工业物联网边缘控制系统轻量级认证方案

尚文利[1]，温旭东[1]，陈卓[1]，熊文泽[2]，常志伟[1]，曹忠[1]
[1]广州大学电子与通信工程学院，中国广州市，510006
[2]机械工业仪器仪表综合技术经济研究所，中国北京市，100055

摘要：在边缘控制系统中，边缘计算需要更强的本地数据处理能力，而传统的工业可编程逻辑控制器无法满足这一需求。因此，边缘智能控制器得到发展，其安全可靠的运行至关重要。然而，由于边缘智能控制器需与资源有限的终端设备进行敏感信息通信，且在终端设备上实现传统的非对称加密具有挑战性，因此迫切需要一种低成本、高效的身份验证解决方案。本文使用低计算成本的哈希函数和异或运算为边缘控制系统设计了一种轻量级身份验证方案；该方案可在边缘智能控制器与终端设备之间实现双向匿名身份验证和密钥协议，以保护设备隐私。安全性分析证明该认证方案可提供必要的安全特性并抵御主要的已知攻击。性能分析和比较表明，所提方案在边缘控制系统中的部署可行、有效。

关键词：边缘智能控制器；边缘控制系统；终端设备；匿名认证；轻量级认证
https://doi.org/10.1631/FITEE.2400497