

基于 Contiki 的 CoAP 协议分析

曹雪峰,傅冬颖,蔡永华,尚宇辉,朱会卿

(河北民族师范学院 数学与计算机科学学院 河北 承德 067000)

摘 要: 受限的应用协议 (CoAP) 是专门为资源受限设备和网络优化设计的一种网络传输协议,它采用 REST 风格架构,为资源受限环境进行重新设计,实现了超文本传输协议的一部分功能子集,允许用户通过浏览器直接访问物联网节点,进行资源发现和数据查询等,是物品万维网技术的核心。文中介绍了受限的应用协议的工作原理,在 Contiki 系统支持下利用 Cooja 搭建虚拟无线传感器网络,设计了受限的应用协议分析的实验环境和实验方案。在无线传感器网络仿真运行过程中,利用协议分析软件捕获受限的应用协议报文,然后对捕获的受限的应用协议报文进行分析,说明了受限的应用协议的报文格式、工作模式和选项字段的作用,描述了 GET 和 POST 方法的工作过程,从理论和实践两方面阐述了受限的应用协议的工作原理。

关键词: 受限的应用协议; REST; 工作模式; 资源描述

中图分类号: TP391.9

文献标识码: A

文章编号: 1673-629X(2019)05-0092-05

doi: 10.3969/j.issn.1673-629X.2019.05.020

Analysis of CoAP Principle Based on Contiki

CAO Xue-feng, FU Dong-ying, CAI Yong-hua, SHANG Yu-hui, ZHU Hui-qing

(School of Mathematics and Computer Science, Hebei Normal University for Nationalities, Chengde 067000, China)

Abstract: The Constrained Application Protocol (CoAP) is a network transport protocol that is specially designed for resource-constrained devices and network optimized design. It uses a REST-style architecture to redesign resource-constrained environments and implements a subset of the HTTP functionality, enabling users to access the IoT node resources through the browser directly, making resource discovery and data query, which is the core of the world wide web technology. We introduce the working principle of the CoAP, adopt Cooja to build a virtual wireless sensor network supported by the Contiki system, and design the experimental environment and scheme of CoAP analysis. During the wireless sensor network simulation running, the protocol analysis software is used to capture the CoAP report, and then the captured CoAP messages are analyzed, explaining the role of CoAP message format, working mode and option fields, description of the working process of GET and POST methods, and elaborating the work principle of the CoAP both theoretically and practically.

Key words: constrained application protocol; representational state transfer; working mode; resource description

0 引 言

将万维网技术与物联网技术相结合的物品万维网技术是物联网的一种实现模式^[1-5]。利用 Web 的设计理念和技术,搭建基于不同通信方式的异构网络和分布式网关的泛在应用开发环境,把物联网网络环境中的设备抽象为资源和服务,并采用 RESTful 框架发布这些资源和服务,让用户能够通过浏览器直接访问到对应的传感器节点,获取或订阅该节点所感知的数据,并对节点进行远程控制。这将大幅度降低物联网应用的开发难度,提升物联网应用创新的可能性,而采用

CoAP 实现基于 RESTful 的 Web 服务机制是目前常用的一种方法^[6-7]。受限的应用协议 (constrained application protocol, CoAP) 是专门为资源受限设备和网络优化设计的网络协议。它采用 REST (representational state transfer) 风格架构,将网络上的所有对象抽象为资源,每个资源对应一个唯一的统一资源标识符 (universal resource identifier, URI),通过 URI 可以对资源进行无状态操作,包括 GET、PUT、POST 和 DELETE 等。CoAP 并不是 HTTP 的压缩协议。CoAP 一方面实现了 HTTP 的一部分功能子集,并为资源受限环境

收稿日期: 2018-06-19

修回日期: 2018-10-24

网络出版时间: 2018-12-21

基金项目: 河北省高等学校科学技术研究项目 (ZC2016116); 2017 年河北省高等学校创新创业教育教学改革研究与实践项目 (2017CXCY168)

作者简介: 曹雪峰 (1967-), 男, 硕士, 副教授, 研究方向为计算机网络。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20181221.1554.048.html>

进行了重新设计; 另一方面提供了内置资源发现、多播支持、异步消息交换等功能。

Contiki 是一个开源操作系统^[8-11], 可以在其官方网站上下载到全套的源代码, 目前最新版本为 Contiki3.0。Contiki 操作系统支持 CoAP 协议。Cooja 是 Contiki 操作系统下的无线传感器网络仿真工具, 在 Cooja 中可以采用目前流行的多种传感器构成的不同传感器网络, 分析无线传感器网络不同层的协议。

1 CoAP 协议原理

1.1 CoAP 报文格式

CoAP 报文格式如图 1 所示^[12-16]。

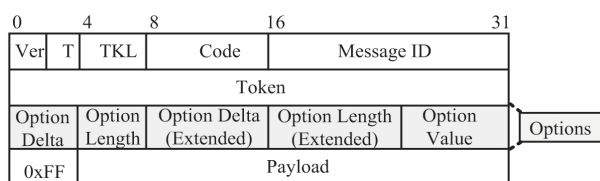


图 1 CoAP 报文格式

Ver: 2 bit, 说明 CoAP 的版本号, 固定值为“1”;

T: 2 bit, 说明 CoAP 的报文类型, CoAP 定义了四种类型报文:

Confirmable(CON): 需要被确认的报文, 值为“00”;

Non-Confirmable(NON): 不需要被确认的报文, 值为“01”;

Acknowledgement(ACK): 应答报文, 值为“10”;

Rest(RST): 复位报文, 值为“11”;

TKL: 4 bit, 说明标签字段的长度, 单位为字节。其值为 0 时表示省略标签字段;

Code: 1 字节, 说明 CoAP 的请求方法或响应状态。该字段分成高 3 位和低 5 位两部分, 用十进制数表示成 x.xx 的形式。CoAP 定义了四种请求方法和四种响应报文:

Code=0.00, 表示空报文;

Code=0.01, 表示 GET 方法;

Code=0.02, 表示 POST 方法;

Code=0.03, 表示 PUT 方法;

Code=0.04, 表示 DELETE 方法;

Code=2.xx, 表示正确响应;

Code=4.xx, 表示客户端错误响应;

Code=5.xx, 表示服务器端错误响应。

Message ID: 2 字节, 说明 CoAP 报文的序号, 用于重复性检查, 实现可靠传输。一对 CoAP 请求和响应的 Message ID 值必须相同;

Token: 长度可变, 是另一种形式的 CoAP 报文序号, 在独立式响应中起着重要作用;

Options: 长度可变, 可以没有或有多多个选项, 具体包括如下内容:

Option Delta: 4 bit, Option 的增值, 相当于顺序编号, 当前的 Option 的具体编号等于之前所有 Option Delta 的总和。它的值可以为 0-12, 或者 13, 14。当为 13 或者 14 时, 需要增加一个 Option Delta (extend) 字段, 此字段长度为 0-2 字节;

Option Length: 4 bit, Option 的长度, 表示 Value 的具体长度, 它的值可以为 0-12, 或者 13, 14。当为 13 或者 14 时, 需要增加一个 Option Length (extend) 字段, 此字段长度为 0-2 字节;

Option Value: 0 或多个字节, 表示 Option 具体内容。

CoAP 的所有选项都采用编号的方式定义, 每个选项字段有 4 个属性: C(Critical)、U(Unsafe)、N(No-CacheKey) 和 R(Repeatable), 前三个属性值是编号的组成部分。常见的选项包括 Uri 相关选项、Content-Format 选项、Accept、Etag、Block1 和 Block2 选项等内容;

0xFF: CoAP 首部与负载之间的分隔符;

Payload: 是和具体应用相关的内容, 包括多种不同格式的媒体。

1.2 工作模式

虽然 CoAP 协议是基于运输层不可靠的 UDP 协议实现的, 但是它利用可靠传输机制提供了可靠传输的请求/响应工作模式。

(1) 捎带式响应(piggybacked response)。

是指发送方的请求报文采用 CON 类型的报文, 如果接收方能立即做出响应, 响应数据就包含在 ACK 类型的确认报文中。

(2) 独立式响应(separate response)。

是指发送方的请求报文采用 CON 类型的报文, 但是接收方因某种原因不能立即做出响应, 因此在接收方返回的 ACK 类型的确认报文中并不包含响应数据。当接收方准备好该请求的响应数据后, 会向发送方发送一个包含响应数据的 CON 类型报文, 该报文需要得到发送方的确认。

如果发送方的报文不需要确认, 可以采用非可靠传输的非确认模式(non-confirmable response) 来实现。在非确认模式中发送方采用 NON 类型报文发送请求, 接收方收到此报文后, 同样放回 NON 类型的响应报文。

1.3 CoAP 资源描述

CoAP 使用 URI 标识一个资源, 然后通过 GET、POST、PUT 和 DELETE 方法来操作这些资源。URI 的格式如下:

coap-URI="coap:" "://" host [":" port] path-abempty ["?" query]

其中 host 为资源所在主机,不能为空,可以使 IP 地址或域名; port 为服务器监听端口,coap 默认为 5683,coaps 为 5684; path 为指定资源在主机上的路径; query 用于参数化资源。

另外,CoAP 协议规定通过访问/.well-known/

core,可以查看传感器节点提供的所有资源,这些资源以层次结构组织起来,用户可以对资源进行进一步的操作。

2 无线传感器网络的组建

2.1 网络拓扑结构

在 Cooja 中按图 2 搭建无线传感器网络。

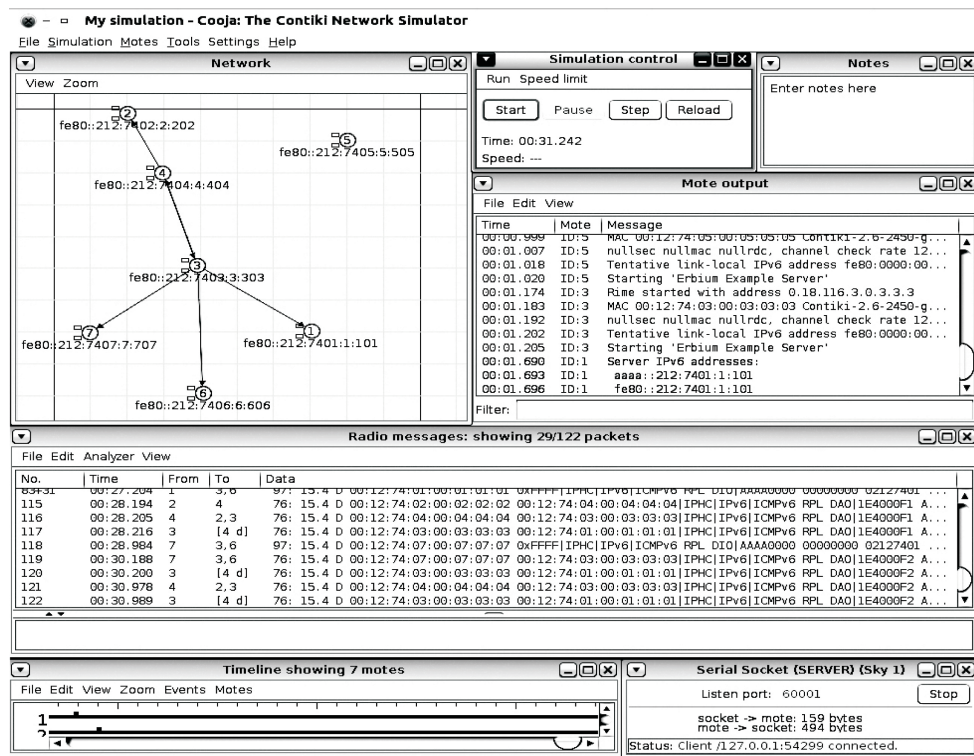


图 2 无线传感器网络拓扑结构

其中节点 1 为无线传感器网络的网关,其上运行程序 border-router.c。其他节点上都运行 CoAP 服务器程序 er-example-server.c。

2.2 环境配置

为了能够通过互联网上的远程用户终端访问传感器节点,需要将链路本地地址映射为 IPv6 的全球单播地址,这一工作由网关完成。首先通过 Cooja 的菜单项“tools->serial socket->sky1”打开网关节点的侦听端口 60001。然后打开新的 ubuntu 终端窗口,改变目录到 contiki/examples/er-rest-example,执行如下命令,完成地址映射。

```
make connect-router-cooja
```

为了生成用于 wireshark 进行协议分析的报文跟踪记录文件,选择 Cooja 的菜单项“tools/radio messages”打开 radio messages 对话框,在 radio messages 对话框中选择“analyzer/6LoWPAN Analyzer with PCAP”菜单项,在仿真过程中的报文跟踪记录文件保存在 Contiki 操作系统的 tools/cooja/build 文件夹中,文件扩展名是.pcap。

然后选择 cooja 的“simulation->start simulation”菜单项启动仿真过程。

在安装了 copper 插件的火狐浏览器中连接无线传感器网络中地址为 aaaa::212:7402:2:202 的节点 2,单击“discover”按钮后,就会在浏览器“discovering”区域列出在其上已激活的资源。

3 CoAP 工作过程分析

3.1 GET 方法工作过程

选中“test/hello”,然后单击浏览器上“GET”按钮,可以看到节点 2 返回的“Hello World!”消息。对此过程捕获的 COAP 报文如图 3 所示。

图中 370 号报文是客户端发送的 GET 请求报文,是需要被确认的报文,省略了标签字段,报文序号为 16637;它有 3 个选项字段,前两个选项字段的编号为 11,是 Uri-Path 选项,指示资源在服务器中的位置,值分别为“test”和“hello”;第三个选项字段的编号为 23 (12+11),是 Block2 块传输选项,因为是 Block2,所以使用的是块传输的控制性用法,希望响应的块序号是

“0” 块大小是 64 字节。

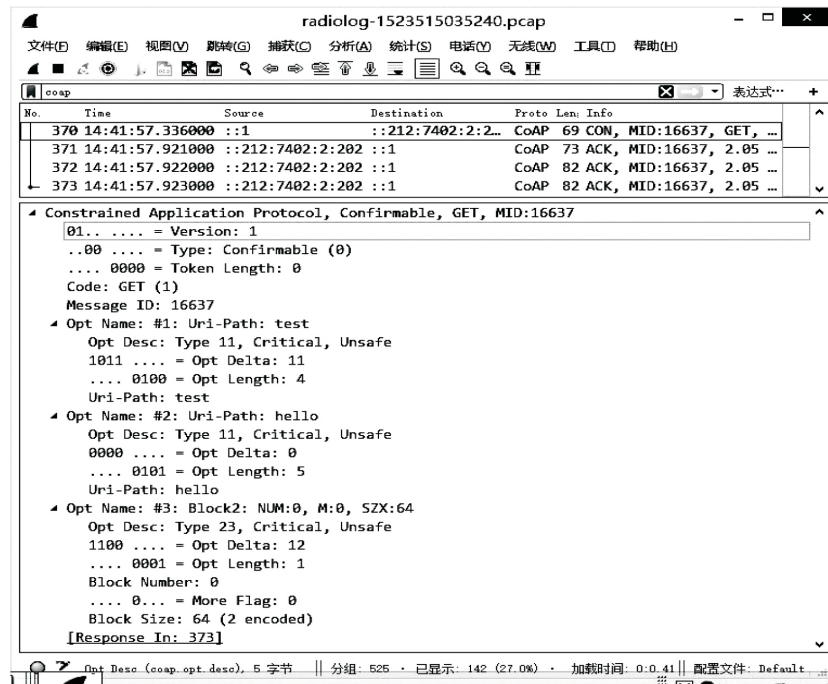


图3 GET 的请求报文

图4中的373号报文是CoAP服务器返回的GET响应报文,是应答报文,省略标签字段,响应代码为“2.05 content”,报文序号为16637,与请求报文一致。它有3个选项字段,第一个选项字段的编号为4,是ETag选项,作为资源本地标识符,用来区分同一资源在不同时间的变化,值为“0C”;第二个选项字段的编号为12(8+4),是Content-Format选项,指明CoAP负载的媒

体类型,值为“text/plain; charset=utf-8”,也就是说负载的媒体类型为文本或二进制类型,采用utf-8编码;第三个选项字段的编号为23,是Block2块传输选项,因为是Block2,所以使用的是块传输的描述性用法,表示当前报文的负载在资源描述中的块序号是“0”,块大小是32字节,负载内容是“Hello World!”。

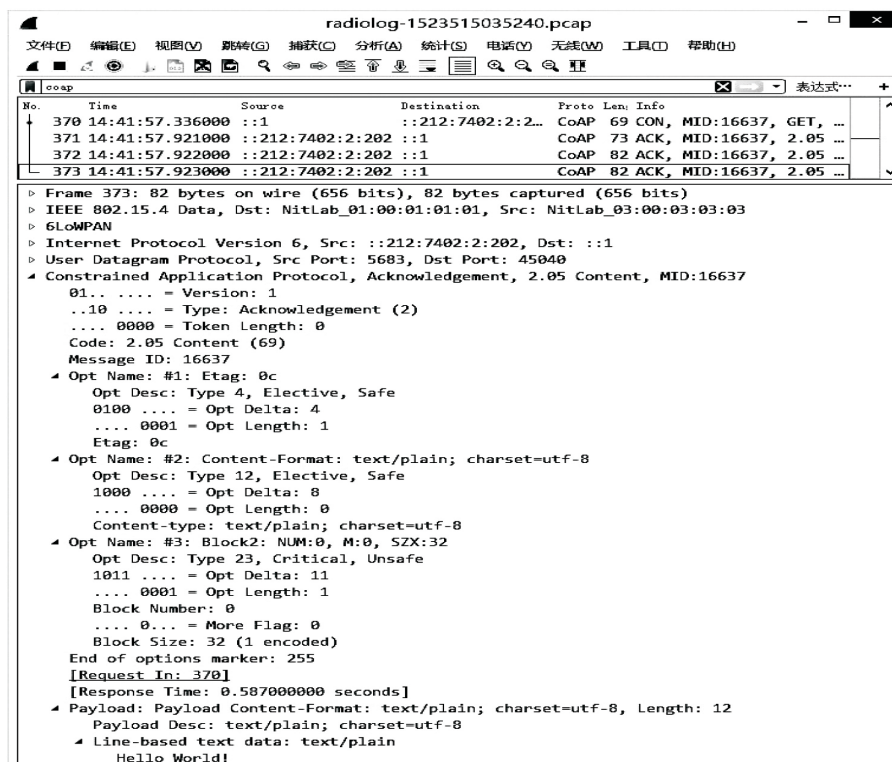


图4 GET 的响应报文

3.2 POST 方法工作过程

通过浏览器上的“POST”按钮就可远程控制传感器节点上的红色 Led 灯。选中“actuators/toggle”,然后单击浏览器上“POST”按钮就可控制节点 2 上的红色 Led 灯亮。该过程捕获的 CoAP 报文如图 5 所示。

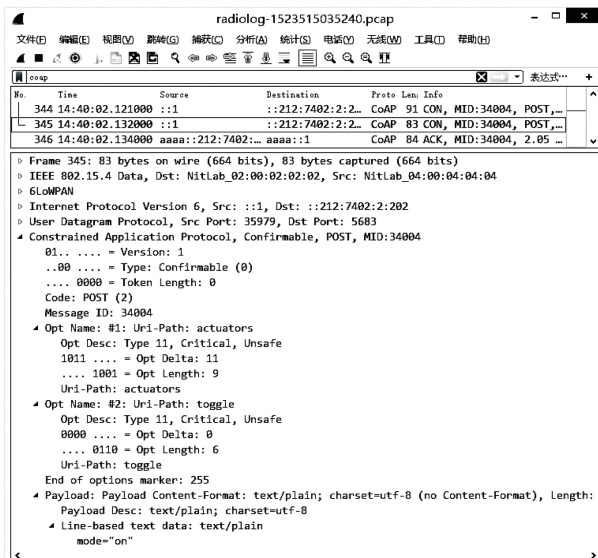


图 5 POST 的请求报文

图中 345 号报文是客户端发送的 POST 请求报文,是需要被确认的报文,省略了标签字段,报文序号为 34004,它有 2 个选项字段,编号都为 11,是 Uri-Path 选项,指示资源在服务器中的位置,值分别为“actuators”和“toggle”;负载字段的值为“mode = “on””。

图 6 中 346 号报文是 CoAP 服务器返回的 POST 响应报文,是应答报文,省略了标签字段,响应代码为“2.05 content”,报文序号为 34004,与请求报文一致。

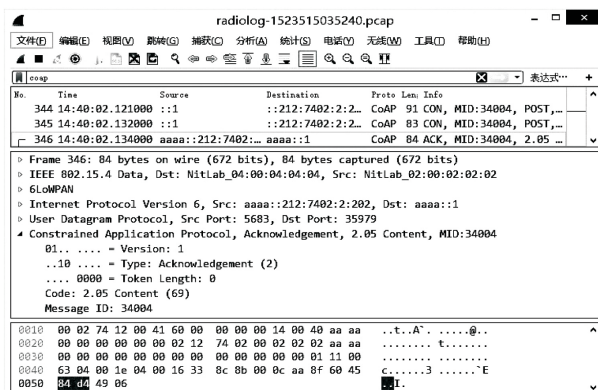


图 6 POST 的响应报文

如果把 POST 请求报文中负载字段内容改为“mode = “off””,重复前面的操作,会看到节点 2 上的红色 Led 灯熄灭。

4 结束语

在 Contiki 无线传感器网络操作系统的支持下,利

用 Cooja 构建了由路由网关节点和 CoAP Server 节点组成的无线传感器网络,用火狐浏览器访问传感器节点,查看传感器节点上的资源,并对传感器节点进行实时控制,实现了全 IP 物联网网络融合目标。利用 Wireshark 对捕获报文进行分析,说明了 CoAP 协议的工作过程,验证了 CoAP 协议的工作原理。

参考文献:

- [1] 纪阳,成城,唐宁. Web of Things: 开放的物联网系统架构研究[J]. 数字通信, 2012, 39(5): 14-19.
- [2] 李养群,沈苏彬,许斌. 物品万维网技术综述[J]. 南京邮电大学学报: 自然科学版, 2014, 34(2): 32-42.
- [3] 付国强,张显金. 适用于 WoT 架构的物联网协议分析[J]. 电信网技术, 2014(3): 4-9.
- [4] 黄忠,葛连升. 基于 CoAP 的物联网 Web 服务统一访问方法[J]. 山东大学学报: 工学版, 2014, 44(4): 18-23.
- [5] DILLON T S, HAI Zhuge, CHEN Wu, et al. Web-of-things framework for cyber - physical systems [J]. Concurrency and Computation: Practice and Experience, 2011, 23(9): 905-923.
- [6] 左文娟,张秋菊. 基于 REST 物联网监控系统设计[J]. 计算机工程与设计, 2016, 37(1): 21-25.
- [7] COLITTI W, STEENHAUT K, DE CARO N, et al. REST enabled wireless sensor networks for seamless integration with web applications [C]//2011 IEEE 8th international conference on mobile ad-hoc and sensor systems. Valencia, Spain: IEEE, 2011: 867-872.
- [8] 朱琳,高德云,罗洪斌. 无线传感器网络的 RPL 路由协议研究[J]. 计算机技术与发展, 2012, 22(8): 1-4.
- [9] 肖湘宁,王鹏,李建立,等. 基于 6LoWPAN 的边缘路由器设计研究[J]. 计算机科学, 2015, 42(12): 215-219.
- [10] 陆慧娟,刘亚卿,夏海霞,等. 6LoWPAN 网络中 RPL 路由协议的仿真与研究[J]. 小型微型计算机系统, 2016, 37(1): 83-87.
- [11] MATTHIAS K, SIMON D, ADAM D. A low-power CoAP for Contiki [C]//2011 IEEE 8th international conference on mobile ad-hoc and sensor systems. Valencia, Spain: IEEE, 2011: 855-860.
- [12] SHELBY Z. Constrained restful environments (CoRE) link format [S]. [s.l.]: IETF, 2012.
- [13] SHELBY Z, HARTKE K, BORMANN C. The constrained application protocol (CoAP) [S]. [s.l.]: IETF, 2014.
- [14] RAHMAN A, DIJK E. Group communication for the constrained application protocol (CoAP) [S]. [s.l.]: IETF, 2014.
- [15] HARTKE K. Observing resources in the constrained application protocol (CoAP) [S]. [s.l.]: IETF, 2015.
- [16] BORMANN C, SHELBY Z. Block-wise transfers in the constrained application protocol (CoAP) [S]. [s.l.]: IETF, 2016.