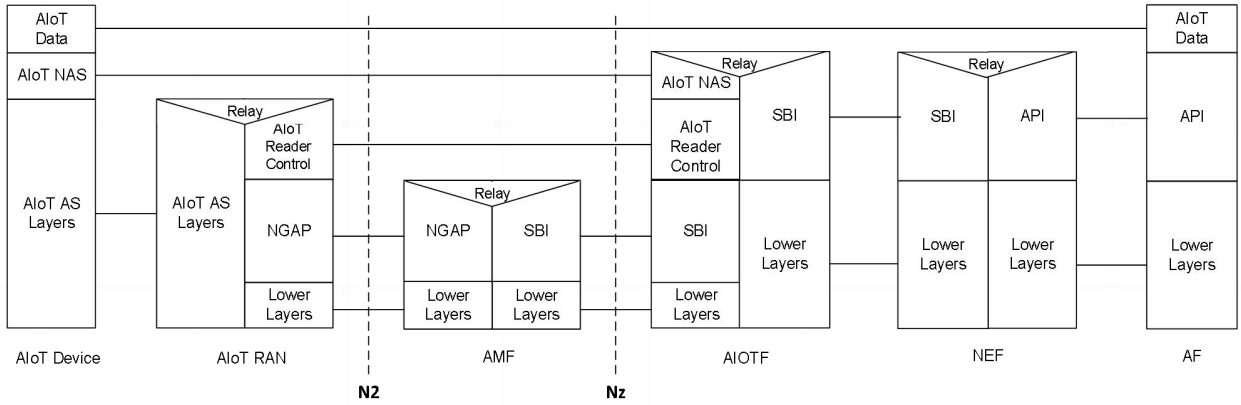

图 11：架构选项 2 协议栈

2.3.2 拓扑 2 的网络架构

支持拓扑 2 的 Ambient IoT 网络架构有两种选项：基于用户面的选项，和基于 RRC 的选项。

拓扑 2 中 UE 作为 AIoT Device 的读写器，对于 UE reader 的原则如下：

- 注册和授权方面：
  - UE reader 向 AMF 初始注册时，指示其可以作为 reader 的能力。
  - 在 UE 注册过程中，AMF 负责对 UE reader 进行授权，具体如下：
    - AMF 根据 UDM 中 UE 能力和签约数据授权 UE 是否可以作为 reader。
    - 当 UE 被授权作为 reader 时，AMF 指示 UE 被授权为 reader 并提供 UE reader 配置，可能包括：reader ID、允许作为 reader 的区域（可选），允许作为 reader 的时间（可选）。
  - AMF 根据 AIoTF 和 AMF 的服务区域为 UE 分配 TA 列表。
  - UDM 中 UE reader 的 UE 签约数据包括：允许 UE 作为 reader 的指示、允许作为 reader 的区域（可选），允许作为 reader 的时间（可选）等。
- UE reader 选择：
  - UE reader 选择支持基于给定的目标区域和给定的目标 UE reader。

2.3.2.1 基于用户面的选项

基于用户名的架构如图 12 所示，UE reader 使用 UE 和 UPF 之间的 IP PDU 会话作为传输，基于 AIoT 应用协议（AIoT-AP）连接到 AIoTF。相关协议栈如图 13 所示。AIoT AP 协议支持 AIoT 业务所需的交互过程和信息传输。

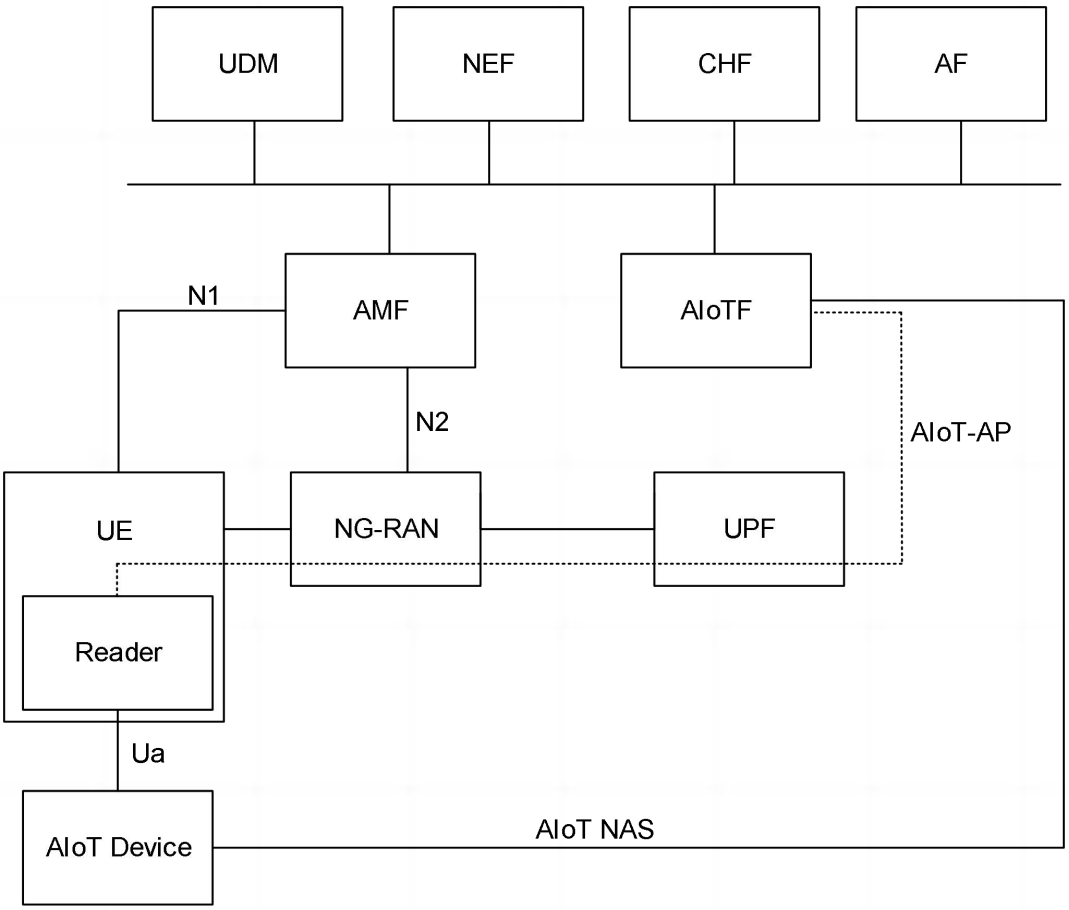

图 12：用户面架构

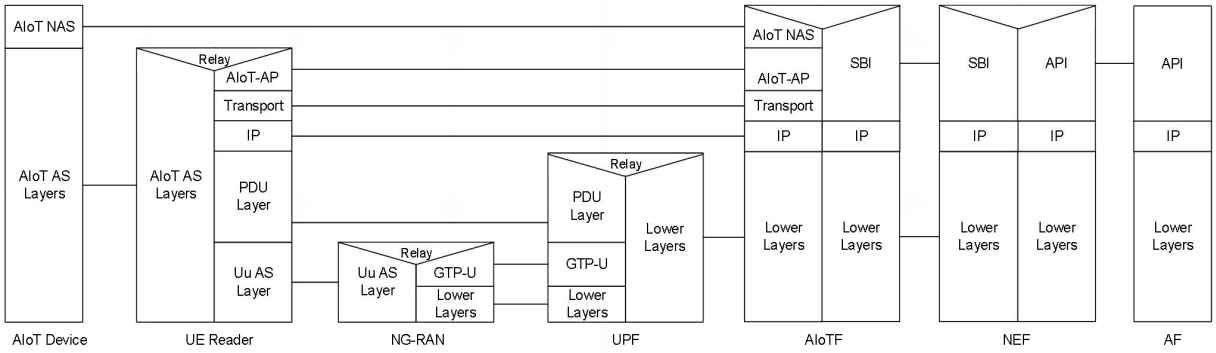

图 13：用户面架构协议栈

- UP 连接建立：
  - 网络为 UE 配置：AIoTF 的 FQDN，DNN/S-NSSAI 信息。
  - 使用专用 DNN 和/或基于 URSP 的 S-NSSAI 建立 PDU 会话。
- UE reader 选择方面:

- 一般原则如 2.3.2 节所述。
- AIoTF 负责 UE reader 选择。
- 对于给定的 UE reader，AIoTF 获取 AF 提供的目标 UE reader ID 或目标区域为 AIoT 操作执行 UE reader 选择。

- UE 与 AIoTF 的关联：
  - UE 请求 AIoTF 通过 UP 连接建立 UE 与 AIoTF 的关联。
  - 建立 UE 关联后，如果需要，通过 UP 连接向 UE 下发 AIoT 业务操作请求。
- 服务 UE 的 RAN 负责为 UE reader 分配资源。
- 计费信息收集：
  - AIoTF 负责 UE reader 的计费信息收集（例如，UE reader 的持续时间）。

2.3.2.2 基于 RRC 的选项

UE reader 和 AIoTF 之间的消息使用 UE 与 AIoT RAN 之间的 RRC 协议、AIoT RAN 与 AMF 之间的 NGAP 协议，以及 AMF 与 AIoTF 之间的 SBI 接口进行传输。相关协议栈如图 14 所示。

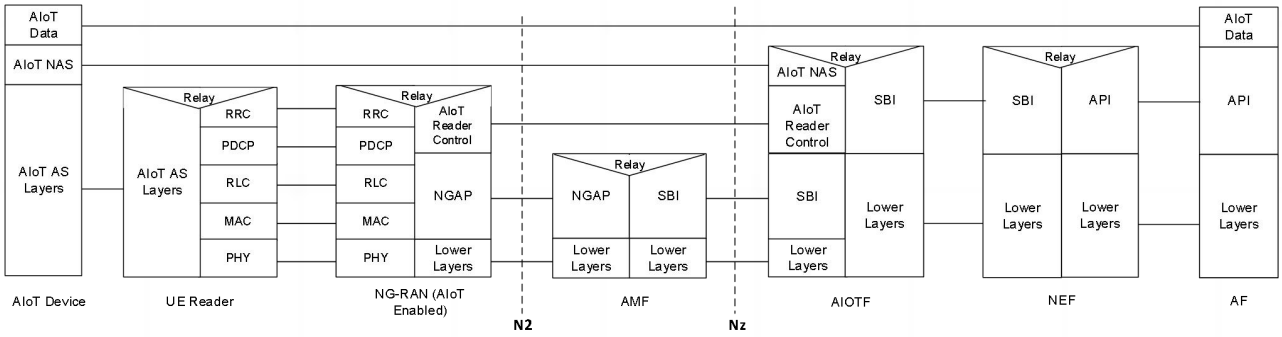

图 14：RRC 选项的协议栈

- AMF 与 AIoTF 之间的互操作：
  - AIoTF 通过 AMF 与 RAN 交互，AMF 为 AIoTF 提供 AIoT 服务操作接口。
- RAN 与 AMF 之间的互操作
  - RAN 与 AMF 之间的 NGAP 协议增强以支持 AIoT。
- UE reader 选择
  - 一般原则如 2.3.2 节所述。
  - 情形 1：AF 指示特定 UE reader 列表，AIoTF 向 RAN 提供特定的 reader 列表。
  - 情形 2：AF 提供给定的目标区域，AIoTF 负责第一轮 UE reader 选择并提供候选 reader 列表，RAN 可以从候选 reader 列表中进一步选择 UE reader。

- RAN 负责为 UE reader 分配资源。
- 计费信息收集：
  - UE 或 RAN 负责计费信息收集（例如 UE reader 持续时间）并报告给 AIoTF。

2.4 Ambient IoT 业务与流程

本章介绍根据业界需求所要支持的 Ambient IoT 业务，及其对于 5G 网络系统的功能要求；并给出 Ambient IoT 典型业务的相关流程。

2.4.1 Ambient IoT 业务

Ambient IoT 可支持室内、室外多种业务场景，按功能或应用可分为如下四类业务：

- 盘存：通过盘存特定区域，可发现区域内存在的物品，如纸箱、包装、工具等。该过程中，网络发起区域盘存请求，附着在物品上的 AIoT 设备响应，上报与该物品关联的标识 ID，同时可上报状态、测量结果和位置等信息。

- 传感数据收集：AIoT 设备与传感器关联，在某些情况下触发传感数据传输，如周期性上报、AIoT 设备有能量时上报或由网络触发的一次性上报。

- 资产跟踪：通过资产跟踪，可确定物品的位置。附着在物品上的 AIoT 设备上报与物品关联的 ID 标识和位置信息，该流程也可由支持 AIoT 的 UE 触发，以发现 UE 周围特定范围内的 AIoT 设备位置。

- 控制指令：AIoT 设备与控制器关联，传输控制指令，该流程通常由网络侧触发。

面向上述业务场景，5G 网络需支持的功能包括如下六个方面：

- 通信：5G 系统需支持 AIoT 设备（组）与 5G 网络和 UE 间通信，支持可信或授权第三方与 AIoT 设备（组）通信。

- 定位：5G 系统需支持 AIoT 设备位置服务，如绝对位置或相对位置。

- 管理：5G 系统需支持激活和去激活一个或多个 AIoT 设备。

- 信息收集和能力开放：基于用户许可、运营商策略和第三方请求，5G 系统需支持获取 AIoT 设备（组）的数据信息，通过 5G 网络将数据或设备（组）信息向可信第三方提供；支持授权的第三方激励特定区域的设备执行操作，如发送 ID、接收信息或发送测量值等。

- 计费：5G 系统需以 AIoT 设备或设备组为粒度收集计费信息。

- 安全与隐私：5G 系统需使能适用于 AIoT 的安全机制，该机制不影响传统 5G 系统的安全；5G 系统需提供隐私信息（如位置和 ID）在交互过程中的保护机制；基于签约和运营商策略，5G 系统需授权 UE 与特定 AIoT 设备或设备组通信。

在标准上，3GPP 首先规定的 Ambient IoT 业务操作包括：盘点(Inventory)、命令(Command)及具体的读(Read)、写(Write)和去激活(Disable)等操作。

2.4.2 Ambient IoT 业务保障 SLA

第三方企业可以和运营商协商确定 Ambient IoT 业务的服务范围。服务范围可以包括以下信息：

1) 允许请求的 Ambient IoT 业务位置区域

2) 允许请求的 Ambient IoT 业务类型（例如：盘存，读数据，写数据，去激活设备）

2.4.3 Ambient IoT 业务流程

Ambient IoT 关键业务包括 Inventory only、Command only 以及 Inventory and Command 等。对于不同的拓扑架构，流程略有不同；3GPP 对于这些业务流程的详细步骤还没有完全确定，本章基于拓扑 1 的架构选项 1 给出 Ambient IoT 业务流程示例。

2.4.3.1 拓扑 1 的业务流程

以 Inventory only 为示例的业务流程如图 15 所示。

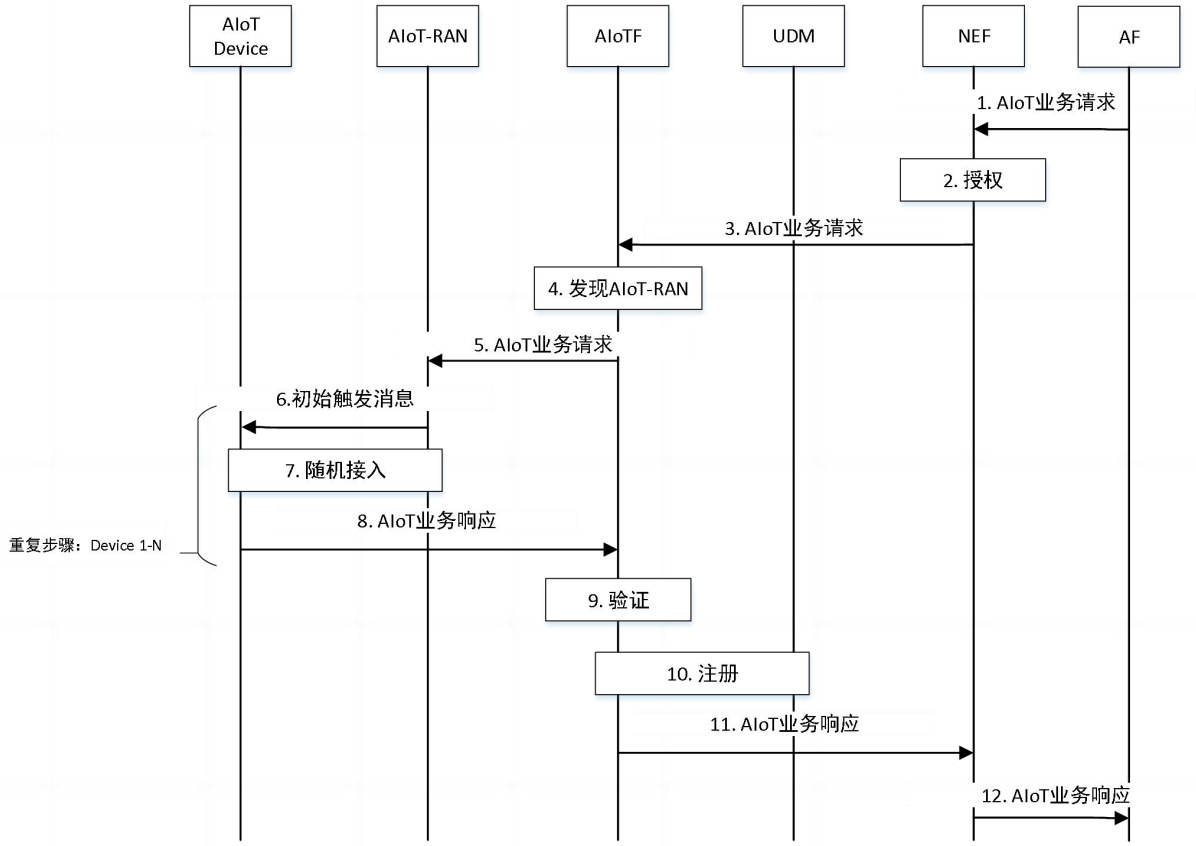

图 15：Inventory only 业务流程

Inventory only 业务流程具体步骤如下：

1、AF 向 NEF 发送 AIoT Service Request 业务请求消息，该消息中包含业务操作指示（Inventory only）、设备信息、区域信息等参数。

2、NEF 对 AF 请求进行授权，NEF 确定执行业务操作的 AIoTF。

3、NEF 向 AIoTF 发送 AIoT Service Request 消息，该消息中包含业务操作指示、设备信息、区域信息等参数。

4、AIoTF 确定执行业务操作的 AIoT-RAN。

5、AIoTF 向 AIoT-RAN 发送 AIoT Service Request 消息，该消息中包含业务操作指示、设备信息等参数。

6、AIoT-RAN 向 AIoT Device 发送 Initial Trigger Message 初始触发消息，该消息中包含设备信息；该步骤由 RAN 定义。

7、AIoT Device 发起 Random Access 随机接入过程；该步骤由 RAN 侧工作组定

义。

8、AIoT Device 通过 AIoT-RAN 向 AIoTF 发送 AIoT Service Response 业务响应消息；对于 Inventory only，该消息中包含 Device ID。

9、AIoTF 对 AIoT Device 进行验证和/或认证过程。

10、AIoTF 将 AIoT Device 的 Device ID 和区域信息 Register 注册到 UDM 中。

11-12、AIoTF 通过 NEF 向 AF 发送 AIoT Service Response 消息。

Command only 业务流程在 Inventory only 基础上，需进一步考虑安全和 NAS 消息封装等方面的因素。

Inventory and Command 业务流程如图 16 所示。

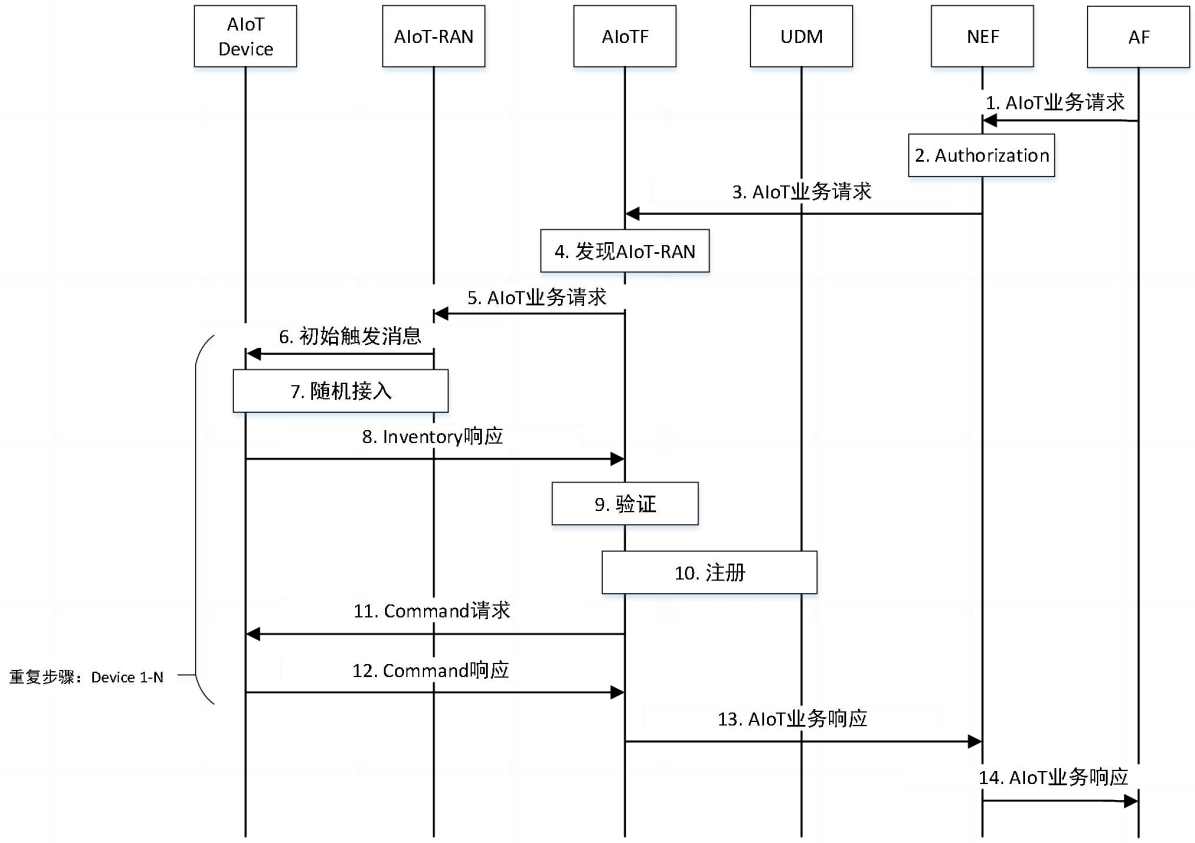

图 16：Inventory and Command 业务流程图

Inventory and Command 业务流程具体步骤如下：

1、AF 向 NEF 发送 AIoT Service Request 业务请求消息，该消息中包含业务操作指示（Inventory and Command）、设备信息、区域信息等参数。

2、NEF 对 AF 请求进行授权，NEF 确定执行业务操作的 AIoTF。

3、NEF 向 AIoTF 发送 AIoT Service Request 消息，该消息中包含业务操作指示（Inventory and Command）、设备信息、区域信息等参数。

4、AIoTF 确定执行业务操作的 AIoT-RAN。

5、AIoTF 向 AIoT-RAN 发送 AIoT Service Request 消息，该消息中包含业务操作指示（Inventory and Command）、设备信息等参数。

6、AIoT-RAN 向 AIoT Device 发送 Initial Trigger Message 初始触发消息，该消息中包含设备信息；该步骤由 RAN 定义。

7、AIoT Device 发起 Random Access 随机接入过程；该步骤由 RAN 定义。

8、AIoT Device 通过 AIoT-RAN 向 AIoTF 发送 AIoT Service Response 业务响应消息，该消息中包含 Device ID。

9、AIoTF 对 AIoT Device 进行验证和/或认证过程。

10、AIoTF 将 AIoT Device 的 Device ID 和区域信息 Register 注册到 UDM 中。

11、AIoTF 通过 AIoT-RAN 向 AIoT Device 发送 Command Request 请求消息。

12、AIoT Device 通过 AIoT-RAN 向 AIoTF 发送 Command Response 响应消息，该消息中包含 Command 执行结果。

13-14、AIoTF 通过 NEF 向 AF 发送 AIoT Service Response 业务响应消息。

2.4.3.2 拓扑 2 的业务流程

拓扑 2 的业务流程与拓扑 1 类似，不同之处在于 AIoTF 与 UE reader 之间消息传输的路径。

对于拓扑 2 的基于用户面选项，AIoTF 与 UE reader 之间的消息通过 UE 建立的与 UPF 之间的 PDU 会话用户面路径传输。

对于拓扑 2 的基于 RRC 选项，AIoTF 与 UE reader 之间的消息由 AMF 和 AIoT RAN 经控制面路径转发。

2.5 Ambient IoT 安全

Ambient IoT 业务潜在的安全风险包括仿冒攻击、命令数据篡改、命令数据窃听等。例如，攻击者仿冒受害者 Ambient IoT 设备，上报虚假结果，影响盘存结果。再如，攻击者修改写指令中待写入 Ambient IoT 设备的数据，导致 Ambient IoT 设备存储被篡改的数据。本章针对这些安全风险，从运营商角度给出解决方案，包括对 Ambient IoT 设备的认证，Ambient IoT 业务数据的安全传输等；这些方案需要在标准化组织进一步研究和讨论，成为 Ambient IoT 规范系列中的重要组成部分。

为解决上述潜在安全风险，Ambient IoT 业务可以由运营商提供安全服务。Ambient IoT 业务由核心网网元作为安全端点，核心网网元对设备进行认证，并建立设备和核心网网元之间的安全传输通道，用于传输命令数据。在这种模式下，设备和 Ambient IoT Reader 间无需进行安全保护。

为实现上述功能，Ambient IoT 设备预配置来自运营商的安全参数（如长期密钥）。由于 5G-AKA 算法复杂度高（如需要管理和维护 SQN），无法直接应用于 Ambient IoT 设备中。为减少 Ambient IoT 设备上的存储开销，网络设备通过下行消息向 Ambient IoT 设备发送挑战值，Ambient IoT 设备基于长期密钥和挑战值计算认证响应，并通过上行消息发送给网络设备进行校验。校验成功则表示网络设备对 Ambient IoT 设备认证成功，反之则认证失败。

在对 Ambient IoT 设备认证成功的情况下，在盘存业务中，网络设备向服务请求方发送 Ambient IoT 设备信息；在命令业务中，网络设备基于长期密钥计算会话密钥，并对命令数据进行机密性和/或完整性保护，并将安全保护后的数据通过下行消息发送给 Ambient IoT 设备。对应的，网络设备基于长期密钥计算会话密钥，并对收到的数据进行解密或完整性校验。示例性的，在命令业务为读时，网络设备对“读”命令进行机密性和/或完整性保护，并发送给 Ambient IoT 设备。Ambient IoT 设备进行解密或完整性校验，对待上报的数据进行机密性和/或完整性保护，并通过上行消息发送给网络设备。对应的，网络设备对收到的数据进行解密或完整性校验，获得最终的业务数据。

第三章　总结与展望

本研究报告首先介绍了 Ambient IoT 的应用场景，包括物流、仓储、交通和智慧城市等多个方面；针对这些业务场景，分析了在标准上已经达成共识的四种拓扑形态；并介绍了国内外标准组织对 Ambient IoT 的研究进展以及主要成果。Ambient IoT 的关键技术方面，分析了设备标识的设计与使用，对 Ambient IoT 设备的管理；对于支持 Ambient IoT 的网络架构，分别针对拓扑 1 和拓扑 2 两种形态给出它们的对应架构和协议栈；然后对需要支持的 Ambient IoT 的业务类别，包括盘点(Inventory)、命令(Command)及具体的读、写等操作和相关的业务流程进行介绍；最后对 Ambient IoT 安全方面的需求和方案进行分析，包括对设备和读写器的认证和授权，业务流程中的数据安全等。

Ambient IoT 依托产业的广泛需求，在技术和标准化方面进展迅速并仍在进一步完善中。Ambient IoT 涉及的核心网关键技术对基本的网络架构和业务流程已经完成初步研究，后续将对这些关键技术进行标准化的工作。另外在 Ambient IoT 安全、读写器授权与选择机制等方面进行完善；同时也将对拓扑形态和对应网络架构方面做进一步研究，拓展无源物联网的应用场景。随着标准的成熟，基于蜂窝网络的 Ambient IoT 作为一种在技术和成本上优势明显的物联网通讯方式，未来将呈现快速增长的趋势，在各行各业得到广泛的应用。

缩略语简表

英文缩写	英文全称	中文解释
AIoT	Ambient Internet of Things	无源物联网
AIoTF	Ambient IoT Function	无源物联网功能
IAB	Integrated Access and Backhaul	融合接入与回传
RFID	Radio-Frequency Identification	射频识别
ID	Identification	标识
RAN	Radio Access Network	无线接入网
RRC	Radio Resource Control	无线资源控制
AP	Application Protocol	应用协议
AF	Application Function	应用功能

参考文献

[1] 3GPP TR 22.840: “Study on Ambient power-enabled Internet of Things”

[2] 3GPP TS 22.369: “Service requirements for ambient power-enabled IoT”

[3] 3GPP TR 38.848: “Study on Ambient IoT (Internet of Things) in RAN”

[4] 3GPP TR 38.769: “Study on solutions for ambient IoT (Internet of Things)”

[5] 3GPP TR 23.700-13: “Study on Architecture support of Ambient power-enabled Internet of Things”

[6] ITU SG20-TD1510 YSTR.Ambient-IoT: “Analysis on requirements and use cases of ambient power-enabled IoT”

[7] CCSA:《基于蜂窝通信的无源物联网应用需求研究》，B-202103220391

[8] CCSA:《支持无源物联网的核心网架构及增强技术研究》，B-202404151435

[9] CCSA:《基于蜂窝通信技术的无源物联服务 第 1 部分：应用场景及需求》，H-202207224229

[10]CCSA:《基于蜂窝通信技术的无源物联服务 第 2 部分：总体技术要求》，H-202302286187

[11]《面向万物互联的无源物联网技术》，无源物联网技术联合创新中心，2022

主要贡献单位


ZTE


HUAWEI


vivo


中信科移动
CICT Mobile


中国移动
China Mobile


ERICSSON

IMT-2020（5G）推进组

地址：北京市海淀区花园北路 52 号 中国信息通信研究院

邮编：100191

邮箱：imt2020@caict.ac.cn

网址：https://www.imt2020.org.cn/