



轻量级工业物联网控制网络协议研究

Research of Lightweight Control Network Protocols for Industrial Internet of Things

■ 上海宝信软件股份有限公司 黄 明

摘 要 针对工业物联网的特点, 提出了一种轻量级的基于 IEEE 1888 网络框架的可靠的二进制协议标准, 解决了 IEEE 1888 存在的信息冗余和效率低等不足, 规定了通信协议接口格式、数据编码格式、通信网络控制等二进制格式。

关键词 IEEE 1888 工业物联网 控制网络协议 服务质量 变长编码 心跳机制 数据质量

Abstract: According to the characteristics of Industrial Internet of Things, the paper proposes a reliable light weight binary Control Network Protocols based on IEEE 1888 network framework, it solves the insufficiency of IEEE 1888 such as the information redundancy and inefficiency. The communication protocol interface, data encoding format, communication network control are all specified.

Keywords: IEEE 1888; Industrial Internet of Things; control network protocols; quality of service; variable length coding; keep alive; quality of data

1 引言

新常态下的绿色发展和绿色经济引起了社会的广泛关注, 成为了当今社会经济发展的主流, 在这一背景下智慧能源迅速崛起。智慧能源旨在利用信息通信技术提高能源使用效率, 利用信息通信技术智慧地管理楼宇、工厂、家庭中的各种能耗设备, 将能源赋予新的数据属性, 从而达到能源的经济性、高效性及环保性的效果。

在构建能源互联网过程中, 如何使数以百亿计的设备与网络互联互通, 同时将这些设备产生的海量数据进行格式统一并最终保证数据安全成为亟需解决的关键问题^[1]。为解决设备与设备、设备与网络、信息与数据间存在的“孤岛”问题, 实现能源互联网产业的广泛部署, 以 IEEE 1888 为代表的互联网通信协议标准应运而生, 在智慧能源, 特别是需求侧管理上发挥了显著成效^[2]。然而, 将其应用于工业物联网领域的过程中, 基于全 IP 思路设计出的 IEEE 1888 存在网络质量控制、协议冗余等诸多问题, 因此

我们在 IEEE 1888 网络架构设计基础上提出了一种可靠的轻量级工业物联网控制网络协议。

2 IEEE 1888

2.1 IEEE 1888 简介

IEEE 1888-2011《泛在绿色社区控制网络协议》是由中国企业主导制定的国际标准, 该标准采用全 IP 的思路, 深度融合 IPv6、物联网、云计算等信息通信技术, 构建了一个开放的能源互联网体系, 可广泛应用于智慧能源系统, 包括下一代电力管理系统、楼宇能源管理系统、设施设备管理系统等领域的通信^[4]。

IEEE 1888 系统由网关 (GW)、存储器 (Storage)、应用单元 (APP)、注册器 (Registry) 等组件构成, 以管控点 (Point) 为单位处理数据, 注册器也是网关、存储器、应用单元的管理平台, 各组件通过 TCP/IP 网络通信。传感器和执行器等设备通过使用某种现场总线网络与网关连接, 进而接入 IEEE 1888 系统;

项目来源: 上海市科学技术委员会科研计划“基于自主可控的物联网控制协议的钢铁供应链协同业务需求和整体框架研究及标准制定”, 项目编号: 16DZ0502900; 上海市青年科技启明星计划, 项目编号: 17QB1400500。

存储器在 IEEE 1888 中将在线化的传感器数据或状态信息长期保存，可在任意时间读取；应用单元则有很多功能和开发方式，例如可视化应用或统计分析应用等；注册器负责在网络中维护“组件与数据信息”的对应关系；管控点则表示现场设施网络领域的检测点、控制点。

2.2 IEEE 1888 在工业物联网应用中面临的问题

在 IEEE 1888 应用于工业物联网过程中，基于全 IP 思路设计出的 IEEE 1888 存在一些问题：(1) 基于 SOAP 的 XML 通信协议容易产生过多的标签信息，特别是网络环境不好的情况下，例如应用于终端设备 GPRS 网络；(2) 工业设备通信的效率不高，工业设备通信需要具备高效低延时的特点，设备终端的通信能力不高，无法确保基于 XML 通信的时效性；(3) 安全性和稳定性不足，基于基础 TCP 通信使得协议执行无法确保交互的准确和严谨性。

3 轻量化的二进制协议标准

针对工业数据的特点，需要解决 IEEE 1888 协议存在的应用不足，以适合要求更为苛刻的工业生产要求。二进制标准中明确了基础数据结构定义规范，以及通信协议接口规范，采用网络服务质量 (Quality of Service, QoS) 控制、数据质量管理、变长编码 / 解码技术、心跳机制与安全通信等相关技术以提高通信效率以及安全可靠。

3.1 数据编码格式

通过引入二进制的编码方式解决信息冗余。与 XML 格式的数据编码方式相比，二进制的编码方式去除了 XML 中大量的冗余标签，使数据表示方式更为紧凑。在同样的流量下，传输的数据量比原协议要多 3~5 倍。因此，在工业传输中不仅极大地降低了对数据传输的带宽要求，而且也减少了数据编解码的计算资源开销，使数据互联的实时性大为提高。

每条消息包含三个部分，分别为消息头、消息体长度和消息体，其格式如图 1 所示。其中，varint

表示变长编码，详见 3.2 节说明；uint8 表示 8 位无符号整型；uint32 表示 32 位无符号整型。

DUP flag 只有在 QoS 值为 1 或 2 时才有效，值为 0 表示发送方第一次发送；1 表示发送方的重复发送。通过 DUP flag 的标识可以提升接收方数据处理的效率。

2-ACK flag 只有在 QoS 值为 2 时有效。如果是第一次应答，则为 0，第二次应答为 1。

消息 ID 用于标识 Message 的唯一性，当 QoS 值为 0 和 3 时，不存在 ID 字段。

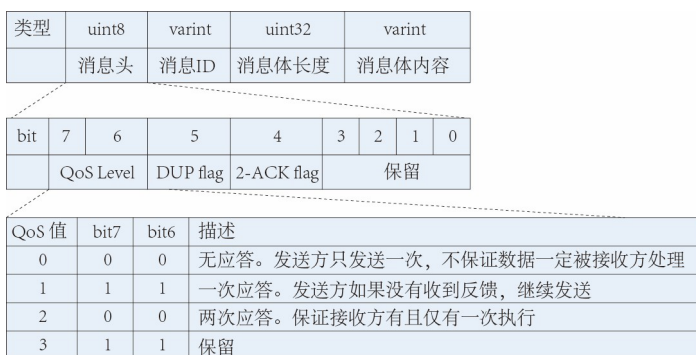


图 1 二进制协议消息结构

3.2 数据变长编码

变长编码 / 解码技术是采用主要针对无符号型整数，该类型采用变长编码方式对整数进行编码。由于网络上传输的整型数大多数情况下数值并不大，如果采用定长编码，就必须预留空间以保证大数值的数也可以进行传输，这样就会浪费宝贵的网络流量。变长编码根据需要传输的整型数的数值范围进行编码，小数使用短的字节进行编码，而大数使用长的字节进行编码。对整数的变长编码和解码操作，可以大大减少数据消息的大小，节省网络流量和负载。

这种方式中，每个 Byte 的最高 bit 位表示后面的一个 Byte 是否是这个整数的一部分，如表 1 所示。

表 1 变长编码每个 Byte 数据格式

bit 位	7	6	5	4	3	2	1	0
含义	标识		有效数字					

如果标识位 bit7 为 0，表示后面紧邻的字节与这个整数表达无关；如果 bit7 为 1，表示后面的字节为

这个整数的一部分。这样，当整数小于 128 时，就可以用一个字节进行表示。

3.3 网络 QoS 控制

网络 QoS 控制指通过协议本身设置的一组数据收发规则，为指定的网络通信提供更好的服务能力，为传输提供一种安全机制，用来解决网络延迟和阻塞等问题。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS。但是对数据传输和控制等关键应用是十分必要的。当网络过载或阻塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行^[5]。

针对工业数据互联的重要性，通过引入三个可靠性等级满足不同的数据传输要求，如图 2 所示。通过定义不同的消息应答模式，实现不同通信场景的应用需求，包括无应答模式、一次应答模式、两次应答模式。特别是二次应答模式对于工业控制极其必要，因为工业中一个设备如果多执行一次，会造成巨大的损失。采用不同的传输可靠性等级使得数据互联更为安全可靠。

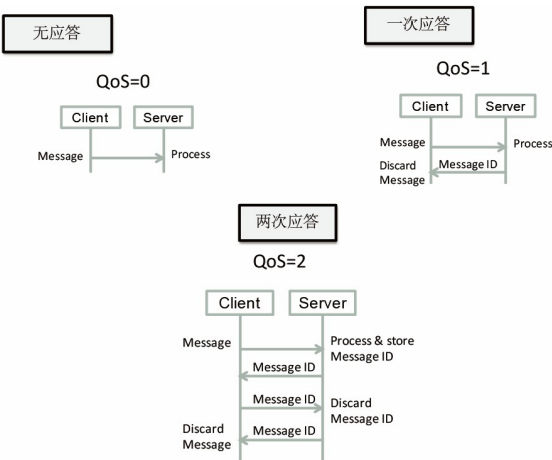


图 2 三个可靠性等级的时序图

(1) 无应答模式

当应用程序对于传输可靠性要求不高，发送方不关心数据是否一定可靠地传送到接收方时，可以采用无应答模式进行传输。此时，消息的头部 (Head) 中设置的 QoS 值为 0。无应答模式特别适合发送方受硬件条件限制，没有足够的数据存储空间，无法

缓存发送数据的场合。另外，如果网络延时特别严重，而发送数据量又非常大时，发送方无法忍受长时间的应答等待，也比较适合这种应答模式。

在无应答模式下，Client 不管数据是否发送成功，只向 Server 发送一次。Server 端仅做数据接收工作，不向 Client 端反馈结果。

(2) 一次应答模式

在大多数情况下，发送端要求数据即使偶尔会发送失败，也必须能够确保数据发送给服务端，此时适合采用一次应答模式。在一次应答模式下，消息的头部 (Head) 中设置的 QoS 值为 0。大多数网络应用适合这种模式发送数据。

在正常流程下，客户端发送一个消息给服务端，服务端收到消息后进行处理，然后将处理结果反馈给客户端。当客户端没有将消息成功发送给服务端，或者服务端没有将处理结果反馈给客户端，客户端都不会收到反馈的消息。如果出现这种情况，客户端会一直向服务端发送数据，直至收到服务端反馈为止。

在一次应答模式下，即使偶尔出现发送失败，客户端也可以保证服务端一定能收到消息。但是服务端有可能会多次收到客户端发送的请求。

(3) 两次应答模式

在某些数据传输要求比较高的场合，比如发送控制指令，希望服务端在收到消息后执行且仅执行一次。这种场合下就需要使用两次应答模式，此时，消息的头部 (Head) 中设置的 QoS 值为 2。

在正常流程下，第一次应答时客户端发送请求给服务端，服务端收到请求后执行指令，保存消息的 ID 并将执行结果发回给客户端。第二次应答时客户端将消息 ID 再传送给服务端，服务端删除保存的消息 ID，并回传给客户端。

在第一次应答时，如果客户端没有收到服务端的第一次回复，会反复进行传送。而服务端第一次收到消息时会执行，但是如果多次收到同一条消息，服务端会去比对存储的消息 ID，如果发现重复，就拒绝再次执行，同时将前一次的执行结果反馈给客

户端。这种机制可以保证服务端对同一个消息会仅执行一次。

3.4 心跳机制和安全通信

心跳机制 (Keep Alive) 和安全通信技术则有助于网络环境的维持和身份识别校验的解决, 提供可靠的通信能力。当采用 TCP 连接, 连接的双方在连接空闲状态时, 如果任意一方意外崩溃、宕机、网线断开或路由器故障, 另一方无法得知 TCP 连接已经失效, 除非继续在此连接上发送数据导致错误返回。这种情况下, 服务端维持了无效的 TCP 连接, 占用了系统资源。因此有必要存在一种机制, 使服务器端和客户端都能及时有效地检测到连接失效, 然后优雅地完成一些清理工作, 及时释放系统资源, 对于需要维持大量 TCP 连接的服务器具有非常重要的意义。

为了及时有效地检测到通信一方的非正常断开, 采用心跳机制。通过通信的一方或双方发送心跳包来告诉对方网络通信是否正常或已断开。

3.5 数据质量管理

数据质量代表了数据获取时的状态, 也就是与设备真实值的关系, 遵从 OPC Foundation 的标准^[6]。从实际使用角度出发, 数据质量只采用 OPC Foundation 中的低 8 位, 共一个字节, 其格式如表 2 所示。

表 2 数据质量编码格式

bit 位	7	6	5	4	3	2	1	0
状态	主质量		子状态				受限状态	

其中, 6~7 两个 bit 位代表了主质量, 2~5 四个 bit 位代表了子状态, 0~1 两个 bit 位代表了受限状态, 不依赖于主质量和子状态。

4 结语

通过对二进制标准与 IEEE 1888 的技术对比 (表 3) 结果显示:

二进制协议技术改进可以实现其网络架构上轻量级的二进制网络控制协议, 特别是满足了工业物联网应用的特点, 打通了不同设备在数据传输和控

表 3 二进制标准与 IEEE 1888 技术特点对比

对比项	IEEE 1888	二进制协议
格式	XML	二进制
压缩	无	变长编码
协议规定	示例说明	严格规范
实时性	低	高
流量敏感	否	是
网络 QoS	无	多种应答模式

制之间的通道, 提供设备、网关、存储器、应用间的标准通信, 为工业物联网领域的整体系统拓展、维护提供了便捷和可操作性。通过实际项目应用, 改进后的协议标准体现了优异的可靠性、实时性, 同时保持了整个网络架构的灵活性。

参考文献

[1] International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things [R/OL].[2017-08-03].http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf.

[2] 达涌. 智慧能源 开启能源互联网新纪元 [N]. 人民邮电, 2015-01-22(1).

[3] IEEE Standards Association. 1888-2011 IEEE standard for ubiquitous green community control network protocol [EB/OL]. (2014-05-30)[2017-08-03]. <http://ieeexplore.ieee.org/document/6823054/>.

[4] 黄钰梅, 董文生, 范昀, 等. 基于 IEEE 1888 的“宝之慧”能源云服务平台 [J]. 信息技术与标准化, 2014(3):60-63.

[5] 裴康乐, 郑巧珍, 李含辉. MPLS DiffServ 在舰内 VoIP QoS 中的仿真与研究 [J]. 舰船电子工程, 2016(1): 51-54,75.

[6] OPC Foundation. OPC data access custom interface specification version 2.05 [EB/OL]. (2002-06-28)[2017-08-03]. <https://opcfoundation.org/developer-tools/specifications-classic/data-access>.

(收稿日期: 2017-08-28)