 DOI: https://doi.org/10.12349/iser.v6i3.5210

Cross domain scheduling security authentication algorithm for large-scale complex heterogeneous industrial control networks

Dongzhou Shen

Shanghai Haibo Science and Technology Co., Ltd., Shanghai, 200000, China

Abstract

In the cross domain scheduling security authentication of large-scale complex heterogeneous industrial control networks, GWN gateway node access is mainly used to generate scheduling security authentication quality, which is easily affected by the fuzzy effect of scheduling data access probability, resulting in a high failure rate of authentication scheduling. Therefore, a large-scale complex heterogeneous industrial control network cross domain scheduling security authentication algorithm is proposed. Preset original association conditions and calculate authentication similarity, consider the same type of data state to calculate scheduling data access probability, generate authentication basis functions, determine authentication protocol processing parameters, and generate heterogeneous industrial control network cross domain scheduling authentication contracts; Sensitive protection is implemented, and a cross domain scheduling security authentication model is constructed by combining authentication contracts to obtain authentication sets and authentication trust relationships. The direct trust degree and inter domain entity trust degree are calculated and mapped for judgment. Fuzzy technology is used to normalize and adjust the trust degree, completing cross domain scheduling security authentication for complex heterogeneous industrial control networks. The experimental results show that the proposed algorithm has a consistently low scheduling failure rate for different malicious node ratios after application, with no abrupt scheduling events occurring and possessing authentication integration integrity.

Keywords

large-scale complex heterogeneous industrial control network; Cross domain scheduling; Security certification; Authentication algorithm; Trust calculation

大规模复杂异构工控网络跨域调度安全认证算法

沈东舟

上海海勃数科技术有限公司，中国 · 上海 200000

摘　要

大规模复杂异构工控网络跨域调度安全认证中，主要采用GWN网关节点访问生成调度安全认证质量，易受调度数据访问概率模糊作用影响，导致认证调度失败率过高。因此，提出大规模复杂异构工控网络跨域调度安全认证算法。预设原始关联条件并计算认证相似度，考虑同类型数据状态计算调度数据访问概率，生成认证基础函数，确定认证协议处理参量，生成异构工控网络跨域调度认证合约；进行敏感保护，结合认证合约构建跨域调度安全认证模型，获取认证集合与认证信任关系，计算直接信任度和域间实体信任度并进行映射判断，结合模糊技术进行信任度归一化调整，完成复杂异构工控网络跨域调度安全认证。实验结果表明，所提算法应用后不同恶意节点比率的调度失败率始终较低，无突变调度事件发生，具有认证集成完整性。

关键词

大规模复杂异构工控网络；跨域调度；安全认证；认证算法；信任度计算

1 引言

大规模复杂异构工控网络是一种提供高效工业通信服务的特殊集成网络，主要以光纤、无线电波技术作为基础，遵循 Modbus 等协议，整体覆盖面积较广，灵活度较高，在智能制造、智慧工厂等领域应用广泛。研究表明 [1]，影响复杂异构网络调度的因素较多，包括资源限制与能力处理矛盾、网络拓扑结构动态变化、跨域认证与信任等，可能造成基础传输异常，甚至出现严重的工控网络安全事故，因此，研究大规模复杂异构工控网络跨域调度安全认证算法是目前的必要选择。

李莉等 [2] 提出基于 AKA 的网络跨域调度安全认证算法。其主要采用轻量级密码算法进行加密传输处理，调整信息传输的顺序，生成哈希链，结合安全认证状态进行通信修正，获取认证参量，易受属性限制作用影响，导致认证调度

【作者简介】沈东舟（1990–），男，中国上海人，硕士，工程师，从事网络安全研究。

失败率过高。李斌等 [3] 提出基于区块链的网络调度安全认证算法。其主要打破数据孤岛，结合节点信任状态处理通信负载，降低数据丢失破坏影响，再利用相似矩阵计算访问认证概率，建立有效合约，输出有效密文完成网络跨域调度安全认证，其易受数据属性含量变化影响，导致认证调度失败率偏高。赖成喆等 [4] 提出基于卷积神经网络的网络调度安全认证算法。其主要结合获取的调度传感数据进行数字孪生训练，结合主成分分析执行特征训练支持向量机分类器，完成安全认证，易受场景周期变化影响，导致认证调度失败率高。张凌浩等 [5] 提出面向无线传感器网络的网络调度安全认证算法。其主要结合匿名认证要求进行 KSSTI 攻击更新，利用安全会话密钥协商网关，完成 BAN 启发式逻辑分析，满足匿名安全属性要求，易受密钥泄露问题影响，导致认证调度失败率较高。

模糊处理技术可以有效确定认证参数与认证实体之间的转换关系，从本域中进行集中查找，添加候选序列，完成调度任务。因此，本文考虑大规模复杂异构工控网络环境设计了一种有效的网络跨域调度安全认证算法。将 PKI 证书作为核心，设置安全凭证功能，调整身份认证与信任决策参量，判断认证者所处状态，确定是否存在实体交互损害，再通过原始认证环境与给定集合特征进行有效标记，考虑笛卡尔积的积分元素关系生成认证集，获取有效的大规模复杂异构工控网络跨域调度安全认证结果。

2 跨域调度安全认证算法设计

2.1 生成异构工控网络跨域调度认证合约

工控网络跨域调度过程涉及的传播次数较多，且不同类型的调度数据关联性较强。因此，结合认证相似度关系，确定调度数据初始状态，计算认证访问概率，生成异构工控网络跨域调度认证合约。即预设原始关联条件，计算认证相似度 $O(T)$ [6]，如式（1）所示。

$$O(T)=\frac{P}{\left|A(T)\right\|A(Y)\|} \tag{1}$$

公式（1）中，P 代表认证相似系数，$A(T)$ 代表输出状态关系，$A(Y)$ 代表认证矩阵。在大量调度数据传输状态下，认证并行指数会发生变化，可以考虑同类型数据状态计算调度数据访问概率 G_K，如式（2）所示。

$$G_K=O(T)*F\left(U,I\right)+(1-P) \tag{2}$$

公式（2）中，$F\left(U,I\right)$ 代表调度数据外溢比率，由此可以将分散调度数据与其相应的类别对应，降低数据篡改风险，此时获取的认证基础函数 d_β 如式（3）所示。

$$d_\beta=G_K\cdot f_\beta \tag{3}$$

公式（3）中，f_β 代表安全合约执行参数。由此可以将调度安全认证设置为不同的阶段，整合初始化密钥绑定，得到的认证协议处理参量 d_m 如式（4）所示。

$$d_m=lh_j\mathrm{g}d_\beta\left[r\left(k,k_a\right)\right]^2 \tag{4}$$

公式（4）中，l 代表加密属性公钥，h_j 代表 rsa 属性密钥 [7,8]，$r\left(k,k_a\right)$ 代表随机素数，由此可以进行初始化加密。按照对应属性集合完成认证读取，生成的异构工控网络跨域调度认证合约 C_A 如式（5）所示。

$$C_A=W\left(\gamma\times x(\delta)\right)\cdot d_m \tag{5}$$

公式（5）中，W 代表认证读取公钥，γ 代表认证属性集合，$x(\delta)$ 代表调度访问令牌，由此可以衡量调度任务安全等级。结合信度权重确定访问认证重要程度。

由此可以确定调度认证传输编码，结合身份指令认证状态进行逻辑均值判断，为后续的异构工控网络跨域调度安全认证模型构建作参考。

2.2 构建复杂异构工控网络跨域调度安全认证模型

工控网络实际跨域调度环境复杂，认证信任无法保证。因此，本文在考虑实体权限验证问题的基础上，进行敏感保护。结合上述设计的认证合约构建跨域调度安全认证模型，如图 1 所示。

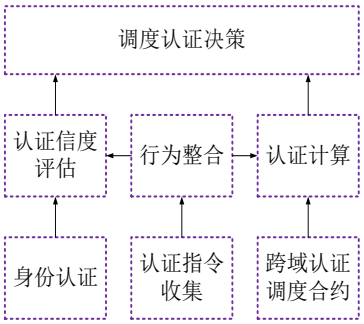


图 1 复杂异构工控网络跨域调度安全认证模型

由图 1 可知，该认证模型主要通过 PKI 证书发挥安全凭证功能，降低身份认证与信任决策影响，判断认证者是否合法，是否存在实体交互损害。

原始认证环境中存在域信任度与实体信任度两个区域 [9,10]，可以按照给定集合特征进行有效标记，考虑笛卡尔积的积分元素关系获取认证集合 D，如式（6）所示。

$$D=\left\{d_1,d_2,...,d_n\right\} \tag{6}$$

公式（6）中，$d_1,d_2,...,d_n$ 代表信任值隶属度元素，此时的认证信任关系示意图如图 2 所示。

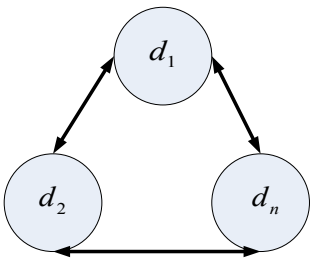


图 2 信任关系示意图

由图2可知，假设某时刻网络跨域调度满足信任度状态，可以立即进行信任度反馈。按照多调度因素权重设置执行契约，计算的直接信任度 $DDTV(d_i)$ 如式（7）所示。

$$DDTV(d_i)=\alpha\times D+\beta\times\varepsilon \tag{7}$$

公式（7）中，α 代表调度需求指数，β 代表调度认证因素权重，ε 代表调度交互参量。若调度信任路径属于推荐信任路径，可以直接按照实体关系进行统一计算，此时的域间实体信任度 y_i 如式（8）所示。

$$y_i=\frac{DDTV(t_i)}{DDTV(d_i)}\times x_j \tag{8}$$

公式（8）中，x_j 代表信任度转换量纲，$DDTV(t_i)$ 代表认证可比常量。受调度关键因素影响，在实际认证过程中 [11-13]，需要满足线性可变与隶属度最大化原则，由此设置模糊关系认证集，按照向量线性变换要求完成论域转换，建立控制因素与权重集，得到认证逻辑中心。认证因素集合主要对安全性、不确定性等风险进行映射判断，得到的信任度映射关系如表 1 所示。

表 1 信任度映射关系

评语集	模糊评语	信任度
v1	完全信任	（0.9999，1]
v2	非常信任	[0.9，0.9999]
v3	信任	[0.6，0.9）
v4	一般信任	[0.3，0.6）
v5	低信任	[0.0001，0.3）
v6	不信任	[0，0.0001）

由表 1 可知，结合上述信任度映射关系可以确定调度认证加权平均算子 [14-15]，生成的工控网络跨域调度安全认证算法的认证优化选择步骤如下：

Step1：域间广度优先搜索，获取可用认证实体；

Step2：按照（8）计算信任度，进行模糊决策对比，将结果降序排列；

Step3: 进行实体信任度转换，使其满足标准信任度要求，结合认证参数完成调度选择；

结合上述认证不好走可以实现本域调度认证实体查找，结合模糊技术进行信任度归一化调整，最大程度上降低调度安全认证失败率

3 实验验证

3.1 参数与准备

选取 KSSTI 作为实验攻击模型，进行集中通信处理，搭建基础测试环境，参数如表 2 所示。

由表 2 可知，上述参数满足调度数据的回传要求，循序实验数据权限判断效果。设置的 a~f 调度类型资源的攻击者需要满足公开信道监听与实体交互标准，且需要预设空间元素基本对称密钥。

按照上述执行代码可以计算信任度初值，建立调度安全认证集合，通过 CVE 漏洞库获取实验构件，实验构件的版本参数如表 3 所示。

表 2 基础测试环境

内容	参数
操作系统	Ubuntu1-128 bit
开发工具	Eclipse JUNO Android Studio4.2.2 Sublimetext MySQL Workbench
内存	Intel（R）Core（RM）I10
CPU	128GB

表 3 实验构件版本参数

构件	参数
处理中心	AliCloud:Yitian 710 TencentCloud HuaweiCloud
操作系统	Ubuntu 18.04 CentOS 7.1804 Windows_Server 2016 1803
编程语言	Java 1.8 Python 3.5.0 Python 3.5.0
数据库软件	MySQL 8.0.1 SQL_Server 2019 Oracle Database Server

由表 3 可知，结合上述版本参数可以生成复杂异构实验执行体，进行服务器初始化，在满足调度周期的基础上执行实验任务，输出跨域调度安全认证结果。

3.2 复杂异构工控网络跨域调度安全认证进程结果

将 CLC 作为初始执行指令，完成 n 模幂运算，结合 Diffie-Hellman 完成密钥交换。此时结合 Java 进行集中处理，调整数组为 MODP，素数发生器参量设置为 2，在满足云环境的基础上执行 RSA 进行安全认证。

上述跨域调度安全认证进程执行状态良好，满足密钥交换要求，未出现认证序列异常问题，由此可知，研究的跨域调度安全认证算法性能良好。

3.3 复杂异构工控网络跨域调度安全认证响应结果

按照认证需求设置统一环境，生成原始认证调试码，进行权限回传，使用的空间采样基本单元为 shuffleNetV2，分割分支为 bottlenet 单元。进行多维度重置，在不同攻击模式下得到的复杂异构工控网络跨域调度安全认证响应结果如图 3 所示。

由图 3 可知，在不同攻击模式下，研究方法的调度安全认证响应时间较短，满足预设标准时间要求，由此可知，研究算法具有高反馈响应鲁棒性。

3.4 工控网络跨域调度安全认证调度失败率性能结果

使用 $simgrid/examples/msg 的 masterslave2.c 目录修改跨域调度认证程序，在满足 sched_struct.c 编码的基础上设

置若干个调入任务，按照调度资源类型编号为 a~f，结合临界值与调度域状态调整恶意节点比率，得到的工控网络跨域调度安全认证调度失败率性能结果如图 4 所示。

由图 4 可知，本文利用模糊处理技术确定调度关键因素，结合认证过程中的线性可变与隶属度最大化原则设置模糊关系认证，按照向量线性变换要求完成论域转换，建立控制因素与权重集，得到认证逻辑中心。在不同恶意节点比率下，研究算法的调度失败率始终较低，且随恶意节点比率增加无突变调度事件发生，证明研究算法能有效完成调度安全认证，满足随机认证安全要求，具有认证集成完整性。

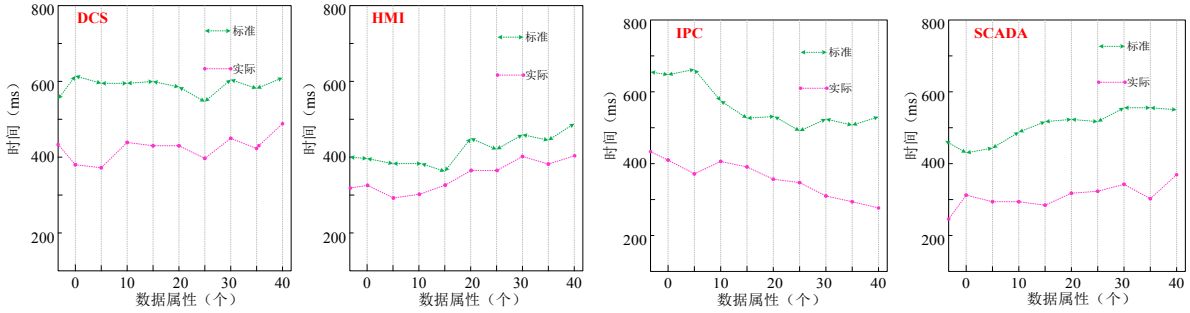


图 3 复杂异构工控网络跨域调度安全认证响应结果

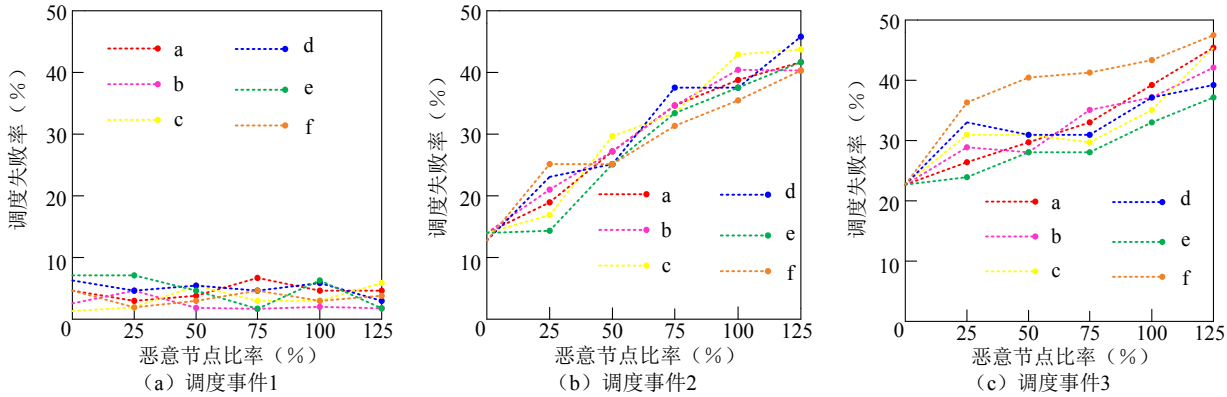


图 4 网络跨域调度安全认证调度失败率性能结果

4 结语

大规模复杂异构工控网络跨域调度安全认证不仅能保证网络安全，降低数据传输过程中存在的身份冒用等风险，由合法用户执行数据访问传输过程，还可以优化调度流程，尽量降低不必要的认证开销。将模糊处理技术与网络跨域调度安全认证融合，可以获取安全特征参数，完成认证匹配，提高调度均衡性，为提高网络综合性能，保证调度传输稳定效果做出了一定的贡献。

参考文献

[1] 张帅亮,杜秀娟,刘昕.基于混沌映射的无线网络环境三因子身份认证协议[J].计算机应用与软件,2024,41(10):349-356+397.

[2] 李莉,马璐瑶,李秀滢.基于AKA的轻量级天地一体化网络终端接入认证方案[J].计算机应用与软件,2024,41(7):309-314.

[3] 李斌,何辉,赵中英,等.基于区块链的多源网络大数据安全访问权限认证仿真[J].电信科学,2024,40(2):107-115.

[4] 赖成喆,张鑫伟,李冠颉,等.基于卷积神经网络的车载数字孪生持续认证方案[J].通信学报,2023,44(11):151-160.

[5] 张凌浩,梁晖辉,邓东,等.面向无线传感器网络的多因素安全增强认证协议[J].电子科技大学学报,2023,52(5):699-708.

[6] 郑路,冯涛,苏春华.基于CPN的车载网络无证书匿名认证和密钥协商方案研究[J].通信学报,2024,45(6):101-116.

[7] 王钺程,朱友文,张志强.无人机网络中基于无证书的群组认证密钥协商协议[J].工程科学与技术,2025,57(1):213-224.

[8] 张楦杰,张敏,刘韬,等.基于区块链的无人机网络跨域身份认证研究[J].计算机应用研究,2024,41(7):1959-1964.

[9] 薛激光,王珺,张笑怡,等.一种低压台区本地HPLC+RF双模自组织通信网络身份认证方法[J].电测与仪表,2024,61(1):219-224.

[10] 张闯,杨昆.一种用于UAV辅助蜂窝网络的基站对无人机群的安全认证协议[J].火力与指挥控制,2023,48(12):94-99.

[11] 陈楠,田立勤,毋泽南,等.基于改进贝叶斯网络的电商用户行为认证方法[J].计算机应用与软件,2023,40(8):330-336.

[12] 张晓均,王文琛,付红,等.智能车载自组织网络中匿名在线注册与安全认证协议[J].电子与信息学报,2022,44(10):3618-3626.

[13] 张毅,吴奇,周霜霜,等.一种面向低轨卫星网络的高效无证书身份认证方案[J].计算机应用研究,2022,39(10):3151-3155.

[14] 张应辉,胡凌云,李艺昕,等.空间信息网络中基于动态撤销机制的安全高效批量认证方案[J].通信学报,2022,43(4):164-176.

[15] 王宝亮,代佳增.6LoWPAN网络中移动集群的边缘认证切换方法[J].计算机仿真,2022,39(3):371-376.