

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1368

(01/2021)

X系列：数据网、开放系统通信和安全性
安全应用和服务（2）– 物联网（IoT）安全

物联网设备的安全固件或软件更新

ITU-T X.1368建议书

ITU-T



ITU-T X系列建议书
数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务 (1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议 (1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务 (2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网 (IoT) 安全	X.1360–X.1369
智能交通系统 (ITS) 安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议 (2)	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G安全	X.1800–X.1819

ITU-T X.1368建议书

物联网设备的安全固件或软件更新

概要

ITU-T X.1368建议书规定：1) 安全更新物联网（IoT）设备固件或软件（FW/SW）的基本模型和程序；2) 更新物联网固件的要求和能力。

本建议书规定通用的安全更新程序及一般要求。该程序方便在物联网环境中的利益攸关方（如物联网设备开发商和物联网系统/服务提供商）之间安全地实施通用物联网软件/固件更新。

本建议书侧重于更新固件，但也适用于更新物联网设备的任何其他软件。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1368	2021-01-07	17	11.1002/1000/14445

关键词

物联网（IoT）；安全；软件更新。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL <http://handle.itu.int/>，随后输入建议书的唯一ID，例如，<http://handle.itu.int/11.1002/1000/11830-en>。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2021

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
3.1	它处定义的术语	1
3.2	本建议书定义的术语	1
4	缩写词和首字母缩略语	1
5	惯例	2
6	基本模型	2
7	更新程序	2
8	部署情形	3
8.1	IoT设备内的功能实体	3
8.2	状态跟踪器部署类型	4
9	发现可用的新固件图像并启动程序	6
10	要求	6
11	能力	7
11.1	固件消费者的能力	7
11.2	状态跟踪器的能力	7
11.3	固件服务器的能力	8
11.4	作者的能力	8
附录I	– ITU-T外的相关活动	9
附录II	– 使用分布式账本技术的物联网软件更新情景示例	10
II.1	概况	10
II.2	软件更新程序	10
参考资料	12

引言

针对物联网（IoT）设备或系统的网络攻击正变得日益复杂、智能和多样化。在此之前，大多数物联网设备的功能是由物联网设备供应商在其初始发布阶段固定的。然而，最近，设备连接到互联网以提供一系列增强的物联网服务，因此，使用中的物联网设备面临着网络威胁或攻击。人们有必要认识到，物联网设备中实施的固件蓝天软件（FW/SW）需要安全更新，以修复其漏洞和弱点。一些设备供应商已经开始通过他们自己的方案提供固件更新服务。

本建议提供物联网软件/固件安全更新的基本模型和程序，以及相关要求和能力。通过基本模型和通用更新程序，物联网软件/固件可以在物联网环境中的利益攸关方之间安全地交换，并鼓励利益攸关方更新过时的物联网软件/固件。

物联网设备的安全固件或软件更新

1 范围

本建议书规定安全更新物联网设备固件或软件（FW/SW）的基本模型和程序。建议书还描述物联网固件/软件更新的要求和能力。本建议书侧重于更新固件，但也适用于更新物联网设备的任何其他软件。

2 参考文献

无。

3 定义

3.1 它处定义的术语

无。

3.2 本建议书定义的术语

本建议书定义了下列术语：

- 3.2.1 作者：**为物联网设备制作固件（FW）图像和软件的实体，示例包括个人或团体，如公司或任何其他类型的组织。作者可能会将图像上传到一个或多个不一定受信任的固件服务器。
- 3.2.2 固件消费者：**在物联网设备上存储、验证和运行固件（FW）图像的任何实体。它应该决定是否运行当前的固件图像。物联网设备有一个或多个固件消费者。
- 3.2.3 固件服务器：**分发固件图像的实体。它可以接受来自多个作者的固件（FW）图像；它可以是特定供应商的存储库，也可以是接受不同供应商的存储库。理想情况下，FW服务器是可信的，但也可能是不可信的；它可以尝试查看或修改从作者那里收到的固件包。
- 3.2.4 清单（Manifest）：**包含固件图元数据的记录。
- 3.2.5 状态追踪器：**一个实体，负责检查并保存一个或多个固件消费者内的固件（FW）图像状态标签，并根据需要启动固件更新。这包括对设备变化的精细监控，例如运行的固件图像版本和设备当前所处的固件更新周期状态。状态追踪器可以位于物联网设备内部、内联网或互联网上。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

DLT	分布式账本技术
FW	固件
IoT	物联网

SW 软件

URL 统一资源定位符

5 惯例

本建议遵循以下与[b-IETF RFC 2119]一致的惯例。

- “须（Shall）” 该词意指：该定义是本规范的一个绝对要求。
- “不得（Shall not）” 该短语意指：该定义是本规范绝对禁止的。
- “应（Should）” 该词意指：在特定环境中有可能存在正当的理由对特定项不予理会，但是，在选择不同的做法之前，应充分理解全部含义和小心权衡理由。
- “应不（Should not）” 该短语意指：在特定环境中有可能存在正当的理由表明特定行为是可以接受的或者甚至是有益的，但用户应了解由此产生的所有影响，并在实施此短语描述的任何行为之前，进行仔细权衡。
- “可（May）” 该词意指：某一项内容是真正可选的。一家厂商可能会因为特定市场需求或因为该项内容能够提高产品的水平等原因而加以使用，而另一家厂商则能忽略不用。

6 基本模型

物联网设备的组网架构各不相同，但在所有情况下都应使用四个功能实体，即 FW-消费者（见第3.2.2节）、状态跟踪器（见第3.2.5节）、作者（见第3.2.1节）和 FW-服务器（见第3.2.3节）。其定义见第3.2段。请注意，多个功能实体可驻留于一个节点中。例如，网络摄像头设备包含多个 FW 消费者和一个状态跟踪器，而网络服务器则包含一个状态跟踪器和一个 FW 服务器。多个 FW 消费者可驻留于一个网络中，并由在网关中实施的状态跟踪器监控。根据物联网设备的限制程度，此类设计可能会有所不同。第8节描述典型的部署模型。

在基本模型中，这些实体在更新物联网SW/FW中扮演着不可或缺的角色。该模型中的基本情形很简单：识别物联网软件/固件更新需求的状态跟踪器启动软件/固件更新程序，该程序方便固件消费者通过固件服务器从作者处接收软件/固件图像。

7 更新程序

图1描述更新固件的基本程序。在启动固件更新程序之前，作者需要向固件服务器上传新的固件图像。图像最好附有数字签名，并由作者加密。

当状态跟踪器接收到用其位置[例如，其统一资源定位符（URL）]更新固件图像的请求时，即会验证该请求，然后，如果请求有效，则通过与固件消费者通信来检查固件的状态，以便确认固件更新的必要性。第9节列出发送此类请求的一些典型方式。

如果确认需要更新固件，则固件消费者通过通知可用固件的位置来启动固件更新。然后，固件消费者向固件服务器提出有关更新的固件图像请求。如果固件消费者拥有接收更新的合法权利，则固件服务器会向固件消费者提供固件图像。否则，服务器会发送带有错误代码的更新消息。

在接收到更新消息时，固件消费者对图像进行验证。如果没有发现错误，则固件消费者安装固件并将状态信息发送给状态跟踪器。请注意，上述四个功能实体的基数是多对多的，即多个状态跟踪器可与多个FW消费者通信，FW消费者可与多个FW服务器通信，FW服务器可与多个作者通信。

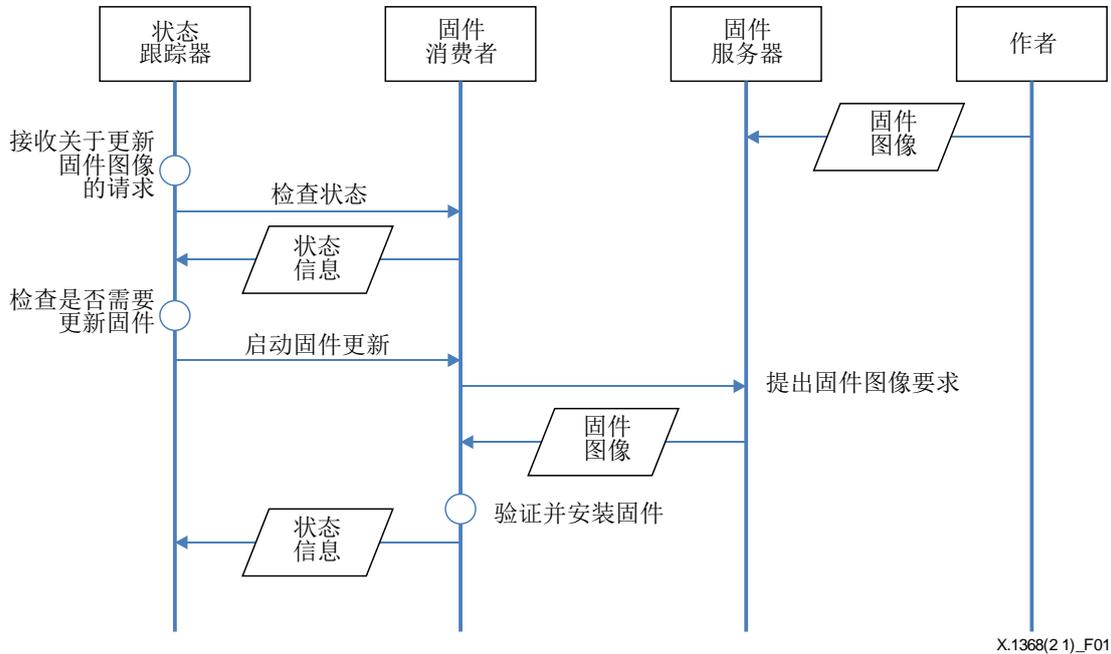


图1 – 协议程序

8 部署情形

如第6节所述，多个功能实体可位于一个节点内，多个实体可作为一个功能实体运行；部署情形可能因情况而异。本节具体说明若干部署情形。

8.1 IoT设备内的功能实体

图2显示四种类型的物联网设备。物联网设备须至少包含一个FW消费者，因为物联网设备包含多个FW图像是很自然的。

物联网设备须至少包含一个状态跟踪器。设备可包含多个状态跟踪器来处理多个FW消费者，但拥有一个处理所有FW消费者的状态跟踪器也是很好的。

资源受限的物联网设备可能希望将状态跟踪器的功能最小化。在这种情况下，状态跟踪器的功能分为部署在物联网设备外部的客户端模块和服务器端模块。最少功能性，例如与FW消费者的交互，被留在客户端，而其他功能被导出到服务器端。服务器端模块可处理多个客户端模块。这通常是首选的部署类型。

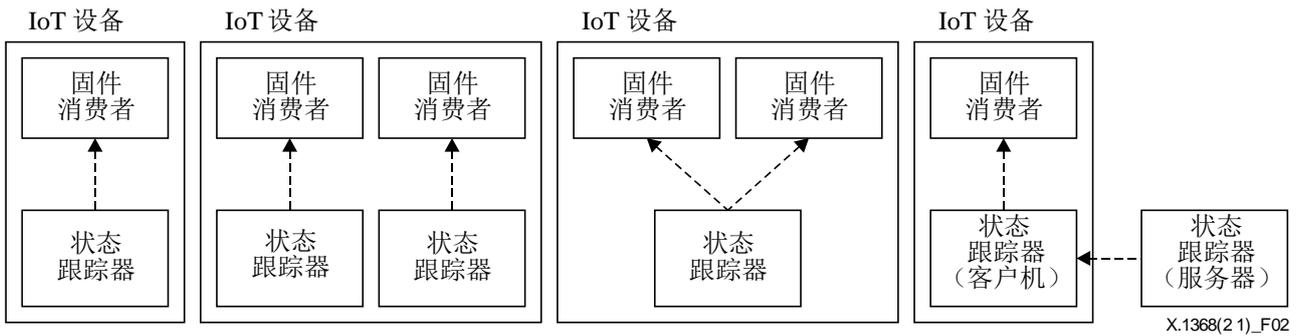


图2 – 不同类型的IoT设备

8.2 状态跟踪器部署类型

物联网设备的资源相差很大；状态跟踪器可位于物联网设备内部，但资源受限的物联网设备可能希望保持跟踪器独立并使其资源消耗最小化。此外，为了方便，可能存在物联网设备首选由集中实体管理的情况。

为了应对这些情况，状态跟踪器可被分成几个模块，并以分层的方式实现。在这种情况下，可以级联多个模块，以便上游模块可判断是否需要更新固件，并通过下游模块启动固件更新程序。

第8.2.1至8.2.3段具体讨论了以下情况：(1) 物联网设备内的状态跟踪器直接与FW服务器通信；(2) 物联网设备内的状态跟踪器通过位于内联网内的另一个状态跟踪器与FW服务器通信；(3) 物联网设备内的状态跟踪器通过多个状态跟踪器与FW服务器通信。

8.2.1 设备内状态跟踪器模型

图3显示设备内状态跟踪器模型。在该模型中，一个FW消费者和一个状态跟踪器驻留于物联网设备中。当状态跟踪器意识到需要进行固件更新时（见第9节），会要求固件消费者从固件服务器接收固件图像。请注意，在本节中通信信道是抽象的，但信道可通过互联网协议或其他协议连接，或者通过需要实体间通信桥的协议组合连接。图3显示互联网，但本建议书中提到的技术也可处理所有其他类型的网络。

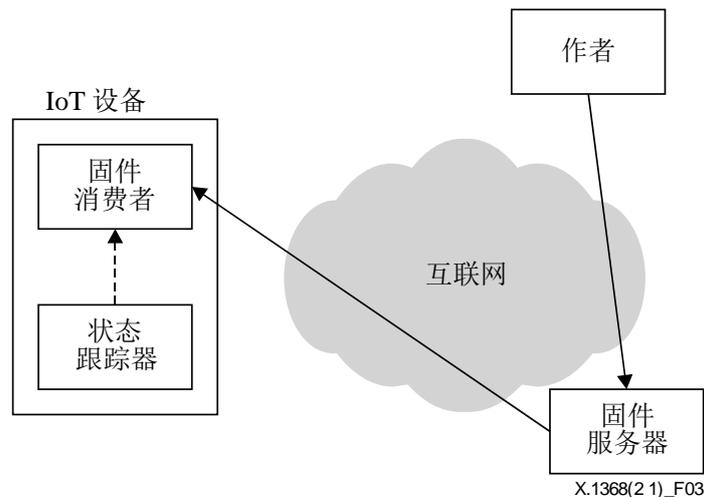


图3 – 设备内状态跟踪器模型部署示例

8.2.2 客户机-服务器状态跟踪器模型

图4显示客户机-服务器状态跟踪器模型。在该模型中，状态跟踪器分为客户机模块和服务器模块。客户机模块位于物联网设备中，而服务器模块则位于网络中。服务器模块通过与客户机模块通信来监控多个物联网设备。客户机器模块简单地验证来自服务器模块的消息，并相应地采取行动。服务器模块启动固件更新程序。

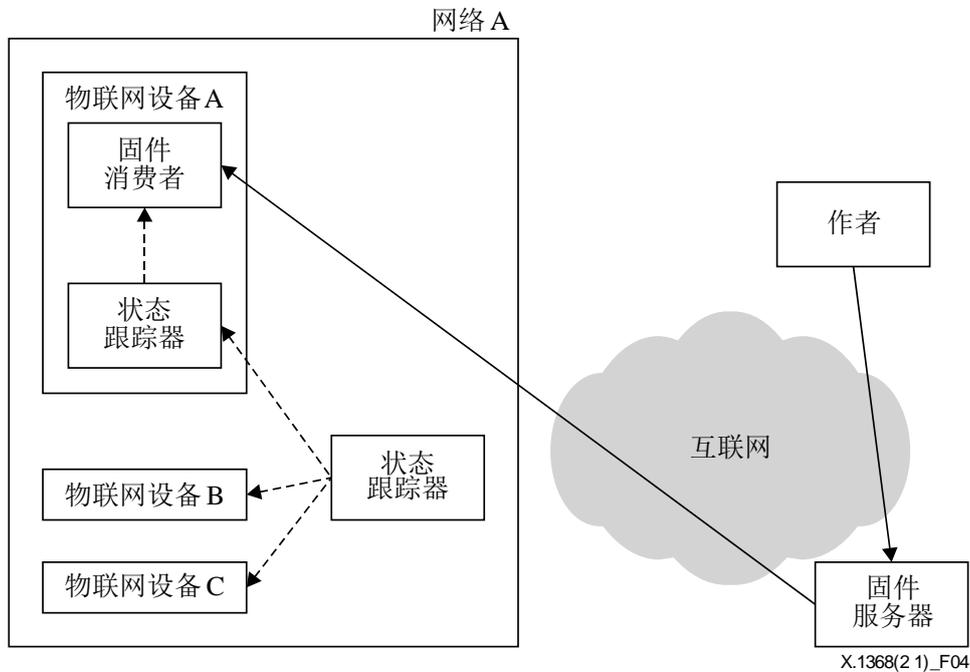


图4 - 客户机-服务器状态跟踪器模型部署示例

8.2.3 分层状态跟踪器模型

图5显示分层状态跟踪器模型。在这个模型中，状态跟踪器被分成几个模块：客户机器模块、中间模块和服务器模块。客户机模块位于物联网设备内，服务器模块和中间模块位于网络内。中间模块通过与客户机模块通信监控几个物联网设备；服务器模块通过与中间模块通信监控所有客户机模块。请注意，中间模块可进行级联，以生成进一步的分层结构。客户机模块简单地验证来自服务器模块的消息，并相应地采取行动。服务器模块启动固件更新程序。

- b) 须对易受攻击的软件/固件采取适当措施：
 - i) 应发现软件/固件的过时版本；
 - ii) 应发现易受攻击的软件/固件。
- c) 更新过程中造成的故障须是可恢复的：
 - i) 如果软件/固件更新失败，则应有通知手段；
 - ii) 在更新过程失败的情况下，应有回退手段或保护手段。
- d) 只应进行预期的和必要的更新：
 - i) 须只安装物联网软件/固件的较新版本；
 - ii) 须只安装可信的物联网软件/固件图像。
- e) 资源限制须得到考虑：
 - i) 如果不需要实现网络资源最小化，则不应进行更新；
 - ii) 状态跟踪器功能可以级联，以将资源受限物联网设备的负担最小化。
- f) 须保护作者的知识产权：
 - i) 软件/固件图像须由作者加密；
 - ii) 物联网软件/固件图像的机密性、完整性和可用性须得到保护；
 - iii) 应从作者那里安全地将SW/FW图像传送到最终目的地。

11 能力

基于第10节中提到的要求，本节列出功能实体的能力。

11.1 固件消费者的能力

- a) 固件消费者应该能够：
 - i) 核实前一次固件更新是否成功；
 - ii) 与有合法权利请求相关信息的各方共享关于其当前软件/固件图像的信息（例如，版本号）；
 - iii) 在更新过程失败的情况下实施回退手段或保护手段；
 - iv) 通知状态跟踪器需要进行固件更新；
 - v) 通过验证其证书自身或通过其它方法确认固件图像的真实性和完整性（例如，将验证过程下放给其它实体）；
 - vi) 做出选择，不安装新版本的软件/固件图像。
- b) 建议固件消费者采用“安全模式”，以最低功能运行物联网设备，并至少提供手动安装、恢复或更新固件的方法。

11.2 状态跟踪器的能力

状态跟踪器应能够：

- a) 充实完善固件消费者列表—有最新固件图像的消费者和固件图像过时的消费者：
 - i) 这些列表应至少包含其唯一标识符，

- ii) 状态追踪器应能够识别其固件已过时的固件消费者；
- b) 了解在其管理下的固件消费者的状况，应有方法能够：
 - i) 通过与固件消费者通信以及检查与固件消费者的通信日志来确认固件消费者（以及包含固件消费者的物联网设备）是否已启动，
 - ii) 确认前一次在固件消费者处运行的固件更新是否成功，
 - iii) 了解FW消费者运行的FW版本；
- c) 判断软件/固件更新是否必要，并在需要时启动固件更新程序；
- d) 当以分级方式实现时，验证上游状态跟踪器的真实性。

当状态跟踪器的功能被分成多个模块时，这些模块须能够：

- a) 保持它们之间通信的保密性和完整性；
- b) 验证彼此发送的信号的真实性；
- c) 完善充实它们的是否到达信息（reachability information）。

11.3 固件服务器的能力

固件服务器应能够：

- a) 接受作者提交的物联网软件/固件图像；
- b) 将其所含软件/固件图像提供给固件消费者；
- c) 识别恶意软件/固件图像，并采取适当的措施，例如从其内部存储中将之删除，并禁止提交此类图像的作者进行提交；
- d) 管理对之使用它的作者和固件消费者列表；
- e) 管理物联网软件/固件图像的版本；
- f) 维护软件固件消费者和他们过去下载的软件/固件图像列表；
- g) 通知过去下载过过时物联网软件/固件图像的物联网设备已有新版本可用；
- h) 检查物联网设备的地理或逻辑位置，以允许或拒绝下载软件/固件图像，从而避免将其分发到政策或其他方式确定禁止的位置。

11.4 作者的能力

作者应能够维护其制作的FW图像的真实性、保密性和完整性。

- a) FW不应被第三方取代或损害（真实性和完整性）。
- b) 应保护固件内供应商的知识产权（保密性）。
- c) 作者应采取措施保护其上传到固件服务器的网络固件图像，因为固件服务器不一定是可信的。

附录I

ITU-T外的相关活动

(本附录不构成本建议书不可分割的一部分)

ITU-T之外研究的与物联网软件更新相关的活动包括:

- 1) IOTSU讲习班 [b-ISOC iotsu];
- 2) IETF SUIT工作组 [b-IETF suit]:
 - 清单 (manifest) 文档 [b-IETF manifest];
 - FW更新架构 [b-IETF architecture];
- 3) oneM2M: M2M和IoT标准 [b-oneM2M]。

附录II

使用分布式账本技术的物联网软件更新情景示例

(本附录不构成本建议书不可分割的一部分)

II.1 概况

物联网基础设施包含管理员需要管理的大量设备。物联网设备根据硬件特性有各种版本，且按照附加的传感器板可能会应用不同的固件。根据硬件版本的不同，支持的软件版本也不同。此外，安装的软件包之间的差异可能会导致出现版本依赖（dependency）问题。通过使用分布式账本技术（DLT）可以解决这一问题。

DLT拥有智能合同，方便基于管理员预先编写的合同进行硬件固件或软件更新。此外，在更新过程中可能出现的安全漏洞可基于一致算法和加密层得到解决。

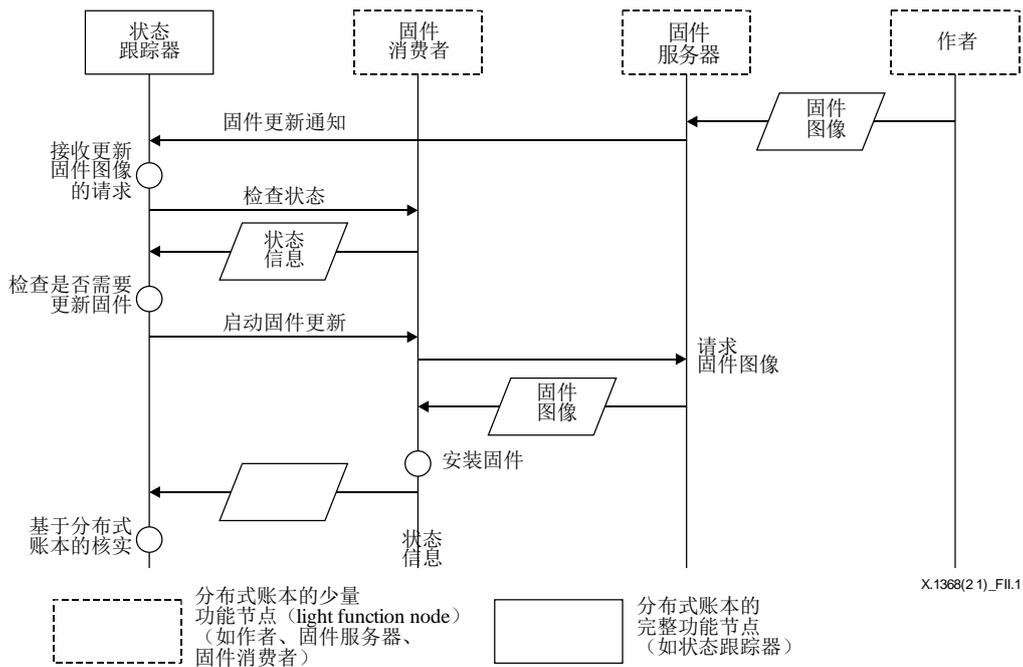
本示例描述如何在具有不同硬件版本和软件版本的环境（如物联网基础设施）中，基于DLT提供安全的固件/软件更新。

II.2 软件更新程序

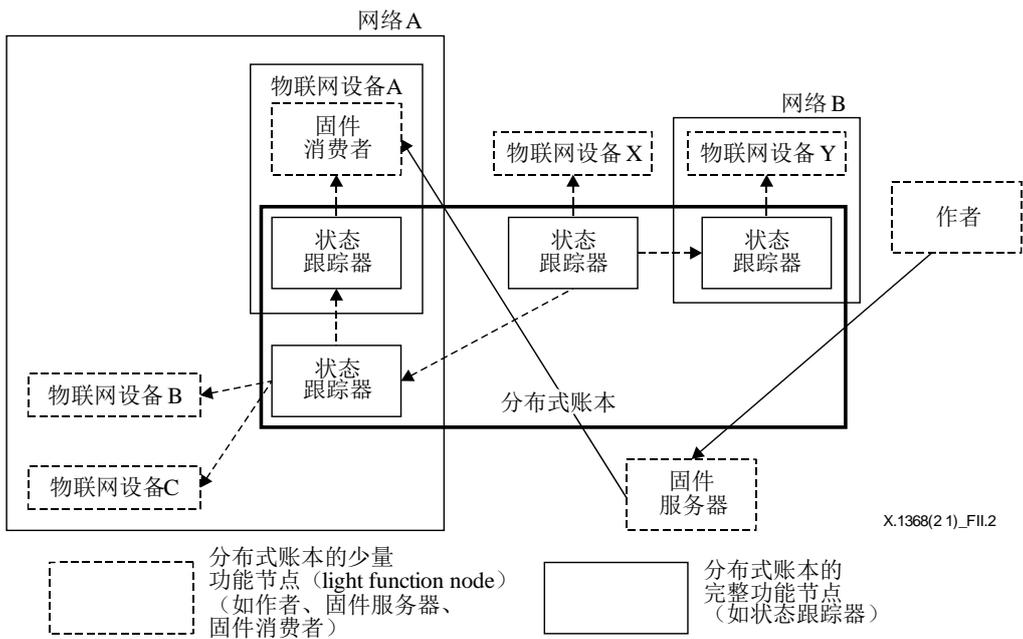
见表II-1以及图II-1和II-2。

表II-1 – 软件更新的块结构

块字头	<ul style="list-style-type: none">- 块大小、版本- 上一个块头散列
块数据	<ul style="list-style-type: none">- 默克根- 提供商名称、发布时间、版本号、文件的散列代码、文件链接、文件名、文件大小、支持硬件、软件依赖性



图II-1 – 基于分布式账本技术的软件更新程序



图II-2 – 基于分布式账本技术的多网络软件更新

参考资料

- [b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels*.
- [b-IETF architecture] IETF SUIT (2019). *A firmware update architecture for Internet of things.*, Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: <https://tools.ietf.org/html/draft-ietf-suit-architecture-08>
- [b-IETF manifest] Moran, B., Tschofenig, H., Birkholz, H. (2019). *Firmware updates for Internet of things devices – An information model for manifests*. Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: <https://tools.ietf.org/id/draft-ietf-suit-information-model-02.html>
- [b-IETF suit] IETF (2021). *Software updates for the internet of things (suit)*, version 7.26.0. Wilmington, DE: Internet Engineering Task Force. Available [viewed 2021-02-19] at: <https://datatracker.ietf.org/wg/suit/about/>
- [b-ISOC iotsu] Internet Architecture Board (Internet), *Internet of things software update workshop (IoTSU) 2016*. Reston, VA: Internet Society. Available [viewed 2021-02-20] at: <https://www.iab.org/activities/workshops/iotsu/>
- [b-oneM2M] oneM2M (2017), *Standards for M2M and the Internet of things*. oneM2M. Available [viewed 2021-02-20] at: <http://www.onem2m.org/technical/published-drafts>

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	数据网、开放系统通信和安全性
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题