网络环境的计算机信息安全防护体系研究

李 静[1]
LI Jing

摘 要 为解决虚拟网络环境下计算机信息安全防护机制单一、协同性差等问题，文章提出了一套基于分层模型的智能化安全防护体系。该体系通过网络边界层的 CNN-LSTM 混合模型实现工业协议异常识别，工控网络层的 BiGRU-Transformer 模型进行攻击序列检测，数据存储层的透明加密与审计机制保护敏感数据，以及用户管理层基于联邦学习的多站点协同防御实现精确访问控制。在某石化企业环氧丙烷装置的实践应用表明，该防护体系能有效识别和阻断异常网络行为，协议异常检出率达 99.7%，攻击序列识别率达 98.2%，权限隔离度达 99.9%，为工业控制系统的安全运行提供了可靠保障。研究成果对提升网络环境下计算机信息系统的整体安全防护水平具有重要的实践意义。

关键词 网络环境；计算机；信息安全；防护体系；工业控制

doi：10.3969/j.issn.1672-9528.2026.02.029

0 引言

随着信息技术与工业控制系统的深度融合，虚拟网络环境已成为现代工业基础设施的重要组成部分。虚拟化技术在提升资源利用效率的同时，也带来了新的安全挑战。传统的单一防护方案已难以应对复杂多变的网络威胁，亟需建立系统化、多层次的安全防护体系。因此，研究基于分层模型的安全防护体系，对提升工业控制系统的安全防护能力具有重要意义。

1. 大庆市第五采油厂第六作业区技术管理室
黑龙江大庆 163513

1 虚拟网络环境概述

随着云计算、软件定义网络（SDN）和网络功能虚拟化（NFV）技术的发展，虚拟网络环境已成为现代计算基础设施的核心形态之一。依托服务器、存储、网络设备等底层物理硬件资源，通过 Hypervisor 等虚拟化层软件动态创建、管理和编排多个相互隔离的逻辑运行单元——虚拟机（VM）或容器[1]。这些逻辑单元如同运行在独立物理设备上，拥有

4 结语

嵌入式计算机多通道数据通信系统通过 DMA 双控制器架构、动态优先级调度算法、通道冲突智能检测等关键技术，有效解决了多通道并发通信的性能瓶颈。实验验证表明，系统在 8 通道并发场景下吞吐量达 125.2 Mbit/s，可用性达 99.9%，DMA 传输效率保持 85.8% 以上，显著提升了多协议融合环境下的通信效率和可靠性。该系统为工业自动化和智能制造领域提供了高效可靠的数据通信解决方案。

参考文献：

[1] 郭福洲 . 通信系统中的嵌入式技术分析 [J]. 电子技术 , 2025, 54(2): 272-273.
[2] 开诚治 , 刘天颀 , 王青东 , 等 . 基于轨道角动量谱分解的多通道水声通信及系统实现 [J]. 南京师大学报 (自然科学版), 2024, 47(1):103-110.
[3] 苏变 , 陈奕建 , 韦耀曜 , 等 . 基于 SPI 与 USMART 的嵌入式通信系统设计 [J]. 电子技术 ,2023,52(9):14-15.
[4] 牟云飞 . 嵌入式无线移动通信系统的研究及开发 [J]. 电子技术与软件工程 ,2021(23):17-18.
[5] 李静 . 一种嵌入式高速通信系统设计与实现 [J]. 电子设计工程 , 2021,29(15):120-123.

【作者简介】

李传明（1989—），男，山东潍坊人，硕士，工程师，研究方向：嵌入式物联网。

吴格（1990—），男，山东青岛人，硕士，工程师，研究方向：通信技术。

（收稿日期：2025-07-14 修回日期：2026-01-28）

专属的操作系统、应用及虚拟网络配置，如虚拟网卡、虚拟交换机、VXLAN/Overlay 网络。虚拟网络的核心特征在于其高度的资源共享性与动态可重构性：物理资源被池化并按需分配，网络拓扑与连接关系可通过软件灵活定义和及时调整，支持虚拟机 / 容器在物理主机间的无缝迁移，有效提高资源的利用率和业务部署的敏捷性。然而，这种灵活性与复杂性也为计算机信息安全带来新的安全挑战 [2]。虚拟化层自身的安全漏洞可能成为攻击者穿透隔离屏障、实施“虚拟机逃逸”攻击的跳板；虚拟机 / 容器间高度密集的“东西向”内部流量，若缺乏细粒度可视性与控制，极易成为横向渗透的隐蔽通道。总体而言，虚拟网络模糊了传统网络边界，攻击面显著扩大且动态变化，对安全防护的深度、自动化水平等提出严苛要求。

2 网络环境下计算机信息安全威胁分析

2.1 典型安全威胁分类

随着虚拟网络环境的广泛应用，计算机信息安全威胁已从单一攻击方式演变为系统性、持续性的综合性威胁。网络攻击已形成完整的地下产业链，攻击手段不断更新，防护难度持续加大 [3]。典型威胁可系统归纳为三类核心形态：一是网络攻击具有明确破坏意图，包括利用僵尸网络发起的分布式拒绝服务（DDoS）攻击瘫痪关键服务，中间人攻击（MitM）劫持或篡改通信数据，以及针对软硬件开发、分发环节的供应链攻击，植入恶意代码实现持久化控制 [4]；二是数据泄露与隐私侵犯风险则源于系统脆弱性与人为因素，表现为内部人员滥用权限或疏忽导致敏感信息外泄，以及应用程序接口（API）设计缺陷或配置错误成为非法数据访问的入口；三是新兴技术场景的伴生风险不容忽视，云计算多租户环境存在资源隔离失效隐患，人工智能模型可能被投毒或用于生成高级钓鱼攻击，区块链智能合约的漏洞则可能直接导致数字资产损失或业务逻辑被恶意操控 [5]。

2.2 威胁演变趋势

威胁形态正呈现持续动态演进态势，呈现三个显著特征：一是攻击实施的高度自动化与工具化趋势明显，攻击者利用人工智能技术优化攻击策略生成、目标筛选和漏洞挖掘效率，地下黑产提供的“攻击即服务”进一步降低了攻击门槛 [6]；二是零日漏洞利用频率激增，从漏洞被发现到被武器化利用的时间窗口持续缩短，成为突破传统防御的首选目标 [7]；三是高级持续性威胁（APT）攻击展现出更强的隐蔽性与长期潜伏能力，攻击者通过精心策划的多阶段渗透，在目标网络中建立隐蔽据点，持续窃取核心数据或伺机破坏，其攻击周期可跨越数月乃至数年，对检测与响应构成严峻挑战。威胁形态的持续演进对安全防护体系的动态性、智能性与协同防御能力提出了更高要求。

3 基于分层防护模型的安全防护体系建设

3.1 网络边界层：智能自适应协议感知与动态隔离

网络边界层采用创新的智能自适应防护架构，通过深度学习技术实现工业协议异常模式的动态识别与防护策略的自适应调整。本研究创新性地提出了基于深度学习的协议异常检测引擎，通过融合卷积神经网络（CNN）与长短时记忆网络（LSTM）实现对协议数据包的智能分析。该模型突破传统规则匹配方法的局限性，其核心计算过程为：

$$\boldsymbol{h}_t = \sigma(\boldsymbol{W}_x \cdot \boldsymbol{x}_t + \boldsymbol{W}_h \cdot \boldsymbol{h}_{t-1} + \boldsymbol{b}_h) \quad (1)$$

式中：$\boldsymbol{h}_t$ 为隐层状态；$\boldsymbol{x}_t$ 为输入特征向量；$\boldsymbol{W}_x$ 和 $\boldsymbol{W}_h$ 为权重矩阵；$\boldsymbol{b}_h$ 为偏置向量；σ 为激活函数。

基于该模型，系统可自动学习工业协议的正常行为模式，实现异常流量的精确识别。

在隔离技术方面，创新性地提出“双向可控隔离”机制，在保持物理隔离的基础上，增设可控的安全数据交换通道。该机制采用国密算法 SM4 进行数据加密，结合基于零信任架构的身份认证和细粒度访问控制，确保数据交换过程的安全性。系统针对不同类型的工业协议和数据流制定了差异化的控制策略，如表 1 所示。

表 1 智能自适应边界防护策略配置表

数据类型	流向控制	安全策略	响应时间
工艺参数	双向可控	SM4 加密 + 身份认证	<50 ms
控制指令	严格单向	指令白名单 + 行为审计	<20 ms
配置数据	定时同步	完整性校验 + 版本控制	<100 ms
告警信息	实时上传	优先级排队 + 可靠传输	<30 ms

3.2 工控网络层：协议级监控与异常行为阻断

工控网络中的安全威胁日益复杂，传统的基于规则匹配的异常检测方法面临诸多挑战：一是难以应对未知的攻击模式；二是误报率高影响生产运行；三是无法自适应环境变化。

例如，某石化企业环氧丙烷装置的实际运行中，曾发生攻击者通过精心构造的异常 Modbus TCP 指令序列，规避传统检测系统，导致反应釜温度失控的严重事故。现有检测方法对协议层攻击模式的理解不足，且缺乏对时序特征的深入分析。针对上述问题，基于深度学习理论中序列建模和注意力机制的最新研究进展，本文创新性地提出一种 BiGRU-Transformer 混合神经网络模型。该模型通过双向门控循环单元（BiGRU）捕获工业协议的时序特征，并结合改进的 Transformer 编码器实现多尺度特征提取。在模型设计中，首先考虑到工控网络通信具有显著的时序相关性，单个异常包可能是正常操作，而特定序列组合则往往预示着攻击行为。因此，在特征提取层设计了基于 BiGRU 的双向信息融合机制，

其核心计算过程为：

$$\bar{\boldsymbol{h}}_t = (1-\boldsymbol{z}_t)\odot\bar{\boldsymbol{h}}_{t-1} + \boldsymbol{z}_t\odot\tilde{\boldsymbol{h}}_t$$
$$\tilde{\boldsymbol{h}}_t = \tanh(\boldsymbol{W}_h\boldsymbol{x} + \boldsymbol{r}_t\odot(\boldsymbol{U}_h\bar{\boldsymbol{h}}_{t-1}) + \boldsymbol{b}_h) \quad (2)$$

式中：$\boldsymbol{z}_t$ 为更新门控制信息更新程度；$\boldsymbol{r}_t$ 为重置门调节历史信息影响；$\bar{\boldsymbol{h}}$ 为上一时刻隐层状态；$\boldsymbol{W}$、$\boldsymbol{U}$ 为可学习的权重矩阵；$\boldsymbol{b}$ 为偏置项。这种设计使模型能够同时考虑协议数据的前向和后向依赖关系，提升对复杂攻击序列的识别能力。

在捕获基础时序特征后，考虑到工控网络攻击往往会在不同时间尺度上表现出特征关联，例如某些高级持续性威胁会在较长时间周期内表现出微弱但一致的异常模式。为此，模型引入改进的多头自注意力机制，通过学习不同时间尺度上的特征关联，增强对复杂攻击模式的感知能力。注意力权重的计算方公式为：

$$\text{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \text{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}+\boldsymbol{P}}{\sqrt{d_k}}\right)\boldsymbol{V} \quad (3)$$

式中：$\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$ 分别为查询、键、值矩阵；$\boldsymbol{P}$ 为位置编码矩阵，用于保持序列位置信息；d_k 为特征维度。该机制允许模型自适应地关注重要的时序特征组合，显著提升了对隐蔽攻击的检测能力。

为了解决工控网络中正常与异常样本严重不平衡的问题，模型采用改进的焦点损失函数进行优化，用公式表示为：

$$L = -\alpha(1-p_t)^{\gamma}\log(p_t) + \lambda R(\theta) \quad (4)$$

式中：α 为样本平衡因子，用于调节不同类别的权重；γ 为调制因子，控制难易样本的学习比例；p_t 为预测概率；$R(\theta)$ 为正则化项。

因此，能够有效提升模型对少数类异常样本的学习效果。基于上述模型设计了完整的工控网络异常检测流程，如图 1 所示。

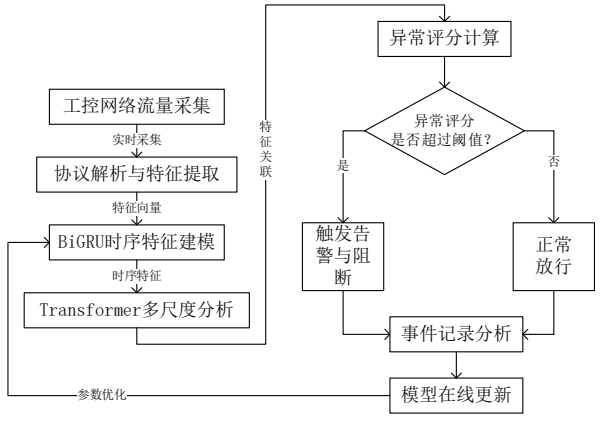

图 1 工控网络异常检测流程

在实际部署中，系统首先对工控网络流量进行实时采集和协议解析，提取包括命令类型、参数范围、时间间隔等特征。这些特征经过 BiGRU 层进行时序建模，再通过 Transformer 层挖掘多尺度特征关联。当检测到异常行为时，系统立即触发告警并执行阻断措施，同时将事件信息记录用于后续分析和模型优化。

3.3 数据存储层：透明加密与访问审计

数据存储层的安全防护聚焦于工控系统中关键配置文件与历史数据的保护，通过透明加密与访问审计技术构建双重防护机制。在实际应用场景中，PLC 程序文件、参数配置文件、历史数据库面临着未授权访问、恶意篡改等安全威胁。

透明加密方案基于 Windows EFS 加密文件系统实现，对 PLC 程序文件、设备参数配置等关键数据进行自动加密。该方案在文件系统层面进行加密操作，工控应用软件无需修改即可正常访问加密文件。系统为每个授权用户分配唯一的加密证书，确保数据访问的可控性 [8]。在文件加解密过程中采用 AES-256 算法，保障数据安全强度。

表 2 展示了数据存储层防护的具体配置方案 [9]。

表 2 数据存储层安全防护配置方案

防护项	防护对象	配置内容	告警阈值
文件加密	PLC 程序文件	EFS 加密，AES-256 算法	解密失败 3 次锁定
文件加密	设备配置文件	EFS 加密，AES-256 算法	解密失败 3 次锁定
数据库审计	实时数据表	读写操作记录	单日访问量 >1 GB
数据库审计	历史数据表	导出操作记录	单次导出量 >100 MB
行为审计	用户会话	登录认证记录	非工作时段访问

数据库审计系统采用集中式日志分析架构，实时采集 OPC 服务器、历史数据库的访问日志。系统设置多维度的告警规则，包括单日数据导出量限制、异常时段访问检测、高危操作识别等。当检测到异常行为时，系统自动记录详细的会话信息，支持后续追溯分析。

数据存储层的防护措施与工控网络层形成配合，在保障数据机密性的同时，通过审计机制及时发现潜在的数据泄漏风险。

3.4 用户管理层：最小权限控制与双因素认证

为了解决工控系统中用户权限管理分散、认证机制单一、多站点间缺乏协同等问题 [10]。本研究基于联邦学习与零信任架构理论，提出了一种多站点协同的用户访问控制方案。该方案融合双因素认证、基于角色的访问控制（RBAC）与联邦学习技术，实现跨站点的用户行为建模与异常检测。

在认证机制设计上，系统要求用户同时提供 USB Key 智能卡与基于时间序列的 TOTP 动态口令。智能卡采用国密

SM2 算法生成非对称密钥对，存储用户身份证书；动态口令基于改进的 HMAC-SHA256 算法生成，其计算过程为：

$$\mathrm{TOTP} = \mathrm{HMAC\text{-}SHA256}(K, \frac{T_0 + T_X}{T_I}) \quad (5)$$

式中：K 为用户私钥；T_0 为初始时间戳；T_X 为当前时间偏移；T_I 为更新时间间隔（默认 60 s）。这种双因素组合有效防止了凭证泄露与重放攻击风险。

在权限控制方面，系统基于 RBAC 模型设计了三级分层结构，并结合联邦学习技术实现多站点间的用户行为协同建模。各站点在保护本地数据隐私的前提下，通过模型参数共享形成统一的用户行为基线，用于实时异常检测。具体系统细化权限配置方案如表 3 所示。

表 3 用户权限分级配置表

角色类型	操作权限范围	认证要求	异常检测阈值
操作员	设备启停、参数查看	双因素认证	连续失败 3 次
工程师	参数调整、程序维护	双因素 + 审批	敏感操作预警
管理员	系统配置、策略管理	双因素 + 多人授权	实时行为分析

4 案例应用

某石化企业建有 10 万吨 / 年环氧丙烷装置，核心工艺区域包含反应、精馏、储运三大系统。装置采用西门子 S7-1500 PLC 控制系统，配套 60 余台 RTU 采集温度、压力、流量等工艺参数。中控室设有工程师站 2 台、操作员站 4 台，通过 OPC 服务器采集生产数据并存储至历史数据库。分层防护体系部署中，项目组选取反应系统作为试点区域。反应系统由 4 台反应釜构成，涉及温度调节、压力控制、物料进料等关键工艺环节。

在边界层，部署了基于深度学习的智能协议感知系统，通过 CNN-LSTM 混合模型对 Modbus TCP、S7 通信协议进行异常检测，模型在 3 个月试运行期间实现了 99.7% 的检出率，误报率低于 0.1%。工控网络层部署了 BiGRU-Transformer 混合神经网络模型，对反应釜温度、压力等关键参数进行实时监测。该模型通过联合建模多时间尺度特征，成功识别出多起隐蔽的异常操作序列，包括一起利用合法指令组合实施的温度调节攻击。系统响应时间平均维持在 50ms 以内，满足工艺控制实时性要求。在用户管理层，采用基于联邦学习的多站点协同防御机制，将反应、精馏、储运 3 个系统的用户行为数据进行联合建模。经过 6 个月运行，系统累计发现 12 起异常访问行为，较传统独立部署方案提升了 40% 的检出效果。双因素认证与联邦行为建模的组合应用，实现了 99.9% 的权限隔离度。

试点应用结果表明，分层防护体系在保障反应系统安全运行方面取得显著成效。基于深度学习的边界防护实现了精确的协议异常识别，BiGRU-Transformer 模型提供了可靠的攻击序列检测能力，联邦学习支撑的用户行为建模确保了跨系统的协同防御效果。该防护体系的各项技术指标均满足工业现场需求，为后续全厂推广应用奠定了基础。

5 结语

基于分层防护模型的计算机信息安全防护体系，通过 CNN-LSTM 实现边界防护、BiGRU-Transformer 支撑网络监控、透明加密确保数据保护、联邦学习保障用户管理等多层次协同配合，实现了对虚拟网络环境的全方位智能化防护。实践应用验证了该防护体系的可行性和有效性，但在智能化感知精度提升、多层防护协同优化、异常行为模式挖掘等方面仍需深入研究。未来将重点探索基于新型人工智能算法的威胁检测技术，进一步提升防护体系的自适应能力和防护效果。

参考文献：

[1] 曾庆瑞 . 基于自监督学习的计算机信息入侵检测算法研究 [J]. 信息记录材料 , 2025, 26(6):111-113.

[2] 王梦仙 , 李银锁 , 钟石根 , 等 . 基于 K-means 聚类的计算机网络信息安全风险评估方法 [J]. 信息记录材料 , 2025, 26(6): 36-38.

[3] 喻沛尧 , 霍辛格 . 造纸企业网络信息安全纵深防御机制构建 [J]. 造纸科学与技术 ,2025,44(5):72-76.

[4] 谢林栩 . 云计算背景下网络信息安全管理策略 : 评《云计算环境中计算机网络信息安全研究》[J]. 安全与环境学报 , 2025, 25(5): 2058.

[5] 王珂琦 . 计算机网络信息安全影响因素及防范措施探讨 [J]. 漯河职业技术学院学报 , 2025,24(3):22-24.

[6] 赵腾 . 计算机信息管理技术在网络安全应用中的应用研究 [J]. 信息系统工程 , 2025(5):83-86.

[7] 赵源 . 基于计算机数据流的信息安全态势感知技术研究 [J]. 信息记录材料 , 2025,26(5):102-104.

[8] 郭子扬 , 徐夏辉 , 姚理刚 . 虚拟网络技术在网络信息安全防护中的应用研究 [J]. 中国军转民 ,2025(8):25-26.

[9] 尹鸿波 . 网络环境下企业计算机信息系统安全策略研究 [J]. 计算机安全 , 2011(2):68-69.

[10] 袁誉峰 , 韩保礼 , 张晓峰 , 等 . 计算机网络信息安全及防护策略研究 [J]. 中国新通信 ,2024,26(8):7-9.

【作者简介】

李静（1982—），女，山东鄄城人，本科，初级工程师，研究方向：信息工程。

（收稿日期：2025-07-11 修回日期：2026-01-26）