物联网信息跨平台访问控制方法设计

刘 祎[1]
LIU Yi

摘 要 针对物联网部署中节点动态迁移、信道时变衰落及多径效应耦合导致的拓扑高频变动与链路质量剧烈波动等问题，传统访问控制机制在跨平台数据交互中的安全防护与环境适配能力均明显不足。为此，文章提出一种基于 MQTT 协议的跨平台访问控制方法。硬件层面，针对传统控制器在高并发与异构兼容场景下的性能瓶颈，构建了集成访问控制器、业务服务器及控制网关的动态拓扑架构，嵌入并行处理模块与多引擎协同调度机制，提升实时响应与负载均衡能力；软件层面，将用户身份认证与行为时序特征深度融合，建立动态可信度量化评估模型，实现细粒度权限的自适应分配。测试表明，所提方法异常访问平均阻断率达 99.9%，可有效抑制潜在安全风险，兼具控制性能与工程可行性，为物联网跨平台安全接入提供软硬件协同优化的理论与技术参考。

关键词 消息队列遥测传输；物联网；跨平台访问；访问控制；可信度评估；动态权限

doi：10.3969/j.issn.1672-9528.2026.06.024

0 引言

物联网推动了物理实体与数字空间的深度融合，已成为智能制造与智慧城市建设的关键底层技术。然而，实际部署中终端节点的高移动性导致网络拓扑持续动态重构，叠加无线信道时变衰落与多径传播的耦合干扰，通信链路呈现明显随机波动特征，由此引发越权访问、恶意入侵及数据泄露等安全风险，在跨平台异构传输场景中尤为突出。

访问控制作为数据访问权限管理的核心屏障，已成为物联网安全研究热点。邓三军等 [1] 基于用户 - 角色信任演化实现权限动态调控并引入区块链存证，但敏感策略存在外泄隐患；张杰等 [2] 利用智能合约管控终端接入，但泛在接入加剧信道扰动，滋生新脆弱点；张江徽等 [3] 构建了智能合约驱动的 FACP 框架，受限于合约逻辑复杂度，易引入代码漏洞，扩大攻击暴露面。上述研究多聚焦策略模型与架构优化，较少兼顾硬件承载能力与动态信任评价的协同设计，难以在高并发与拓扑实时变迁场景下兼顾性能与安全。

针对上述不足，本文提出一种基于 MQTT 协议的跨平台访问控制优化方案。硬件层面，针对传统控制器在高并发与多协议异构场景下的性能瓶颈，构建集成访问控制器、业务服务器与控制网关的一体化动态架构，引入并行处理单元与多引擎协同调度机制，提升实时响应与负载均衡能力；软件层面，融合身份核验信息与在线行为监测数据，建立动态可信度量化评价模型，以信任等级驱动细粒度权限的自适应分配，实现复杂时变环境下高精度、自适配的安全访问管控。

1 物联网访问权限控制问题分析

访问控制机制的运行效能与安全防护水平高度依赖底层硬件架构的承载能力。在动态异构的物联网环境中，传统硬件设计在高并发请求处理、动态信任运算及跨协议适配等方面存在显著局限 [4]。本文结合系统核心组件架构，对上述硬件层面的技术瓶颈进行系统分析与论证。

1.1 控制器集中化瓶颈与性能固化问题

访问权限控制器其架构的合理性直接影响系统效能。如图 1 所示，该控制器采用集成模块化设计，虽便于功能划分与统一调度，但在架构层面仍存在制约性能的固有缺陷。

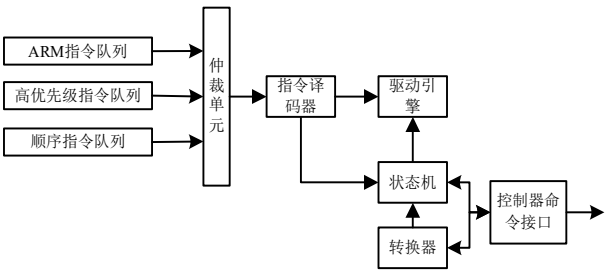

图 1 访问权限控制器架构图

从图 1 可以看出，控制器的数据处理与权限判决集中于核心模块。在物联网高并发场景下，海量的访问请求集中涌向控制器，极易导致单点处理延迟甚至过载，成为系统性能的天花板，形成集中化处理瓶颈。该架构展现了清晰的逻辑

1. 陇南市卫生学校 甘肃陇南 746041

控制流，但缺乏实时、细粒度的信任反馈通道。这导致其权限判决多依赖于预设的静态策略，难以融入用户行为的实时动态信息，无法应对物联网中因位置、信号质量变化而引发的信任波动，从而难以实现精准的访问控制，形成僵化的权限判决瓶颈。

1.2 控制网关协议转换与边界安全风险

控制网关承担内外网数据交互中转职能，其安全稳定性直接影响物联网边界防护效能，详细架构如图 2 所示。

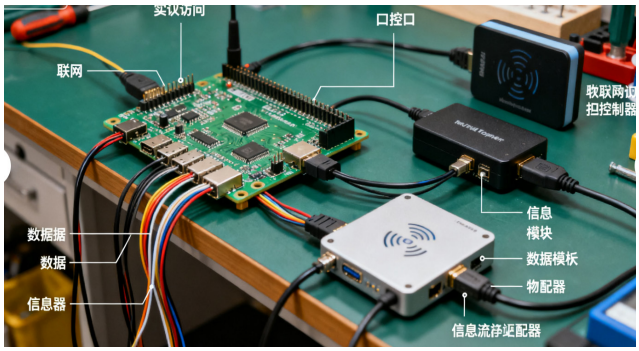

图 2 访问权限控制网关组成结构图

图 2 显示，协议转换环节存在显著安全隐患。网关经串口连接单片机，负责异构数据至标准协议的转换，涉及解析与重组等复杂逻辑。信道波动易致解析异常，攻击者可借此构造畸形报文实施协议层渗透，威胁内网安全 [5-6]。

1.3 网络处理器负载处理与动态适应能力挑战

图 3 展示了其多引擎并行处理的框架。多 RISC 引擎虽具有良好报文吞吐能力，但因终端数量动态变化导致请求分布不均，固定负载分配机制无法自适应感知引擎实时负荷，难以智能分发任务至空闲单元，引发部分引擎过载而其余资源闲置的配置失衡，制约了并行架构优势的发挥。此外，现有引擎以高速转发为核心目标，缺乏安全上下文感知能力，无法与上层信任判定等安全策略协同联动，既不能识别高危会话实施优先级管控，也无法将行为特征回传至信任评估模块，导致精细化权限判定缺乏数据支撑。

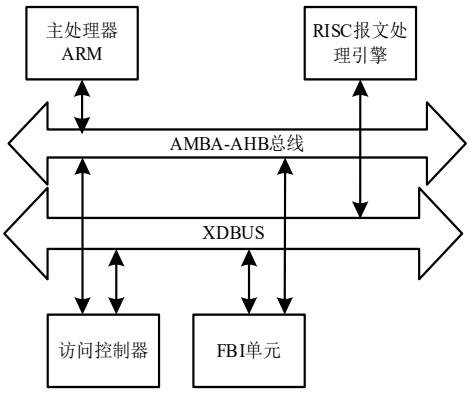

图 3 网络并行处理器框架图

2 访问权限控制方法设计

基于此前对集中式架构瓶颈、协议转换安全隐患及动态负载调度问题的系统分析，提出融合 MQTT 协议与动态可信度检测模型的访问控制方案，旨在突破静态粗粒度权限判定局限，构建与硬件处理能力匹配、可实时响应环境波动的动态细粒度访问控制机制。

2.1 基于 MQTT 的跨平台访问流程建模与轻量化卸载

为解决控制网关在协议转换中面临的安全风险与性能压力，并减轻控制器集中处理的负担，本方法首先在访问流程层进行优化。引入消息队列遥测传输协议 作为跨平台交互的统一通信标准。MQTT 协议采用发布 / 订阅模式，实现了信息交互的解耦，使得物联网设备（发布者）与访问申请终端（订阅者）无需直接建立点对点连接，从而从架构上降低了因动态拓扑和直接连接带来的安全风险。基于此，对物联网信息的跨平台访问过程进行形式化建模。该过程描述了用户访问申请与物联网信息交付之间的逻辑关系：

$$x_{\text{access}}=\begin{cases}0,U_{\text{not allow}}\\ \kappa_{\text{transmit}}x_{\text{Industrial networking}},U_{\text{allow}}\end{cases} \tag{1}$$

式中：κ_{transmit} 为传输系数，$x_{\text{Industrial networking}}$ 和 x_{access} 分别为物联网的实际工作数据与访问获取数据，$U_{\text{not allow}}$ 和 U_{allow} 分别为未通过访问申请以及通过访问申请的用户。按照上述流程，完成对物联网信息访问。

2.2 访问用户可信度检测

在物联网访问过程中，通过消息队列遥测传输协议的设定可以确保信息访问的安全性。然而，仅仅依靠协议本身可能不足以有效防止非法访问和安全威胁 [7-8]。为了更好地保障访问的可靠性和安全性，可信度检测起到了重要的作用，在访问申请过程中，用户需要同时满足物联网以及用户所在通信网络的身份安全认证，并检测用户在网络环境中的行为，从而计算访问用户的可信度。用户身份认证是通过身份验证系统验证自己的身份，确保自己的身份与访问申请中填写的身份匹配，并与对方交换会话密钥 [9]。用户的身份认证结果可表示为：

$$s_{\text{identity}}=x_{\text{access}}\frac{\psi_{\text{apply for}}\cdot\psi_{\text{verification}}}{\left\|\psi_{\text{apply for}}\right\|\cdot\left\|\psi_{\text{verification}}\right\|} \tag{2}$$

式中：变量 $\psi_{\text{apply for}}$ 和 $\psi_{\text{verification}}$ 分别对应的是申请身份信息和验证身份信息，若式（2）的计算结果高于阈值 s'_{identity}，则证明当前用户通过身份认证环节，否则认为用户身份存在异常，不予通过，直接退出信息跨平台访问程序，此时直接输出用户可信度为 0。结合用户身份与用户行为的检测结果，得出用户可信度的检测结果为：

$$\gamma = \left| s_{\text{behaviour}} - s'_{\text{behaviour}} \right| \otimes \left| s_{\text{identity}} - s'_{\text{identity}} \right| \quad (3)$$

通过式（3）的计算，得出用户可信度参数的计算结果。

2.3 确定访问权限实现访问控制

依据用户可信度量化结果，划分信任层级并研判安全风险，驱动访问控制策略动态优化。针对不同信任层级用户，实施细粒度行为分类，对高危操作施加额外安全约束，以压缩威胁影响范围并兼顾合法访问需求。用户信任等级量化求解过程可表示为：

$$J = \begin{cases} J_1, \gamma \in [0.75, 1] \\ J_2, \gamma \in [0.5, 0.75] \\ J_3, \gamma \in [0.25, 0.5] \\ J_4, \gamma \in [0, 0.25] \end{cases} \quad (4)$$

式中：J_1、J_2、J_3 和 J_4 分别表示用户信任的四个等级，将式（3）的计算结果代入到式（4）中，即可确定用户的信任等级[10]。若用户信任等级为 J_1，则直接对其进行信息访问授权，否则不予对用户赋予访问权限。

3 实验分析

3.1 实验环境搭建

以验证优化设计基于消息队列遥测传输的物联网信息跨平台访问控制系统的访问控制功能与运行性能为目的，设计系统测试实验。布设的物联网覆盖面积为 320 ㎡。通过平台的覆盖面积大小不一，内部包含的用户数量也存在较大差异。根据覆盖面积为 320 ㎡，布设 6 个传感器，每个传感器覆盖面积为 50 ㎡，该传感器的精度为 ±0.5，分辨率为 0.1。硬件软件设备如图 4 所示。

图 4 硬件软件设计图

硬件环境，采用 30 个 ESP32 微控制器模块，模拟不同类型的物联网设备（如温度、湿度、光照、门磁传感器及智能执行器）。每个 ESP32 均集成 Wi-Fi 模块，以模拟无线动态接入。边缘处理层的访问控制网关采用树莓派 4B（4 GB 内存）充当，负责运行 MQTT Broker（Mosquitto）、协议转换及初步的访问过滤功能。攻击模拟终端使用 3 台高性能台式机（Intel i5-12600KF, 16 GB RAM），安装 Kali Linux 系统，用于模拟异常用户和发起各类攻击流量。软件与网络环境中通信协议采用设备与网关间采用 Wi-Fi IEEE 802.11ac 标准。测试工具使用 Python 编写的自动化测试脚本模拟正常用户访问行为；使用 Metasploit 框架和自定义脚本模拟恶意攻击。

3.2 实验参数设计

实验参数的设计旨在覆盖物联网典型应用场景，并充分考验系统的安全与性能边界。系统负载参数模拟的正常用户并发数梯度设置为：100、500、1 000、2 000。每位用户会话期内，访问请求的发包频率模拟为泊松分布，均值 λ=10 包 / 分钟。MQTT 消息平均大小为 512 B。可信度评估参数中的身份认证阈值设置为 0.85。低于此值则认证失败。行为特征权重中历史访问成功率（权重 0.4）请求频率异常度（权重 0.3）访问时间规律性（权重 0.3）。性能评估指标：安全性指标：异常用户访问成功拦截率、系统风险参数（根据未拦截的异常请求数量与严重程度综合计算）。

物联网在工作状态下，每小时能产生 2 GB 信息，以此作为待访问的物联网信息样本。部分物联网信息样本的生成结果如图 5 所示。

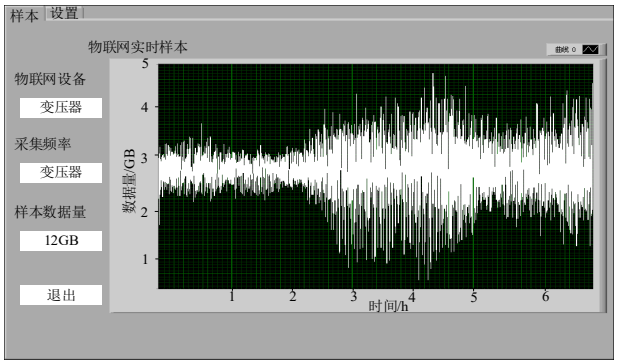

图 5 物联网信息样本示意图

图 5 展示了物联网在运行状态下生成的信息样本结构，反映了系统处理的数据类型、格式与规模。根据文中描述，物联网每小时产生约 2 GB 信息，表明系统处理的是高吞吐量、实时性强的流式数据。图中样本可能包含多源异构数据（如传感器读数、设备状态、用户请求等），体现了物联网环境的典型特征——多模态、高维度。该样本作为实验输入，用于测试系统在真实数据流下的处理能力，尤其是访问控制机制对数据包的解析、过滤与转发性能。每小时 2 GB 的数据量对存储系统和实时处理引擎提出了更高要求，进一步凸显了本文提出的网络并行处理器与多引擎机制的必要性。

通过相关数据的统计，得出异常用户访问成功拦截率的测试结果，如图 6 所示。图中对比了三种系统（RBAC、TBAC、本文系统）在异常用户访问拦截率方面的表现。结果显示：RBAC 系统平均拦截率：94.3%。TBAC 系统平均拦

截率：97.6%。本文系统平均拦截率：99.9%。本文系统在拦截率上接近完美（99.9%），说明其动态可信度评估机制能有效识别并阻断恶意行为。相比静态角色或信任模型，本文系统通过实时行为分析 + 身份认证，实现了细粒度、自适应的访问控制。该结果基于高并发、多攻击场景，具有较强的现实代表性和说服力。

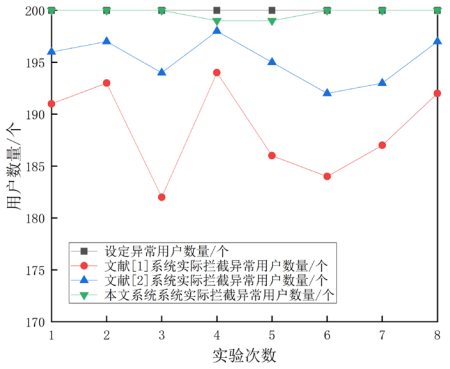

图 6 异常用户访问成功拦截率测试数据表

另外，在系统控制作用下，通过相关数据的统计与计算，得出物联网的风险测试结果如图 7 所示。

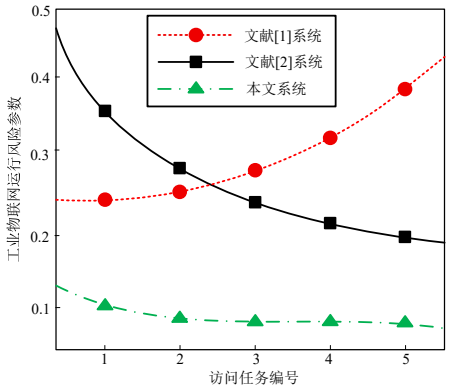

图 7 控制系统作用下物联网风险测试结果

图 7 展示了三种部署模式下风险参量的演化对比。结果表明，所提架构在未拦截请求数、攻击危害度及系统响应延迟等多维指标上均显著优于 RBAC 与 TBAC 模型。较低的风险水平反映出方案在持续攻击环境下仍能维持业务平稳运行，具备优异的抗干扰与抗入侵能力。其本质源于底层并行处理单元与上层动态信任评估机制的协同增益。对于智能制造、智慧城市等高安全等级场景，长期维持低风险运行状态是评判系统工程可行性的关键指标。

4 结语

针对物联网终端高移动性与拓扑动态变化引发的跨平台访问控制难题，本文提出融合 MQTT 协议与动态可信度评估的协同管控策略。核心创新在于弥合硬件计算能力与软件管控策略间的协同脱节：硬件层构建集成网络并行处理单元与多引擎调度的控制体系，显著提升实时响应与负载均衡性能；软件层深度融合身份认证与行为特征数据，建立量化动态可信度评价模型，实现从静态角色授权向动态细粒度权限管控的转变。

参考文献：

[1] 邓三军，袁凌云，孙丽梅．基于信任度的物联网访问控制模型研究 [J]. 计算机工程与设计 ,2022,43(11):3030-3036.

[2] 张杰，许姗姗，袁凌云．基于区块链与边缘计算的物联网访问控制模型 [J]. 计算机应用 ,2022,42(7):2104-2111.

[3] 张江徽，崔波，李茹，等．基于智能合约的物联网访问控制系统 [J]. 计算机工程 ,2021,47(4):21-31.

[4] 李玲，王峥，李娜．雾计算中支持计算外包的访问控制方案 [J]. 计算机工程与应用 ,2021,57(6):81-87.

[5] 宋丽华，朱宗科，李梦晨，等．基于区块链的细粒度物联网访问控制模型 [J]. 计算机工程与设计 ,2022,43(2):352-360.

[6] 韩宗芮，郭渊博，秦晰．基于 NGAC 的物联网访问控制授权方案 [J]. 小型微型计算机系统 ,2022,43(9):1968-1975.

[7] 王思源，邹仕洪．多域物联网中基于区块链和权能的访问控制机制 [J]. 应用科学学报 ,2021,39(1):55-69.

[8] 巩坪，王九如，宋万水，等．基于智能合约的物联网权限传递访问控制模型 [J]. 郑州大学学报 (理学版), 2023, 55(3): 28-33.

[9] 林莉，储振兴，刘子萌，等．基于区块链的策略隐藏大数据访问控制方法 [J]. 自动化学报 ,2023,49(5):1031-1049.

[10] 董建军，樊建伟．物联网内节点信任传递能耗智能感知仿真 [J]. 计算机仿真 ,2024,41(7):442-446.

【作者简介】

刘祎（1989—），女，甘肃陇南人，本科，中职讲师，研究方向：计算机应用基础、人工智能。

（收稿日期：2025-10-20 修回日期：2026-06-04）