基于物联网的通信协议优化研究

林建新　屈台洪*
浙江方大通信有限公司　浙江杭州　310012

摘　要：随着信息技术的迅猛发展，物联网（IoT）已成为推动智能化社会建设的重要力量，通信协议作为物联网系统中实现设备间互联互通的核心技术，其性能优劣直接影响整个系统的效率与稳定性。当前，物联网面临设备异构性高、数据量大、应用场景复杂等挑战，传统通信协议在数据传输速率、能耗控制、可靠性和安全性等方面已难以满足实际需求。本文以通信协议优化为研究对象，系统分析了物联网通信架构和主流通信协议的技术特点，探讨其在不同应用场景中的适应性问题，并从数据传输效率、协议协同机制、安全策略等方面提出优化方案，旨在为构建高效、稳定、安全的物联网通信系统提供理论依据与技术支持，为今后的物联网协议标准化与智能化发展奠定基础。

关键词：物联网；通信协议；数据传输效率；协议优化

序言

物联网作为新一代信息技术的重要组成部分，正在广泛渗透到智能交通、智慧医疗、工业制造、智能家居等多个领域。其核心在于通过各种传感器和终端设备感知现实世界，并通过网络实现数据的远程传输与处理。通信协议在其中扮演着至关重要的角色，是连接“感知层—网络层—应用层”的纽带。近年来，虽然众多通信协议如MQTT、CoAP、NB-IoT等在不同场景中得到了广泛应用，但在协议轻量化、异构设备互联、低功耗控制和网络安全保障等方面仍存在诸多不足。本文从技术演进和应用需求出发，系统梳理物联网通信协议的技术体系，并提出具有实际应用价值的优化策略，以期为物联网通信系统的高效运行和可持续发展提供新思路。

一、物联网通信协议技术概述

（一）物联网通信架构简述

物联网通信架构通常由感知层、网络层和应用层三部分组成，各层之间通过通信协议实现数据的交互与协同，感知层主要负责数据的采集与初步处理，涉及各类传感器、标签、控制终端等，其数据需通过网络层上传至应用系统。网络层作为物联网的中枢，承担着数据传输、交换与路由的任务，常用的通信方式包括Wi-Fi、蜂窝网络、LoRa、ZigBee等，还涉及网络拓扑结构设计与数据中继策略[1]。应用层是面向用户的最终交互界面，依据不同领域需求，对接后台数据平台，实现数据分析、远程控制和智能决策等功能。为了实现各层设备的无缝连接和数据协同，必须有一套完善的通信协议体系作为支撑，理想的通信架构应具备高扩展性、强兼容性、低功耗和高安全性，才能适应物联网多场景、多终端的运行需求[2]。

（二）主流通信协议介绍

目前，物联网中常见的通信协议主要包括MQTT、CoAP、ZigBee、LoRa、NB-IoT等，其各具特点并适应不同的应用场景，MQTT是一种基于发布/订阅模式的轻量级协议，适合带宽受限、设备资源有限的环境，广泛用于智能家居和工业监控[3]。CoAP基于REST架构，支持UDP传输，具有传输效率高、功耗低的特点，适用于受限设备间的点对点通信[4]。ZigBee则是一种短距离无线通信协议，适用于低速率、低功耗场景，如家庭自动化系统，而LoRa具有远距离通信能力和良好的穿透性，广泛用于环境监测和智慧农业领域[5]。NB-IoT作为蜂窝网络衍生出的窄带物联网技术，具有覆盖广、连接密度大和低功耗等优势，尤其适用于城市级别的大规模部署。尽管这些协议在性能上各有侧重，但在面对大规模接入、异构

作者简介：
林建新（1983.9-）男，汉族，浙江丽水人，本科，研究方向为通讯技术；
屈台洪（1983.3-）男，汉族，浙江临海人，本科，研究方向为通讯技术。

终端协同、实时性与安全性等挑战时，仍有优化空间。

二、通信协议存在的问题分析

（一）高延迟与低吞吐问题

在物联网应用场景中，通信协议面临的高延迟与低吞吐问题严重制约了系统的实时性和效率。物联网设备通常部署于边缘环境，节点资源受限，网络拓扑复杂，导致数据传输过程中存在多跳路由、链路不稳定、时延累积等问题，进而造成较高的通信延迟。尤其是在大规模设备同时接入的情况下，传统通信协议在调度机制、缓存管理和链路控制方面存在明显不足，难以保证数据传输的连续性和及时性。同时，通信协议的设计往往未充分考虑物联网环境的动态性和多样性，造成协议在处理高并发、大数据量场景下的吞吐能力有限。此外，一些协议为了保证可靠性采用大量确认应答机制，进一步增加了信道占用和通信负担，从而降低了整体吞吐率。这种低效率的传输方式不仅影响系统的响应速度，还影响数据的时效性和业务决策的准确性。因此，优化通信协议，提高其在复杂环境下的数据传输速率和处理能力，是解决物联网实时性问题的关键。

（二）协议适应性差与兼容性问题

随着物联网应用场景的不断拓展，不同设备、平台和网络技术之间的互联互通成为基础需求。然而，现有通信协议普遍存在适应性差与兼容性不足的问题，难以满足异构环境下设备间的高效协同工作。一方面，许多通信协议是为特定场景或设备类型定制开发的，缺乏通用性与灵活性，难以适配多种硬件平台和操作系统。例如，在感知层使用的轻量级协议在向网络层或应用层扩展时，常出现接口不统一、协议栈不兼容等问题，影响了整体系统的集成效率。另一方面，不同厂商设备采用私有协议或未遵循统一标准，使得协议间缺乏互操作性，增加了设备接入的复杂度和系统部署成本。此外，物联网环境变化频繁，网络拓扑动态变化显著，而现有协议对环境变化响应迟缓，缺乏自适应机制，也制约了网络的可扩展性和稳定性。

（三）网络拥塞与数据丢失问题

物联网系统中通常存在大量终端节点在同一时间段内产生数据，尤其是在突发事件或集中上报场景下，极易引发网络拥塞现象。由于通信协议在设计时对并发处理和流量控制机制考虑不足，造成链路资源分配不均，进而引起数据排队等待、延迟增加甚至数据丢失等问题。例如，在使用CSMA/CA等协议机制时，多个节点同时竞争信道，可能出现冲突、退避等待甚至长时间无法访问信道的情况，降低了整体网络性能。同时，缓冲区溢出、队列管理不当也会导致部分数据包在传输过程中被丢弃。此外，在多跳传输和无线链路质量不稳定的环境中，数据包因路径损耗、干扰或信道衰减而丢失的概率大大增加。数据丢失不仅影响物联网系统对环境的准确感知，还可能造成控制命令失效、业务逻辑中断等严重后果。

（四）协议安全性不足问题

物联网设备广泛分布在开放、复杂的环境中，容易成为网络攻击的目标，而现有通信协议普遍在安全性设计上存在薄弱环节。许多轻量级协议为了追求低功耗和简化实现，往往忽略了加密机制、身份认证和完整性校验等安全功能，导致数据在传输过程中易被截获、篡改或伪造。此外，设备间的通信往往缺乏动态密钥更新机制和安全认证流程，使得攻击者可通过中间人攻击、重放攻击等方式对系统造成严重威胁。例如，一旦攻击者伪装成合法节点接入网络，不仅能获取敏感数据，还可能发布恶意指令干扰系统运行。

三、通信协议优化设计与实现

（一）优化设计思路

物联网通信协议的优化设计需从整体架构出发，兼顾低功耗、高效率、强鲁棒性与可扩展性等关键需求。首先，在体系结构上应遵循模块化设计原则，将协议划分为可独立优化的层级模块，便于后续的定制与部署。其次，针对物联网设备资源受限的特点，应优化传输流程，减少通信开销。例如，可通过精简协议头部信息、合并冗余控制帧等方式，提升传输效率。在数据处理层面，采用边缘计算协助处理部分数据，降低网络负载并减少延迟。此外，还需引入自适应机制，根据网络拓扑变化或节点状态，动态调整通信参数，实现协议的智能优化。设计过程中应注重软硬件协同，合理利用硬件特性（如低功耗芯片、节能射频模块）支持协议运行，提升整体系统的运行效率。最后，在兼容性方面，应尽量保留与现有主流通信标准（如MQTT、CoAP、6LoWPAN）的接口，确保优化方案具备良好的可移植性与互操作性，从而满足多样化物联网应用场景的需求。

（二）协议栈压缩与简化策略

为适应物联网中设备资源受限的实际需求，通信协议栈的压缩与简化成为优化设计的核心任务之一。传统的通信协议栈结构较为臃肿，不适用于低功耗、小存储、低计算能力的物联网终端。为此，可通过裁剪非关键功

能模块来减小协议栈体积，例如，删除不常用的头部字段、精简握手机制和异常处理流程等。同时，采用融合协议策略，将多个功能模块集成在同一通信流程中，以减少层间切换带来的处理开销。在协议编码上，可使用二进制压缩表示法替代传统文本协议，从而进一步降低传输数据量和解析复杂度。针对应用层协议，可通过定制轻量级格式如CBOR、EXI等替代传统JSON或XML，减轻负载并提升响应速度。与此同时，为确保简化后的协议仍具备基本功能和扩展性，可设计模块化可插拔机制，支持用户按需加载或卸载功能模块。总体而言，协议栈的压缩与简化不仅显著提升了通信效率，也为低成本、大规模部署奠定了基础。

（三）QoS保障机制

物联网环境中设备异构、应用多样，通信协议在设计中必须集成有效的QoS（服务质量）保障机制，以确保数据传输的可靠性、实时性与公平性。首先，应在协议中划分服务等级，根据业务类型（如环境监测、视频监控、工业控制等）设定不同的优先级队列，从而实现差异化服务。其次，在拥塞控制方面，可采用基于速率控制和队列管理的混合机制，例如使用自适应速率调整算法与队列限流策略，在高流量时避免网络阻塞。针对实时性强的应用，应实现延迟敏感调度机制，如EDF（Earliest Deadline First）调度，保障关键任务优先传输。在数据丢包控制方面，可引入FEC（前向纠错编码）与ACK/NACK机制结合的方式，提升链路可靠性。同时，利用网络状态监测模块对当前网络带宽、丢包率与延迟等参数进行实时分析，动态优化路由与传输策略。综合来看，完善的QoS机制能有效提升物联网系统在多场景、多任务下的稳定性与服务性能。

（四）安全机制改进

物联网通信协议在开放环境下运行，面临诸多安全威胁，如数据窃听、身份伪造、非法接入等，因此必须在协议层面进行有效的安全机制改进。首先，应采用轻量级加密算法（如AES-CCM、ECC等），在确保数据保密性与完整性的前提下，降低资源消耗，适配物联网终端的计算能力。其次，改进认证机制，结合基于对称密钥的快速认证方式与一次性令牌机制（Token），确保节点身份合法性，并防止重放攻击。在关键数据传输环节中，应加入完整性校验与数据签名机制，防止数据在传输过程中被篡改或伪造。此外，为防止非法设备接入网络，应引入基于白名单或信任模型的接入控制策略，实现细粒度的访问管理。安全机制的部署还需兼顾动态更新能力，支持远程补丁升级与密钥轮换功能，提升协议应对新型攻击的适应能力。整体而言，协议层安全机制的优化是构建可信物联网系统的基础，需在轻量化与高防护之间寻求平衡。

结语

综上所述，物联网通信协议作为连接设备、传递数据的核心桥梁，其性能优劣直接决定了整个系统的效率、安全与可扩展性。本文围绕当前通信协议在物联网应用中面临的高延迟、能耗高、兼容性差、安全性不足等问题展开系统分析，并从协议栈压缩、自适应机制、多协议协同与安全增强等方面提出针对性优化策略。根据应用场景灵活设计，能够实现可扩展、高效、低功耗和安全的通信协议体系，进而可以更好支撑物联网的多样化应用与未来的智能演进。

参考文献

[1]张凌哲，朱妤晴，安彦哲等.工业物联网数据管理中的系统负载均衡最优化问题及其求解.中国科学：信息科学，2024，54（10）：2343-2367.

[2]叶竹辉.基于工业物联网通信协议的高炉热负荷监测系统设计研究.工业加热，2024，53（01）：63-65+70.

[3]邵泽华，刘彬，权亚强等.智能制造工业物联网体系研究与分析）.物联网技术，2023，13（04）：140-143.

[4]施昕昕，顾宇扬.基于MQTT协议的工业物联网数据采集和控制系统）.南京工程学院学报（自然科学版），2022，20（02）：31-37.

[5]朱家祺.物联网通信协议转换技术的研究与实现[D].湖北：华中科技大学，2022.