周报 向嘉豪(2025-12-29)

摘要: 本周完成 ML-DSA 论文核心技术贡献扩展，新增 Adaptive Security Level Selection Protocol 章节，提出基于消息关键性与设备资源状态的自适应安全级别选择协议。重点工作包括：自适应协议算法设计与形式化描述、消息关键性分类体系建立、资源状态评估模型构建、以及协议性能评估实验设计与结果分析。

下周计划: 1 月 5 日(下周一)为博士复试，望请假一周

1 Adaptive Security Level Selection Protocol 设计

完成了自适应安全级别选择协议的完整设计与形式化描述。协议核心思想为根据消息关键性、设备资源状态和运行上下文动态选择 ML-DSA 参数集，解决固定最高安全级别配置在异构 IoT 部署中造成的资源浪费问题。

协议设计遵循三项原则：Message Criticality Classification 将消息按安全敏感度分类，高关键性消息获得更强加密保护；Resource-Aware Selection 根据设备资源状态（电池电量、可用内存、热状态）影响参数选择，防止资源耗尽；Minimum Security Guarantees 强制执行每类消息的最低安全级别，确保自适应选择不会将安全性降低至应用定义阈值以下。

2 消息关键性分类体系

建立了四级消息关键性分类体系。Critical 级别（固件、凭证、密钥）强制使用 ML-DSA-87; High 级别（告警、配置、命令）默认 ML-DSA-87，资源受限时允许降级至 ML-DSA-65；Medium 级别（聚合数据、状态报告）默认 ML-DSA-65，最低 ML-DSA-44；Low 级别（常规遥测、心跳）使用 ML-DSA-44 作为默认和最低级别。

消息关键性通过 MQTT 主题层次结构静态分配：`device/{id}/critical/*`用于固件和凭证，`device/{id}/alert/*`用于安全事件，`device/{id}/telemetry/*`用于常规传感器数据。此静态分类避免逐消息开销，同时支持细粒度安全策略。

3 资源状态评估模型

构建了综合资源评分模型量化设备可用计算能力。模型监控三个资源维度：Energy State (E)为归一化电池电量，直接影响可持续签名吞吐量；Memory Availability (M)为相对于 ML-DSA-87 需求（43.1 KB）的可用 SRAM 归一化值；Thermal State (T)为归一化处理器温度。

综合资源评分$R = \alpha \cdot E + \beta \cdot M + \gamma \cdot (1 - T)$，其中权重系数$\alpha$、$\beta$、$\gamma$为部署特定参数。默认配置采用$\alpha = 0.5$、$\beta = 0.3$、$\gamma = 0.2$，优先考虑电池供电部署的能源节约。

4 自适应选择算法实现

完成了 Algorithm Adaptive-ML-DSA-Select 的形式化描述。算法首先从 MQTT 主题层次结构检索消息关键性，查找对应的最低和默认安全级别。资源评分R从当前设备状态计算。Critical 消息绕过资源选择，始终使用 ML-DSA-87。非关键消息根据资源评分阈值确定参数选择：高资源可用性（$R \geq 0.7$）允许默认安全级别，中等可用性（$0.4 \leq R < 0.7$）触发一级降级，低可用性（$R < 0.4$）选择最低安全级别。内存约束施加硬性覆盖。

协议开销包括主题字符串解析（12–18 μs）、资源状态采样（8–15 μs）和选择算法执行（3–5 μs），总计 23–38 μs 每消息，占 ML-DSA-44 签名延迟的 0.006% 以下。

5 协议性能评估

完成了三种代表性 IoT 工作负载的协议评估。Environmental Monitoring 工作负载（80% 低关键性遥测）实现 35.6–41.2% 签名延迟降低；Industrial Control 工作负载（60% 低关键性状态更新）实现 25.3–34.6% 降低；Security-Sensitive 工作负载（40% 低关键性遥测）实现 15.8–25.4% 降低。

能耗分析显示，对于每日传输 100 条认证消息的设备，自适应协议节省 0.90–2.02 J/天，转化为 18.8–55.2% 电池寿命延长。Environmental Monitoring 部署实现最大收益，将运行寿命从 4,190 天（固定 ML-DSA-87）延长至 6,503 天（自适应），代表 6.3 年额外运行时间。