

DOI:10.19344/j.cnki.issn1671-5276.2025.05.057

基于 NSM 的无人值守变电站实时监控研究

张继超, 刘浩东, 孙文凯, 刘名轶, 高原

(国网河北省电力有限公司 雄安新区供电公司, 河北 雄安 071699)

摘要:针对 IEC 61850 变电站在安全监控方面的问题,提出基于 IEC 62351-7 网络和系统管理(NSM)的解决方案,通过深度学习框架和 NSM 数据对象的应用,实现对异常行为和网络攻击的实时检测和识别。研究构建详细的变电站模型,包括电力组件、保护设备、控制方案、通信协议和 NSM 应用,结合两步深度学习框架进行异常检测和网络攻击识别。实验结果表明:该方法能有效检测针对 GOOSE 协议的注入和延迟攻击, $F1$ 分数达到 0.98 以上。

关键词:变电站;异常检测;深度学习;集成学习;IEC 61850;网络和系统管理

中图分类号:TM63 **文献标志码:**B **文章编号:**1671-5276(2025)05-0294-05

Research on Real-time Monitoring of Unattended Substation Based on NSM

ZHANG Jichao, LIU Haodong, SUN Wenkai, LIU Mingyi, GAO Yuan

(Xiongan New Area Power Supply Company, State Grid Hebei Electric Power Supply Co., Ltd., Xiongan 071699, China)

Abstract: A solution based on IEC 62351-7 Network and System Management (NSM) was proposed to address the security monitoring issues of IEC 61850 substations. The aim was to achieve real-time detection and identification of anomalies and network attacks through the application of deep learning frameworks and NSM data objects. A detailed substation model was constructed, including power components, protection devices, control schemes, communication protocols, and NSM applications. A two-step deep learning framework was integrated for anomaly detection and network attack identification. Experimental results showed that the proposed method effectively detected GOOSE protocol injection and delay attacks, with $F1$ scores exceeding 0.98.

Keywords: transformer station; anomaly detection; deep learning; integrated learning; IEC 61850; network and system management

0 引言

随着电力系统的数字化转型,智能电网基础设施面临新的网络安全威胁^[1-6]。IEC 62351-7 标准规定了使用网络和系统管理(network and system management, NSM)数据对象支持智能电网的安全监控^[7]。近年来,研究者们探索了多种 IEC 61850 变电站异常检测方法^[8-12]。YOO 等^[13]提出了结合期望最大化、局部异常因子和 SVM 的方法。FENG 等^[14]开发了基于 LSTM 模型的工业控制系统异常检测框架。CERRONI 等^[15]研究了利用 SNMP MIB 数据进行入侵检测的方法。钟化兰等^[16]提出了一种变电站设备运行状态数据实时监测方法。

然而,现有研究未能充分利用 IEC 62351-7 规定的 NSM 数据对象,也缺乏在真实的网络物理环境中评估检测性能^[17-20]。本文旨在通过实现

NSM 安全监控平台和提出基于深度学习的异常检测框架来弥补这些不足,使用硬件在环测试平台对其有效性进行了评估,揭示了基于 NSM 安全监控的能力和局限性,并为完善 IEC 62351-7 标准提出了建议。

1 系统建模与协同仿真测试床

1.1 实验系统

1) IEEE 9 节点系统

IEEE 9 节点系统包括 3 个发电单元(节点 1、节点 2 和节点 3)和 3 个负荷变电站(节点 4、节点 5 和节点 6),通过 6 条输电线相连。电网总负荷需求为 315 MW 和 115 MVar。系统单线图及详细参数如图 1 所示。

2) IEC 61850 数字变电站

变电站物理部分包括电流互感器(current transformer, CT)、合并单元、断路器、变压器和控

基金项目:国家电网有限公司科技项目(5600-202046347A-0-0-00)

第一作者简介:张继超(1985—),男,河北临漳人,高级工程师,硕士,研究方向为变电运维及监控技术,hvqy066@163.com。

制室。CT 将电流幅值降至适合控制/保护系统的水平,合并单元将 CT 测量值转换为数字保护系统的采样值协议。控制和保护系统用于调节电网参数并保护电网。

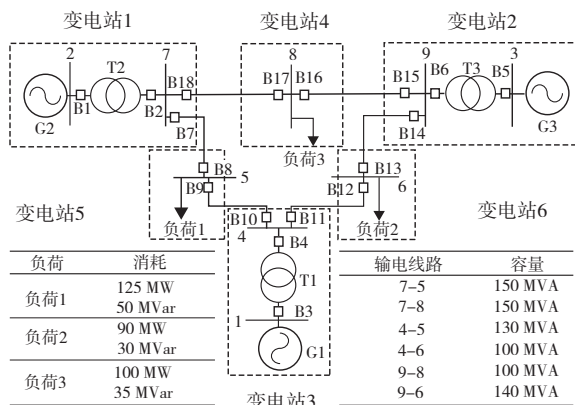


图1 IEEE 9节点系统

保护系统及其智能电子设备 (intelligent electronic device, IED) 的主要目标是检测并隔离电气故障。所开发的变电站模型中部署了 3 种继电器: 过电流继电器 (50/51)、距离继电器 (21) 和差动继电器 (87), 采样频率为 2~3 kHz, 编号依据 ANSI/IEEE C37.2 标准。

控制方案的主要目标是确保系统参数 (如电压) 在可接受范围内。本研究开发了一种使用变压器负载调压器的电压调节方案, 在变压器次级侧测量电压, 计算变压器分接头以确保电压保持在可接受范围内。系统运行点变化后, 控制系统延迟 1.25 s 调节电压, 然后分接开关机制以每单位 1.25% 的步长激活。模拟的变压器有 23 个分接头。发电机配备了自动电压调节器、电力系统稳定器等。

1.2 网络系统

1) 协议

本研究实现了采样值、通用面向对象变电站事件 (GOOSE) 和可路由 GOOSE (R-GOOSE) 协议。采样值用于从合并单元向其他 IED 传输测量值, GOOSE 用于变电站内 IED 向断路器传输控制信号, R-GOOSE 用于变电站间传输控制信号。安全性方面, 采用 IEC 62351 建议的安全措施。

2) 通信网络

IEC 61850 变电站通信模式如图 2 所示。变电站通信分为过程层、间隔层和站控层, 层次间通过网络交换机连接。所有 IED 和控制器均具有 NSM 功能。变电站网络通过协同仿真测试床进

行仿真。

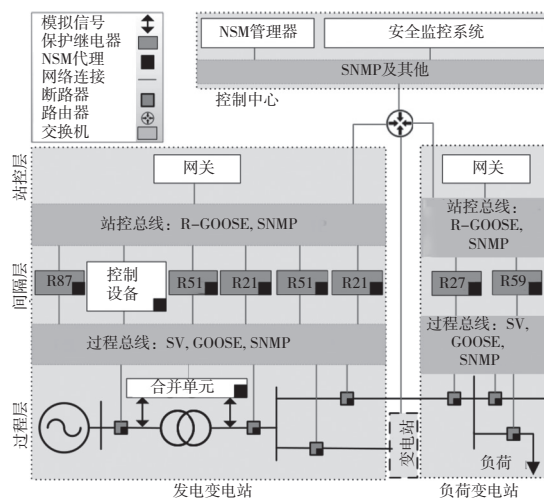


图2 IEC 61850 变电站模型

1.3 NSM

NSM 旨在收集变电站中不同 IED 的统计数据 (图 2)。这些 IED 的测量数据和 NSM 收集的数据分别用于操作决策和保障变电站的安全。在 NSM 平台中, 代理收集 MIB 对象值并通过 SNMP 发送给管理器进行监控。NSM 的总体方案如图 3 所示, 其中管理器根据 IEC 62351-7 查询所有代理收集的 MIB 对象值。

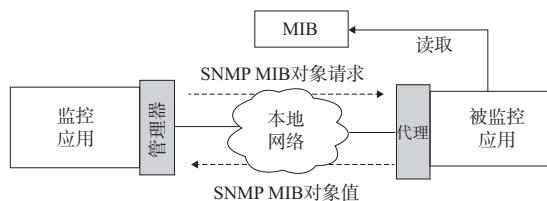


图3 NSM 的总体方案

NSM 数据对象 (data object, DO) 的收集方法主要有两种: 轮询和陷阱。所提出的测试床使用轮询从代理中检索最新的 DO 值, 以提高异常检测速度。

1.4 协同仿真测试床

本研究使用网络虚拟化系统构建通信网络, 以传输电力测量值和控制命令。测试床由 OPAL-RT 数字模拟器和 OpenStack 组成。OPAL-RT 实时模拟电网, 并提供 I/O 接口连接物理 IED, 支持多种协议 (如 IEC 61850、Modbus 等), 用于评估安全攻击的影响。OpenStack 模拟智能电网的网络通信, 提供 VM, 并通过自定义透明桥控制通信网络质量参数。

2 威胁建模

本文考虑了简单和复杂的攻击场景,例如通过发送恶意控制命令或复杂的未被检测到的攻击来颠覆电网。同时,识别变量用于生成针对工业控制系统(industrial control system, ICS)协议的网络攻击列表(表1)。研究考虑了能够注入恶意GOOSE数据包并延迟合法数据包的攻击者模型。GOOSE协议用于传递保护继电器到断路器的命令,攻击者可以通过伪造或修改数据包来进行攻击。GOOSE注入攻击在透明桥VM上进行模拟,Python代码在透明桥上运行以执行攻击。

3 异常检测技术

本文通过提升深度学习模型的预测性能来增强安全监控系统,使用LSTM、GRU和RNN,并结合自动编码器改善预测结果。此外,使用集成学习方法结合3种模型的结果,以提高整体预测效果。

检测系统构建包括数据收集、数据预处理、训练和验证4个阶段。正常操作下的故障位置和事

件如表2所示。使用集成学习进行组合模型的实时异常检测过程,检测到异常时,将异常数据替换为预测数据并发送警报,组合模型的训练和检测过程如图4所示。

表1 ICS 协议的网络攻击列表

ID	攻击类型
G1	修改 PDU 长度
G2	修改、注入或重放具有较高 stNum 的协议数据单元(PDU)
G3	修改 PDU 的 t 值使其超出偏差周期
G4	延迟 PDU 直到其超出偏差周期
G5	修改、注入或重放具有较小存活时间(TAL)的 PDU 以强制 TAL 过期
G6	丢弃 PDU 直到 TAL 过期
G7	延迟 PDU 直到 TAL 过期
G8	修改 PDU 的 confRev 字段
G9	修改、注入或重放带有测试标志的 PDU
G10	使数字签名无效

表2 正常操作下的故障位置和事件

ID	故障类型	位置	检测到的故障	跳闸的断路器
Tr0	变压器故障	变压器 2	变电站 1 继电器 87	B1, B2
Tr1	变压器故障	变压器 3	变电站 2 继电器 87	B5, B6
Tr2	变压器故障	变压器 1	变电站 3 继电器 87	B3, B4
L0	线路故障	母线 7-8	变电站 1 继电器 51, 21	B18, B17
L1	线路故障	母线 8-9	变电站 2 继电器 51, 21	B15, B16
L2	线路故障	母线 9-6	变电站 2 继电器 51, 21	B13, B14
L3	线路故障	母线 6-4	变电站 3 继电器 51, 21	B11, B12
L4	线路故障	母线 4-5	变电站 3 继电器 51, 21	B9, B10
L5	线路故障	母线 5-7	变电站 1 继电器 51, 21	B7, B8

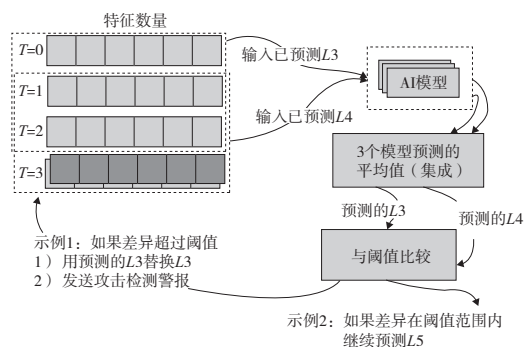


图4 组合模型的训练和检测过程

4 实验结果

实验使用平衡数据对检测方法进行了评估,计算了真阳性(T_p)、假阴性(F_N)、真阴性(T_N)、假阳性(F_p)、召回率 R_{recall} 、精度 P_{recision} 和 F1 值。召回率、精度和 F1 评分计算公式如下:

$$R_{\text{recall}} = \frac{T_p}{T_p + F_N} \quad (1)$$

$$P_{\text{recision}} = \frac{T_p}{T_p + F_p} \quad (2)$$

$$F1 = \frac{2 \cdot R_{\text{recall}} \cdot P_{\text{recision}}}{R_{\text{recall}} + P_{\text{recision}}} \quad (3)$$

本研究通过两个实验衡量检测方法的性能和准确性。第 1 个实验包括无物理故障的正常运行、GOOSE 注入攻击和 GOOSE 延迟攻击。第 2 个实验包括有物理故障的正常运行、GOOSE 注入攻击和 GOOSE 延迟攻击。检测性能结果如表 3 和表 4 所示。

表 3 在无物理故障情况下的检测性能

T_P	F_N	F_P	T_N	召回率	精度	F1 值	α
477	23	2	498	0.954	0.995 8	0.974 5	1.0
489	11	20	480	0.978	0.960 7	0.969 3	0.9
497	3	111	389	0.994	0.817 4	0.897 1	0.8

表 4 故障存在情况下的检测性能

T_P	F_N	F_P	T_N	召回率	精度	F1 值	α
481	19	12	488	0.962	0.975 7	0.968 8	1.0
492	8	27	473	0.984	0.948 0	0.965 7	0.9
499	1	131	369	0.998	0.792 1	0.883 2	0.8

异常检测方法通过比较 MIB 对象值与预测值的偏差和分配给 MIB 对象的异常阈值,判断新的 MIB 对象读数是否异常。阈值等于 α 与损失的乘积,其中 α 是常数乘法因子,损失是训练过程验证步骤中发现的 MIB 对象的最大预测损失。 α 选择结果如表 3 和表 4 所示。

验证检测时间性能的实验在 Intel Core i7-7700k CPU 上进行,平均生成时间为 0.64 ms,符合 IEC 61850 对已部署协议的时间要求。通过训练多个深度学习模型,检测系统可以指出具体异常的 MIB 对象及受影响的设备,详细记录异常信息,用于区分不同攻击。

4.1 检测针对保护系统的网络攻击

1) 注入具有更高 stNum 的 GOOSE PDU

这种攻击通过注入假 GOOSE 消息中断发布者(如继电器)与订阅者(如断路器)之间的通信,使订阅者无法处理合法的跳闸命令,导致系统故障级联扩散,可能引发停电(攻击 ID:G2)。该攻击在场景 S1 中的影响如图 5 所示,该攻击可以通过分析 GOOSE 消息速率的异常来检测。

2) 修改具有更高 stNum 的 GOOSE PDU

在此攻击中,攻击者修改已传输的 GOOSE 消息的 stNum 为更大值,使订阅者丢弃合法消息(攻

击 ID:G2)。由于修改攻击不改变消息速率,因此难以检测。

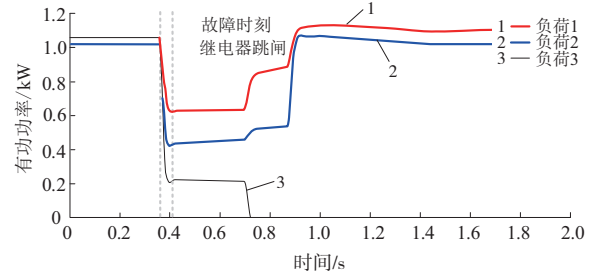


图 5 场景 S1 各负荷下的 VRMS

4.2 检测针对控制系统的网络攻击

1) 注入具有更高 stNum 的 GOOSE PDU

这种攻击通过注入假 GOOSE 消息,迫使变压器分接开关持续上调,导致过电压,触发保护系统跳闸,导致停电(攻击 ID:G2)。该攻击可通过分析 GOOSE 消息速率的异常检测到,如图 6 所示。

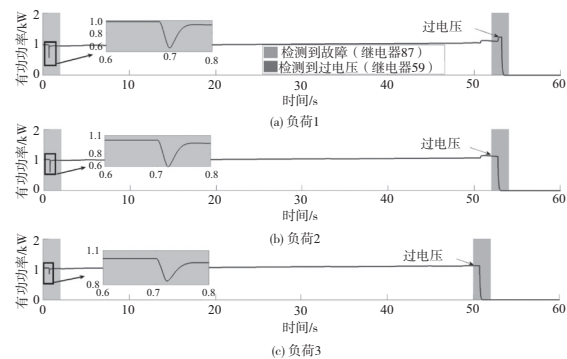


图 6 场景 S5 各负荷下的 VRMS

2) 修改 GOOSE PDU(畸形 PDU)

攻击者修改 GOOSE 消息内容,迫使变压器分接开关下调,导致欠电压,引发保护系统跳闸,导致停电(攻击 ID:G1)。由于没有 MIB 对象报告此活动,该攻击难以检测。

5 安全评估

NSM 的 IEC 62351-7 数据对象可以检测多种针对 IEC 61850 变电站的攻击,但在某些情况下只能提供部分检测能力。通过更精确地定义现有 NSM DOs 或添加新 DOs,可以增强其检测能力,特别是在检测如 DoS 攻击等无法从物理系统测量中检测到的攻击时。

5.1 NSM 与 GOOSE/SV 协议

NSM DOs 可以帮助检测多种 GOOSE 协议攻击,包括 InErrCnt、Decrypt FailCnt 和 Message

Integrity FailCnt 等。

5.2 NSM 与 MMS 协议

NSM DOs 能有效检测针对 MMS 协议的多类攻击,跟踪发送和接收的 PDU 总数以及篡改 PDU 的错误或解密失败计数器。尽管 NSM 无法检测嗅探或修改 MMS PDU 的攻击,但使用 IEC 62351-4 的 TLS 可解决这些问题。

6 结语

本研究实现了一个基于 NSM 的 IEC 61850 变电站安全监控平台。通过硬件在环仿真环境中详细建模电力系统动态、保护措施、控制方案和通信协议,开发了一个两步深度学习框架来检测网络攻击和异常。实验结果表明,所提出的方法能够有效识别针对变电站通信协议的多种攻击,同时揭示了 NSM 数据对象在检测某些复杂攻击方面的局限性。基于评估结果,本文对 IEC 62351-7 标准提出了一系列改进建议,包括增加新的 NSM 数据对象以增强检测能力。未来的研究方向包括扩展 NSM 数据对象集以进一步提高防御系统性能,以及结合深度包检测等技术来增强攻击检测能力。

参考文献:

- [1] 郭剑黎,彭磊,郭祥富,等. 智能电网环境下配网调度系统及关键技术研究[J]. 微型电脑应用, 2023, 39(12):179-182,190.
- [2] 陈兆强,王圣达,杨宇,等. 智能电网中的网络安全关键技术分析[J]. 集成电路应用, 2024, 41(11): 406-408.
- [3] 马克勤. 基于支持向量机的电网安全抽检数据分析方法[J]. 网络安全和信息化, 2024(8):68-70.
- [4] 金志刚,刘凯,武晓栋. 智能电网 AMI 领域 IDS 研究综述[J]. 信息网络安全, 2023, 23(1):1-8.
- [5] 余越,贺丰婕. 智能变电站通信安全技术研究[J]. 上海电气技术, 2025, 18(1):20-24.
- [6] 王赛,赵燕,王伟,等. 变电站电力监控系统网络安全防御体系[J]. 网络安全技术与应用, 2025(3): 132-135.
- [7] 曹璐,张娜,林师哲. 电力系统的信息基础设施可靠性和安全性提升分析[J]. 电气技术与经济, 2024(7):305-307.

- [8] 赵武智,樊国盛,邬小坤,等. 基于 IEC 61850 的智能变电站二次回路安全隔离研究[J]. 自动化技术与应用, 2024, 43(6):141-145.
- [9] 谭康,杨洋. 基于 SDN 技术的变电站网络通信模型[J]. 电子设计工程, 2024, 32(19):81-85.
- [10] 王珠峰,孔凡坊,陈培训,等. 基于 IEC 61850 标准的智能变电站 SCL 文件验证算法[J]. 电工技术, 2024(18):126-131,134.
- [11] 谢天祥,张磊,冯浩然,等. 基于 IEC61850 信息模型的智能变电站信息流可视化系统设计[J]. 信息技术, 2023, 47(8):51-56,64.
- [12] 祝尧涵. 基于 IEC61850 的智能变电站通信网络分析[J]. 自动化应用, 2022(12):91-93.
- [13] YOO H, SHON T. Novel approach for detecting network anomalies for substation automation based on IEC 61850[J]. Multimedia Tools and Applications, 2015, 74(1):303-318.
- [14] FENG C, LI T T, ZHU Z X, et al. A deep learning-based framework for conducting stealthy attacks in industrial control systems[EB/OL]. (2017-09-19) [2024-06-10]. <https://arxiv.org/abs/1709.06397v1>.
- [15] CERRONI W, MORO G, PASOLINI R, et al. Decentralized detection of network attacks through P2P data clustering of SNMP data[J]. Computers & Security, 2015, 52:1-16.
- [16] 钟化兰,黄扬海. 基于 IEC61850 的智能变电站设备运行状态数据实时监测方法[J]. 计算机应用与软件, 2024, 41(5):96-100,137.
- [17] 王子杰,潘啸天. 工业变电站运维系统异常数据入侵检测互信息实现[J]. 现代工业经济和信息化, 2024, 14(8):94-95,104.
- [18] 张涤. 基于异常检测的电力系统网络攻击检测分析[J]. 通讯世界, 2024, 31(9):49-51.
- [19] 蒋亚坤,林旭,黄博. 基于多模型仿真的变电站数据监控与性能评估研究[J]. 电工电气, 2025(4): 53-58.
- [20] 冯宇,马伟哲,陈光,等. 基于 Modbus 通信协议的智能变电站安全监控交互数据监测[J]. 计算技术与自动化, 2024, 43(3):60-64,94.

收稿日期:2024-08-02