

[无人值守]

基于入侵检测系统的无人值守 新能源电场网络安全防护

文/杨金贵 刘艳 刘军 方志明
云南滇能智慧能源有限公司

随着新能源电场的迅猛发展，网络安全成为无人值守电场运行中的关键挑战。入侵检测系统（IDS）作为网络安全防护的重要技术，能够有效监测并应对复杂网络威胁。基于入侵检测系统，详细探讨其在无人值守新能源电场中的行为分析、深度包检测、机器学习攻击模式识别以及协同入侵响应等应用，提出有效的网络安全防护策略，以应对潜在的网络威胁并提升整体安全性。

入侵检测系统（Intrusion Detection System，IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。在无人值守新能源电场中，网络安全防护面临严峻挑战，对网络攻击的防御能力提出更高要求。为此，本文研究IDS在无人值守新能源电场网络安全防护中的应用，结合深度包检测（DPI）、行为基线分析、机器学习算法和协同入侵响应等技术，探讨其应对高级持续性威胁等复杂攻击的有效性。

入侵检测系统概述

1. 入侵检测系统的基本结构

入侵检测系统的基本结构主要由信息收集模块、入侵分析模块、告警响应模块组成，如图1所示。

信息收集模块负责从系统运行中采集系统日志、网络数据、审计记录以及其他告警信息等数据，确保全面监控网络和主机活动。这是入侵检测系统的前端环节，提供所有后续分析所需的原始数据。其次，入侵分析模块通过对收集的数据进行深入分析，利用特征匹配、历史行为对比以及异常行为检测等技术，从知识库中提取相似的行为模式，

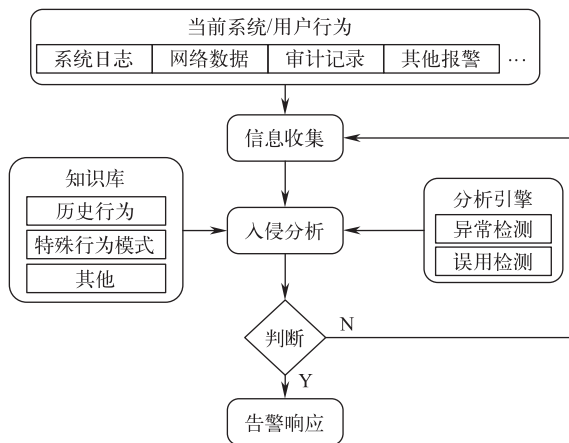


图1 入侵检测系统的基本结构

并结合分析引擎进行异常检测和误用检测。该模块能够识别异常行为与潜在威胁，通过判断当前行为与系统基准的偏差，准确发现可能的入侵行为。最后，告警响应模块根据入侵分析模块的判断结果，自动触发预设的安全响应措施。一旦确认存在威胁，该模块会发出告警信号，或采取阻断恶意连接、隔离受感染设备等防御措施，并及时通知管理人员。整个系统通过这三个模块的协同运作，形成了一个实时、有效的网络安全防护体系，保障了无人值守新能源电场的网络安全。

2. 入侵检测系统的分类

IDS根据核心分析引擎的不同，可分为基于异常的入侵检测系统（Anomaly-based IDS）和基于误用的入侵检测系统（Misuse-based IDS）。基于异常的入侵检测系统通过学习和训练正常行为模式，建立一个正常行为特征库。在系统运行时，信息采集子系统利用传感器或其他数据收集方式实时获取当前的行为数据，并将其与正常行为特征库中的标准进行比对。检测器根据设定的阈值判断行为是否属于正常行为。当行为未超出预设的阈值时，判定为正常行为；而一旦行为超出阈值范围，则视为异常行为，并发出告警。该系统能够识别未知威胁和零日攻击，但由于正常行为模式的复杂性，可能导致误报率较高。基于异常的入侵检测系统基本结构如图2所示。

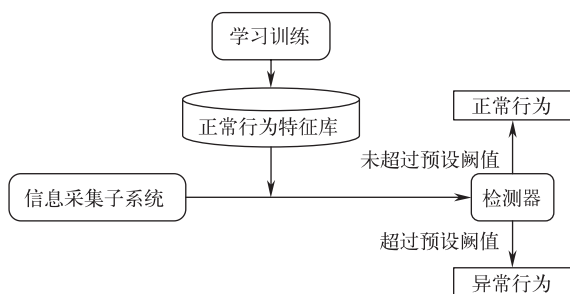


图2 基于异常的入侵检测系统基本结构

基于误用的入侵检测系统通过学习已知攻击行为模式，建立一个入侵行为特征库。当信息采集子系统获取到实时的网络流量和系统行为时，检测器将其与入侵行为特征库中的模式进行比对。当检测器识别出匹配的行为时，判定为入侵行为，并触发相应的防护措施；如果不匹配，则认为是正常行为。该系统能够准确识别已知威胁，具有较低的误报率，但对未知攻击的检测能力有限。基于误用的入侵检测系统基本结构如图3所示。

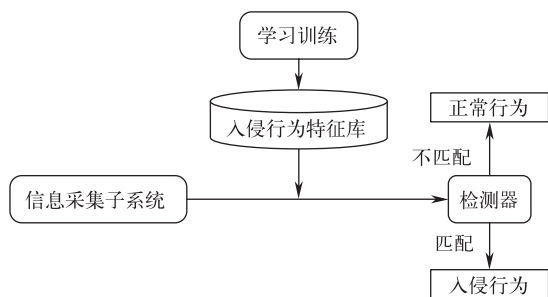


图3 基于误用的入侵检测系统基本结构

入侵检测系统在无人值守新能源电场网络安全防护中的应用

1. 基于行为分析的异常检测

在无人值守新能源电场中，基于行为分析的异常检测通过建立设备和网络的正常行为基线，有效识别异常的网络活动，显著提升网络安全防护水平。首先，入侵检测系统会持续采集电场中各类设备的网络流量数据、用户访问日志和控制系统操作记录等多种数据，并对其进行综合分析。系统通过部署网络监控探针和日志分析平台，结合PLC的日志记录模块，对电场内部的通信行为进行实时监控。入侵检测系统设定10 min为时间窗口，重点分析网络通信的频率、数据包大小、源IP和目标IP等关键参数，进而构建出正常业务行为模型。针对ABB逆变器、GE风力发电机等关键设备，入侵检测系统能够依据这些设备的常规通信模式，及时检测出网络中出现的流量突增、未经授权的控制指令及非正常时间的登录尝试等异常行为。系统通过对这些关键设备的常规行为进行长期监控与分析，确保其在异常情况下能够迅速做出反应。为此，异常检测模块结合K-Means聚类 and 隐马尔可夫模型（HMM）等机器学习算法，用来对这些设备的实时通信行为进行动态建模和自动分析。当系统发现某些设备的通信行为与正常基线出现显著偏离时，入侵检测系统会立刻触发警报，并采用自动化通知机制向安全运维团队发出警告，确保潜在威胁在最短时间内得到响应和处理。这种基于行为分析的检测机制，能够有效应对APT攻击、零日漏洞利用等复杂威胁，全面保障无人值守新能源电场的网络安全运行。

2. 基于深度包检测的网络流量审查

基于深度包检测（Deep Packet Inspection, DPI）技术，入侵检测系统能够深入解析OSI模型第7层的数据包内容，精确分析应用层协议以及其中的细节，以发现隐藏在表层流量下的恶意行为或异常数据流。首先，IDS部署在新能源电场的核心路由器或防火墙设备，利用硬件设备的高性能计算能力和流量镜像功能，实时获取网络中的进出数据包。系统使用Snort或Suricata作为DPI引擎，这些引擎基于预设的规则集对数据包进行深度解析。规则集可以针对特定的应用层协议制定专门的解析

策略，分析协议是否遵循标准、是否存在不合规的异常行为。例如，在分析HTTP协议时，系统可以识别是否存在跨站脚本（XSS）攻击或SQL注入等常见的应用层攻击行为；在分析DNS协议时，IDS则可以检测通过DNS隧道进行的隐蔽数据泄露行为。其次，IDS可以基于预设的攻击签名库识别SQL注入、跨站脚本（XSS）、缓冲区溢出等常见网络威胁。这种基于签名匹配的检测方式能够有效应对已知威胁，迅速识别攻击模式并做出反应。同时，IDS通过对非标准端口和非协议流量的行为分析，检测潜在的规避行为。为提高流量审查的准确性，IDS配置了基于正则表达式的过滤规则，针对HTTP、DNS、FTP等高频协议中的异常使用进行深入检测，确保精确捕获高级持续性威胁（APT）。在系统调优过程中，IDS会结合历史流量基线数据，通过调整流量审查的数据包深度分析上限和会话超时等阈值参数，以确保在保持高性能的同时，全面覆盖潜在的网络攻击行为。

3. 基于机器学习的攻击模式识别

在无人值守新能源电场网络安全防护中，基于机器学习的攻击模式识别方法通过深度神经网络（DNN）、支持向量机（SVM）和卷积神经网络（CNN）等算法，对电场中的网络流量、设备日志、访问控制日志等多维数据进行特征提取与建模，从而使IDS能够自动识别并应对复杂的网络攻击模式。

1) IDS通过在新能源电场的网络交换机上部署NetFlow流量采集器，对网络数据进行实时监控，并将流量采样率设置为1:1 000，以确保数据分析的实时性和准确性。

2) IDS会对采集到的流量数据进行归一化处理，结合历史攻击特征库，使用自适应Boosting算法对数据进行分类，识别潜在的网络攻击行为。当检测到异常流量或未知的攻击模式时，IDS会进一步应用长短时记忆网络（LSTM），结合NVIDIA Tesla V100 GPU加速器对检测结果进行深度学习模型的训练与优化。在此过程中，系统依托高性能计算平台，对大规模网络流量数据进行训练，自动生成新的攻击特征，并实时更新入侵检测模型的权重参数，确保对零日攻击和高级持续性威胁（APT）的有效识别。

3) IDS将生成的攻击特征反馈至策略引擎，自动更新防火墙策略并调整访问控制列表，进一步强化对新能源电场核心控制设备的安全防护，实现网络环境的自适应调整与精准防护，确保无人值守电场的安全运行。

4. 基于协同入侵响应的实时防护

在无人值守新能源电场网络安全防护中，协同入侵响应系统通过入侵检测系统（IDS）与防火墙、入侵防御系统（IPS）、安全信息与事件管理系统（SIEM）等多种网络安全设备的联动，实现高效的实时防护机制。

1) IDS在检测到异常网络流量或入侵行为时，利用深度包检测技术和行为分析算法对威胁进行初步分析，并基于安全信息与SIEM将检测到的威胁信息发送至集成响应平台。

2) SIEM结合IPS自动生成相应的防护策略，实时调整电场内部网络的访问控制列表与防火墙规则，封锁可疑IP地址并隔离受感染设备。在此过程中，IDS与IPS配合运用自适应安全架构（ASA）技术实时动态更新规则库，并触发边缘计算节点中的虚拟局域网隔离机制（VLAN Isolation），保障SCADA系统与PLC等关键设备的安全运行。为提升防护效率，SIEM还会结合时序数据分析与多维数据融合技术，实时整合历史网络日志、设备操作日志等数据，以提高系统对未知威胁的防御能力。

在此协同防护过程中，Cisco ASA 5506-X防火墙、Snort IDS、Palo Alto Networks PA-220防火墙以及Splunk SIEM系统共同构成了防护的核心。将IPS的阈值设置为1 000包/s，ACL的动态刷新时间为5 s，VLAN隔离的响应延迟控制在1 s以内，确保在高负荷运行下，系统依然能够迅速检测和隔离潜在威胁，保证电场网络的安全性和稳定性。

结束语

综上所述，基于入侵检测系统的无人值守新能源电场网络安全防护体系，在实时性、智能化和协同防御方面表现出显著优势。未来，结合大数据分析和人工智能算法的入侵检测系统将进一步增强新能源电场网络的安全性和可控性。EA

（收稿日期：2024-10-14）