周报 向嘉豪(2025-11-17)

摘要: 本周完成了论文三个维度的系统化改进工作。新增 Implementation Architecture 章节，描述 MQTT 发布-订阅拓扑、硬件平台、软件架构、TLV 消息格式、密钥管理和错误处理机制。增强 Experimental Methodology 章节，、编译器优化分析、网络参数、环境控制、栈水印方法、载荷分布论证、统计措施，阐述五个创新方法论框架（DWT 硬件剖析±1 周期精度、多维资源特征化、六阶段协议层评估、多阶段延迟归因、度量框架）。完成全文学术语言优化，转换被动语态，消除口语表达，提升数值精度，统一时态。

下周计划: 1) 优化实现架构以提升 ML-DSA 签名操作性能 2) 论文 Results and Analysis 章节的深入分析和讨论部分撰写

1 实现架构章节撰写

完成了 Section 3 Implementation Architecture 章节撰写，从系统层级、硬件平台、软件架构和协议集成四个维度描述 ML-DSA 签名集成在 MQTT 通信框架中的实现架构。系统架构描述了 MQTT 发布-订阅拓扑在引入 ML-DSA 签名认证后的消息流程，包含发布者设备（签名生成）、MQTT 代理（消息路由）和订阅者设备（签名验证）三个组件。该架构实现端到端密码学认证，ML-DSA 签名嵌入 MQTT 载荷内部，提供独立于传输层的不可否认性和身份认证能力。硬件平台采用 STM32F407VG（ARM Cortex-M4F，168 MHz，1 MB Flash，192 KB SRAM）配合 ESP32-WROOM-32 无线模块（UART 115,200 波特率，IEEE 802.11n WiFi），电源架构包含 3.3V±1% 稳压和 INA219 电流传感器（12 位分辨率，±0.8 mA 精度）支持能耗剖析。软件架构分层设计包含 HAL 硬件抽象层、FreeRTOS 任务调度、pqm4 密码学库（ML-DSA-44/65/87 参数集）和 Paho MQTT 客户端（MQTT 3.1.1 协议）。密码学库导出 crypto_sign_keypair()、crypto_sign()、crypto_sign_verify()三个核心 API。消息格式采用 TLV 编码封装传感器数据和签名，密钥管理使用预分发模型配合 Flash 读保护机制，错误处理覆盖签名失败、连接中断和超时场景（指数退避重连：1-60 秒，5 秒超时）。

2 实验方法论章节增强

完成了 Section 4 Experimental Methodology 章节增强，补充技术参数规格和阐述创新性评估方法论框架。平台选择合理性通过 ARM Cortex-M4 市场数据支撑（38% 份额，127 亿片年出货量），编译器配置采用 GCC -O3（18-23% 速度提升，12-15% 体积增加），网络参数控制 WiFi 信号-45 至-52 dBm 和 0.1% 丢包率，环境规格包括 25°C±2°C 温度、3.3V±1% 电压和 5 分钟热稳定化。栈峰值测量采用 32 字节间隔水印方法（±32 字节精度），载荷选择 10/50/100 字节覆盖 92% 流量（23%/51%/18% 分布），统计措施使用 IQR 检测配合 100 次重复测量（0.8-2.3% 剔除率），QoS 测试规格包含 5 秒超时和指数退避重传（500 毫秒基础延迟，8 秒最大延迟，3 次重传上限）。引入五个创新方法论框架填补后量子密码学 IoT 性能评估空白。硬件辅助剖析利用 DWT 单元实现±1 周期精度的指令级测量，超越软件计时器方法（典型±100 周期精度）。多维资源特征化同时量化 CPU 时间、内存占用和能耗三个维度。协议层评估框架通过六阶段插桩（发布准备、签名开始、签名完成、传输开始、传输完成、验证完成）实现延迟归因，多阶段延迟归因区分计算延迟、网络延迟和系统延迟，度量框架解决现有研究缺乏协议级开销量化、可持续吞吐量测试和多参数集对比的空白。

3 学术语言优化

完成了全文学术语言优化，提升文本规范性和技术精确性，涵盖 Abstract、Introduction、Related Work、Results 等章节，修改类型包括语态转换、口语消除、数值精度提升和时态统一。Abstract 优化聚焦被动语态转换和冗余消除，将“This research evaluates”改为“is evaluated”符合学术惯例，“imminent threat”简化为“necessitate migration”消除修饰词，“remains unexplored”修改为“remains inadequately characterized”避免绝对化，长度从 7 句压缩至 6 句。Introduction 消除口语表达并提升技术精确性，“existential threat”改为“fundamentally undermines”避免夸张修辞，“extend beyond”简化为“extending beyond”提升简洁性，“30-70× size increases”补充“2,420-4,627 bytes”提供完整信息，“creates a critical gap”改为“creates critical challenges”避免口语表达。Related Work 聚焦数值精度和术语规范，“approximately 45% additional”改为“1.45×”消除模糊限定词并统一倍数表达，“migrating to newer cores”改为“migration to newer cores”使用名词短语提升学术性，“keeping near the edge”改为“positioning at the threshold”采用技术术语。Results 针对时态一致性和表述精确性，统一使用一般现在时替代混用的现在时和将来时，“reduce latency”补充“maintain in tens-of-milliseconds regime”提供具体时间范围，“substantially exceeding”改为“exceeding sub-second latency constraints”替换模糊表述，消除“firmly”和“acceptable”等冗余修饰词。