



物联网云平台终端远程更新技术研究与应用

魏民, 王艺

(中国电信股份有限公司上海研究院, 上海 200122)

摘要: 物联网终端远程更新是支持其迭代式优化、规模化部署和低成本维护的基础。分析了物联网终端远程更新现状与统一管理控制需求间的矛盾, 基于 LWM2M 协议提出了物联网终端远程升级技术解决方案, 探讨物联网云平台对异构式操作系统、多形态终端远程更新的统一管理和控制, 降低了终端规模升级对网络冲击, 提高远程更新的通用性、可靠性和稳定性。

关键词: 物联网云平台; IoT 终端远程更新; 统一管理控制

中图分类号: TP319

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018273

Research and application of remote update technology of IoT terminal

WEI Min, WANG Yi

Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: Remote updating of IoT terminal is the basis of supporting its iterative optimization, large-scale deployment and low-cost maintenance. The contradiction between the present status of remote updating of IoT terminals and the requirement of unified management and control was analyzed. Based on LWM2M protocol, a solution of remote updating of IoT terminals was proposed. In this solution, IoT platform provides the unified management and control of IoT terminals with heterogeneous operating systems and multi-model terminals, which helps reducing the impact of terminal scale updating on the network and improving the generality, reliability and stability of remote updating.

Key words: IoT cloud platform, remote updating of IoT terminal, unified management and control

1 引言

随着物联网技术发展、应用的深入, 物联网云平台 (IoT 平台) 价值逐渐显现。降低终端接入的难度和维护成本是 IoT 平台服务的基础, 当物联网云平台接入的终端投入实际环境运行后, 用户对终端的远程更新需求日益迫切^[1]。物联网终

端一旦部署, 将会运行相当长的时间, 而物联网市场正处于迅速变化、快速发展的阶段, 新兴技术和持续创新需求不断涌现。终端设备厂商在不更改硬件的情况下, 通过终端固件和软件的在线更新以完成最新功能的部署, 实现终端固件完善、软件功能增强。另外, 人们在享受万物互联带来便利的同时, 物联网终端的安全问题逐渐暴露。只有持



续、完备的终端更新机制，才能确保新出现的安全漏洞能够及时得到修复^[2]。传统人工现场对终端更新的方式需要大量的人力、物力，很多应用场景由于地理环境限制（如环境监测、战场感知等）无法实现终端的近场更新，所以终端的远程更新功能是物联网云平台必不可少的组成部分。

物联网云平台接入的终端具有数量多、差异大、分布区域广、环境条件复杂等特点，同时由于低带宽、高时延和终端资源受限等因素，物联网云平台实现远程更新功能面临许多挑战。

（1）升级的速度和效率

在低带宽、高时延、资源受限的环境下，云平台面临着传输效率低、终端更新时间长的问题。升级包传输效率低、传输时间长，传输过程中容易出现分组丢失现象。终端更新时间太长，不仅增加终端功耗，而且对需要长时间稳定工作的终端也是个极大的不利因素。

（2）多任务、多设备同时升级

IoT 平台的远程升级服务应能执行多个任务，对不同需求的多个终端同时执行远程更新的管理和控制，提高云平台的服务效率。另外 IoT 平台需要解决大规模、高并发远程更新操作对无线资源造成的阻塞和冲击，避免对正常业务造成影响。

（3）远程更新服务的标准化和通用性

IoT 平台虽然接入终端种类多，差异大，但提供的远程更新功能和服务必须统一、通用，这样才能降低终端接入难度以及用户自服务、自管理的门槛，实现规模服务的目标。但目前远程更新领域没有一个统一的升级规范或者架构，多种更新机制、服务流程和通信协议并存，所以 IoT 平台面临终端远程更新技术解决方案通用性和终端异构间的兼容性问题。

2 终端更新现状与目标

终端更新技术发展与物联网终端部署应用场景紧密相关。传统物联网终端成本较高，主要应

用于专业垂直领域，以局域网近场通信为主，垂直领域的专业流程决定了当时场景下终端更新技术和机制是专业化和定制化的。近几年，终端成本降低、低功耗广域通信技术成熟，促进了物联网终端设备在白色家电、环境监测等公共事业领域的规模应用，同时激发了市场对“万众创新、万物互联”的期盼，IoT 平台应运而生，但目前 IoT 平台尚处于起步阶段。

IoT 平台接入的终端来自不同终端厂商、应用于不同领域，一些芯片或模组厂商基于自身在移动互联网终端市场的经验为生产的物联网终端提供私有化的远程更新方案，终端侧内置有配套的远程更新模块。这些远程更新方案缺乏对物联网低带宽、高时延、低功耗等特性的考量，从 IoT 平台远程更新服务角度存在以下问题：用户自服务自管理门槛高，不统一、不通用；端云交互协议私有化，缺乏在低带宽、高时延、资源受限场景下传输效率、可靠性方面的设计；远程更新方案相对封闭，只能为自己的终端提供远程更新服务。

终端远程更新技术中，升级包或镜像文件生成和大小也直接影响着技术方案的可行性。即使是很小的客户端 footprint 变化都需要一个很大的更新文件，这大大增加了带宽成本和更新时间。除此之外，大量连网设备都有 Flash 和 RAM 受限的问题，如汽车中的电子控制单元。为了更好地解决这个问题，当前最成熟也最普遍的解决方案是使用差分分组（delta）升级方案。用差分分组升级时只会生成新旧两个版本间的差异部分。根据第三方供应商的检测，某 FOTA 厂商的差分分组文件比全镜像文件小 97%，并且只需全镜像文件升级 8% 的时间就能完成全部更新。目前差分服务一般由独立于终端设备厂商之外的第三方差分服务商为客户提供更新分组的差分制作和管理。

基于物联网云平台远程更新所面临的挑战和终端更新技术的现状，IoT 平台远程更新方案目标

和设计思路如下。

(1) 时间短、效率高

IoT 平台应尽可能地减少远程升级的时间,提高升级效率。第一,通过控制升级包的大小,采用差分分组处理来降低升级包的体积,减少远程网络传输时间,提高更新升级速度。第二,通过模块内升级提高升级的灵活度,降低升级的时间。第三,增加断点续传功能,避免终端故障或通信中断造成的数据重传,减少数据传输时间,提升远程更新的速度。

(2) 合理使用无线资源,提升终端更新的服务效率

为了提高 IoT 平台的服务效率,终端远程更新服务应能实现多任务的并发,一个任务对应一次远程更新计划,包含一组待更新的远程终端。同时为了保障同一无线小区下其他终端业务的正常使用,IoT 平台应对同一小区下的终端更新操作数量进行限制。

(3) 高可靠性

高可靠性是为了保障终端更新的效率。第一,远程更新的管理和控制要精细、准确、智能。IoT 平台应根据具体终端状态进行有效性检查后(如版本、文件类型、升级包大小等),再触发终端远程更新流程。第二,远程更新过程中通过状态机机制引入、实施、控制和异常处理,保障端云间控制的协同,降低远程更新操作的风险。第三,远程升级过程中,升级包数据可能出错或丢失,升级包的校验机制保证了升级包的完整性,传输协议保证数据传输的可靠性,IoT 平台的重试策略保证传输和升级过程的稳定性。

(4) 通用性

通用性是指 IoT 平台接入的不同领域、不同种类的异构终端使用相同的终端更新流程。这样可以最大限度降低终端远程更新的维护成本,实现用户的自服务、自管理以及对异构终端规模化更新的目标。第一,终端远程更新方案中需要做

到控制流和业务流的分离,控制流与终端具体的环境和类型无关。第二,控制流采用标准、开放的国际标准协议承载,保证技术方案的可实施性。第三,兼容升级包和业务流的个性化,支持第三方差分服务商差分服务。

3 物联网远程更新解决方案

3.1 系统结构

物联网云平台远程更新系统结构如图 1 所示,由服务端和终端两部分组成。

远程更新服务端为 IoT 平台的一个功能模块,主要实现用户自服务和远程更新的管理控制功能。用户自服务是支持用户通过门户方式进行远程更新任务制定和远程更新状态的查询。任务制定设置的内容包括更新版本、升级包、待升级终端组和更新策略等;远程更新管理控制包括远程更新的触发、升级包下载和安装控制以及下载和安装失败时的策略执行控制。

升级包生成和下载服务支持两种方式。一种是 IoT 平台为待升级终端提供下载服务,这种方式是用户通过门户上传升级包,IoT 平台负责升级包的管理;另一种是第三方差分服务商提供差分分组的生成和下载服务,在这种方式下,用户在任务制定时需要选择第三方差分服务器的访问地址。上述下载服务云和端侧必须同时支持断点续传功能。

远程更新对终端的要求为终端根据服务端的指示进行升级包的下载、安装以及下载和安装操作结果的上报。终端下载应支持下载、断点续传功能和升级包的校验功能。终端安装应支持安装和容错功能,容错是指终端在安装阶段对故障的隔离和处理,以确保安装失败时不影响终端的正常运行。

3.2 服务流程

远程更新服务流程包括任务制定、更新触发、升级包下载和安装 4 个阶段,如图 2 所示。

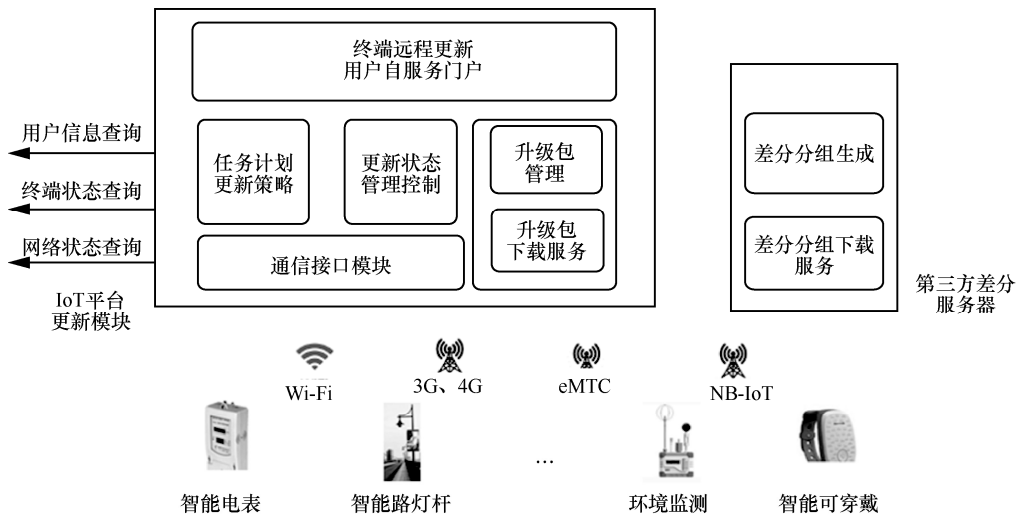


图1 远程更新系统结构示意图

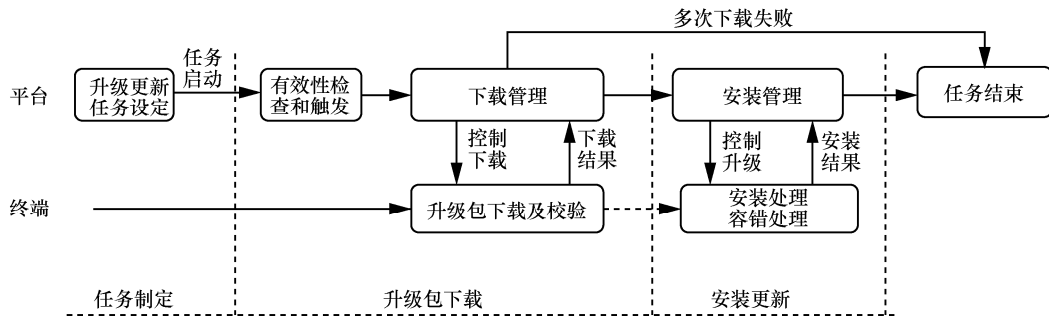


图2 远程更新服务流程示意图

(1) 任务制定

用户通过物联网云平台自服务门户制定更新任务计划。包括：待更新终端组、目标版本、下载和安装失败后的重试策略、升级包生成和下载的方式。

(2) 更新触发

为了保证更新的有效性，在触发更新之前，服务端对任务计划进行有效性检查。检查内容包括设备厂商、型号、目标版本、升级包文件类型等。另外，服务端结合终端状态、网络状态、同一无线小区下正在下载终端的并发数来决定任务的触发时间点。服务端通过向终端配置下载 URI 触发终端更新流程。

(3) 升级包下载

升级包下载是终端从下载服务器获得升级包。若用户选择 IoT 平台的下载服务，服务端下

发的 URI 地址为 IoT 平台下载服务器地址。若用户选择第三方差分服务，服务端下发的 URI 地址为第三方差分服务器地址。

(4) 升级包安装

终端升级包下载完成后，向服务端上报下载的结果。若下载成功，服务端指示终端进行安装更新操作，终端执行完安装程序后，将安装结果上报服务端。

当服务端收到终端上报结果为下载失败或安装失败，服务端应根据具体的失败原因进行重试或结束更新流程。

3.3 端云交互协议

服务端和终端之间交互包含控制信息（控制流）和业务信息（业务流）。为了实现异构终端的统一管理，技术方案采用了控制流和业务流相分离

的方式, 管理控制流与终端的类型和运行环境无关, 这样可以标准化、规范化。业务流和升级包则依赖于终端具体的运行环境, 这样可以兼容设备间的异构性, 保留原有的协议和文件方式。

管理控制协议采用 OMA (Open Mobile Alliance) 组织定义的 LWM2M (lightweight machine to machine) 国际标准, LWM2M 协议为应用层协议, 底层基于 CoAP/UDP 传输, DTLS (datagram transport layer security) 加密, 非常适用于网络和资源受限的终端^[3-5]。LWM2M 协议主要实现终端远程更新流程中服务端和终端之间的管理控制。管理控制状态机如图 3 所示。

整个升级流程状态转换机包含 IDLE、DOWNLOADING、DOWNLOADED、UPDATING 4 个状态。终端使用 LWM2M Object5 来和平台交互实现整个升级过程的管控。

步骤 1 IoT 平台使用 LWM2M CREATE 原语在终端上创建 Object5。

步骤 2 IoT 平台使用 LWM2M WRITE 原语向终端写入升级 URI。

步骤 3 终端使用升级 URI 下载升级差分分组。

步骤 4 IoT 平台使用 LWM2M EXECUTE 原语指示终端开始升级。

步骤 5 终端进行本地升级安装。

步骤 6 终端升级完成后重启, 向 IoT 平台报告升级结果。

其中, IoT 平台在创建 Object5 之后, 对 Object Instance 5/0 执行 Observe 操作。这样之后, 终端在升级过程中关于 State 和 Result 两个 Resource 的任何状态变化都可以上报到 IoT 平台。

终端远程更新直接影响终端的安全性和稳定性, 因此方案安全性要求比较高, 尤其是更新分组的安全性。更新分组的上传和下载必须采用签名和校验机制, 更新分组下载传输采用 TLS 或 DTLS 通道加密机制或者采用网络隔离方案。

4 需要进一步考虑的问题

在上述基本升级控制流程实现外, 尚有其他问题需要进一步分析和解决, 主要包括以下。

(1) 批量终端升级的离散化处理

连入网络的物联网终端数量会越来越多。达到一定程度后, 如果不加控制地在一个小区内同时进行大量差分分组的下载, 很可能导致

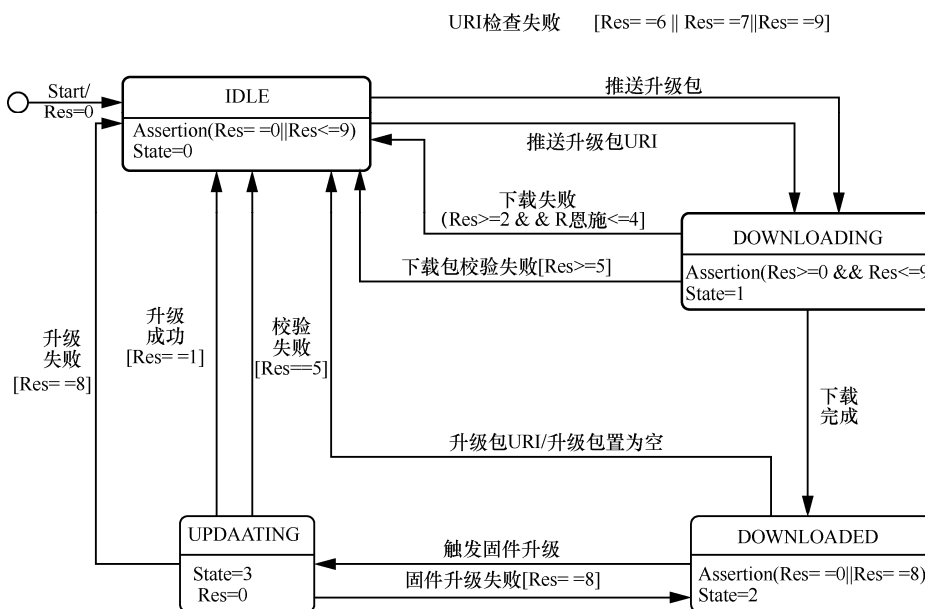


图3 LWM2M 远程更新状态机转换图



网络传输的拥塞。尤其在 NB-IoT 网络下, 问题更为突出。

因此, 有必要进行批量终端升级的离散化处理。核心的做法是根据终端所在 cell ID 来区分终端的位置, 对于同一 cell ID 下同时进行升级的终端数量进行控制。由于 NB-IoT 终端的移动性相对较弱, 因此上述做法是基本可行的。

(2) 模块升级和 MCU 软件升级

模块升级是指在终端块内完成终端软件升级。目前很多模块本身已经考虑了软件升级。

MCU 软件升级指的是使用通信模块的终端本身还有一块运行在 MCU 所运行的操作系统上的终端应用软件 (也可包含 OS 原件)。MCU 软件升级的一种做法是终端开发商自行实现全部的下载、本地升级和升级流程控制; 另外一种做法则是利用模块已有的差分软件升级能力去下载目标软件, 通过模块接口将软件传递给 MCU, MCU 再进行本地安装升级。这里的目标软件可以是全量软件, 也可以是差分分组。如果是后者, 终端开发商仍然需要在终端上加载差分软件厂商提供的本地 Agent 进行相应的差分升级处理。

(3) 升级协议的选择

LTE 环境下, HTTP 使用较多。行业尤其看重其在升级控制指令的传输稳定性。目前的通信模块处理能力实际上都比较强, 使用 HTTP 本身没有任何问题。在信号较好的情况下, HTTP 的传输效率也是不错的。在 NB-IoT 网络中, 终端根据 RSRP 门限确定覆盖增强等级 CE Level, 根据 CE Level 确定其对应的 NPRACH 资源和重复次数, NB-IoT 通过重复发送达到覆盖增强效果, 重复次数越多, 终端速率越低。在某些情况下, TCP 的使用是否能提高下载的传输效率有待验证。也有一些模块厂商在标准下载协议之外, 实现了私有的基于 UDP 的下载协议, 力图实现较高的下载传输速率。

5 结束语

本文针对物联网终端数量多、差异大、分布区域广、环境条件复杂等特点, 提出了 IoT 平台终端远程更新技术解决方案。技术方案采用了控制流和业务流相分离思路, 控制流相对独立、通用, 基于开放、标准的 LWM2M 协议制定了通用的服务流程, 实现了不同领域、不同类型终端的统一管理和控制, 同时保留了业务流和升级包的个性化, 与现有物联网终端千差万别的开发运行环境相兼容。

物联网云平台远程更新技术方案降低了物联网终端的维护成本, 满足终端迭代式优化、规模化部署的需求, 降低了终端规模升级对网络的冲击, 提高了远程更新的通用性、可靠性和稳定性。

参考文献:

- [1] 彭昭. 物联网使能平台的体系结构与服务模式[J]. 电信科学, 2017, 33(11): 141-145.
PENG Z. Architecture and service model of IoT enabled platform[J]. Telecommunications Science, 2017, 33(11): 141-145.
- [2] 侯玉华, 周晓龙. 智能终端操作系统安全问题及解决方案[J]. 电信科学, 2015, 31(3): 8-12.
HOU Y H, ZHOU X L. Security problems and solutions of smart terminal mobile operating system[J]. Telecommunications Science, 2015, 31(3): 8-12.
- [3] OMA. LWM2M:OMA-TS-LightweightM2M-V1_0-20180209-A[S]. 2018.
- [4] OMA. LWM2M:OMA-TS-LightweightM2M_Transport-V1_1-20180710-A[S]. 2018.
- [5] OMA. LWM2M:OMA-TS-LWM2M_SwMgmt-V1_0-20180301-A[S]. 2018.

[作者简介]



魏民 (1970-), 女, 中国电信股份有限公司上海研究院高级工程师, 主要研究方向为物联网。

王艺 (1973-), 男, 中国电信股份有限公司上海研究院高级工程师, 主要研究方向为物联网。