电力信息系统的入侵检测与响应机制优化研究

李　岳　吴成珂　施玉彬
国网浙江省电力有限公司青田县供电公司　浙江　丽水　323900

摘　要：本文聚焦于电力信息系统的入侵检测与响应机制优化。首先分析了电力信息系统面临的安全威胁及现有入侵检测与响应机制存在的问题，进而从检测技术、响应策略、系统架构等方面提出优化方法，并通过实验验证优化机制的有效性，旨在提升电力信息系统的安全防护能力，保障电力系统的稳定运行。

关键词：电力信息系统；入侵检测；响应机制；优化研究

1 电力信息系统面临的安全威胁分析

1.1 网络层安全威胁

在网络层，电力信息系统面临着多种形式的攻击。拒绝服务攻击（DoS/DDoS）是较为常见且危害较大的一种攻击方式。攻击者通过控制大量僵尸网络，向电力信息系统的服务器发送海量的无用请求，耗尽服务器的带宽、CPU 资源等，导致系统无法正常响应合法用户的请求，进而影响电力调度、监控等关键业务的正常运行，可能引发大面积停电等严重后果。端口扫描和嗅探也是黑客常用的手段。端口扫描可以探测系统中开放的端口，从而发现可能存在的服务漏洞；嗅探则能截获网络中传输的数据包，获取系统敏感信息，如用户账号、密码、设备配置参数等。这些信息一旦被黑客获取，就可能被用于进一步的攻击，如非法访问系统、篡改数据等，对电力信息系统的安全构成严重威胁[1]。

1.2 应用层安全威胁

应用层是电力信息系统与用户交互的重要层面，也是安全威胁的高发区域。恶意软件，如病毒、木马等，常常通过电子邮件、网页下载、移动存储设备等途径侵入系统。一旦恶意软件在系统中扎根，就会窃取或篡改重要数据，如电力设备的运行参数、用户用电信息等。例如，某些木马程序可以潜伏在系统中，实时监控用户的操作，将敏感信息发送给攻击者；病毒则可能破坏系统的文件和数据，导致系统崩溃或功能失效。此外，应用层的软件漏洞也为攻击者提供了可乘之机。由于电力信息系统的应用软件通常具有较高的复杂性和专业性，开发过程中难免会存在一些安全漏洞。攻击者可以利用这些漏洞进行注入攻击、跨站脚本攻击等，获取系统的控制权或窃取敏感数据。

1.3 内部安全威胁

内部人员的误操作或恶意行为对电力信息系统的安全同样构成严重威胁。由于电力信息系统的操作和管理需要专业的知识和技能，内部人员在操作过程中可能因疏忽大意或缺乏经验而进行违规操作，如越权访问敏感数据、错误配置系统参数等，导致系统出现安全漏洞或数据泄露。更有甚者，个别内部人员可能出于个人利益或其他不良动机，主动泄露系统关键信息或进行恶意破坏。他们熟悉系统的内部结构和运行机制，能够更精准地实施攻击，给电力系统带来巨大的损失。例如，内部人员可以通过修改电力设备的控制参数，导致设备运行异常，影响电力供应的稳定性。

2 现有入侵检测与响应机制存在的问题

2.1 入侵检测技术局限

现有的入侵检测技术主要分为基于误用检测和基于异常检测两种。基于误用检测依赖于已知的攻击特征库，就像一个有着固定规则的守门人，只能识别那些已经在特征库中记录的攻击行为。然而，随着网络攻击技术的不断发展，新的攻击手段层出不穷，黑客可以通过变形、加密等方式绕过特征库的检测。因此，基于误用检测对于未知攻击的检测能力非常有限，无法及时发现那些尚未被收录在特征库中的新型攻击，给电力信息系统留下了安全隐患。基于异常检测虽然能够检测未知攻击，它通过建立正常行为的模型，将偏离模型的行为视为异常，从而发现潜在的攻击。但这种方法存在较高的误报率。因为电力信息系统的运行环境复杂多变，正常的业务操作也可能产生一些与常规行为不同的模式，导致系统将这些正常行为误判为攻击行为。例如，在电力设备进行定期维护或升级时，系统的网络流量和操作模式可能会发生较大变化，基于异常检测的系统可能会将这些变化误认为是入侵行为，从而发出大量误报，增加了安全管理人员的工作负担，也降低了系统的可信度。

2.2 响应策略不足

现有的响应策略大多为被动响应，缺乏主动防御能力。系统通常在检测到入侵后才采取措施，此时攻击可

能已经对系统造成了一定程度的损害，而且无法及时阻止攻击的进一步蔓延。例如，当系统检测到 DDoS 攻击时，攻击可能已经导致服务器瘫痪，影响了部分业务的正常运行。此外，响应过程往往缺乏智能化决策支持。安全管理人员需要根据经验手动判断攻击的严重程度并制定响应策略，响应效率低下[2]。在面对大规模、复杂的网络攻击时，人工响应可能无法及时做出反应，导致攻击得逞。而且，不同的安全管理人员对攻击的判断和处理方式可能存在差异，缺乏统一的标准和规范，影响了响应的效果。

2.3 系统架构缺陷

现有入侵检测与响应系统大多采用集中式架构，这种架构将所有的检测和响应功能集中在一个中心节点上。虽然集中式架构在一定程度上便于管理和控制，但存在单点故障风险。一旦中心节点出现故障，如硬件损坏、软件崩溃或遭受攻击，整个入侵检测与响应系统将陷入瘫痪，无法对电力信息系统进行有效的安全防护。而且，集中式架构的可扩展性较差。随着电力信息系统规模的不断扩大和业务的日益复杂，系统的检测和响应任务会不断增加，集中式架构难以适应这种大规模、分布式的发展需求，无法及时有效地处理大量的安全事件。

3 电力信息系统入侵检测与响应机制优化方案

3.1 入侵检测技术优化

为了提高入侵检测的准确率和有效性，本文提出一种融合多种检测技术的混合检测模型。该模型结合了基于误用检测和基于异常检测的优势，同时引入深度学习算法和关联分析技术。深度学习算法具有强大的数据挖掘和特征提取能力，能够对系统日志、网络流量等数据进行深度分析。通过构建深度神经网络模型，对正常行为和异常行为进行分类训练。在训练过程中，模型会不断调整自身的参数，以最小化分类误差，从而提高对未知攻击的检测能力。例如，对于网络流量数据，深度神经网络可以学习到正常流量的特征分布，当出现异常流量时，能够准确识别并发出警报。关联分析技术则用于对不同来源的检测信息进行关联分析。在电力信息系统中，各种检测设备会从不同的角度收集安全信息，如网络流量监测设备、主机日志审计设备等。这些信息之间可能存在着潜在的关联关系。通过关联分析技术，可以将这些分散的信息整合起来，从多个维度对安全事件进行综合判断。例如，当检测到某个主机的网络流量异常时，结合该主机的系统日志信息，查看是否有异常的进程启动或文件访问操作。如果同时发现网络流量异常和系统日志中的异常操作，那么就可以更准确地判断是否存在真正的入侵行为，避免因单一检测信息的误判而导致误报。

3.2 响应策略优化

针对现有响应策略的不足，本文提出一种基于风险评估的主动响应机制。该机制首先对检测到的入侵行为进行全面的风险评估，综合考虑攻击的类型、来源、目标、潜在影响等多个因素。不同类型的攻击具有不同的危害程度，例如，DDoS 攻击可能会导致系统服务中断，而数据窃取攻击则可能泄露敏感信息。攻击的来源也可以反映其威胁程度，来自外部黑客组织的攻击可能比内部人员的误操作更具危险性。攻击的目标也很重要，如果攻击目标是电力系统的关键控制设备，那么其潜在影响将非常巨大。通过对这些因素的综合分析，确定攻击的风险等级。根据风险等级，制定相应的响应策略。对于高风险攻击，立即采取阻断网络连接、隔离受攻击设备等强硬措施，就像在敌人发起猛烈攻击时迅速筑起坚固的防线，阻止攻击的进一步蔓延，保护系统的核心部分不受损害。对于中低风险攻击，采用警告、限制访问权限等较为温和的方式进行响应，既能够对攻击者起到威慑作用，又不会对系统的正常运行造成过大影响。同时，引入自动化响应技术提高响应效率。通过预设的响应规则和脚本，实现响应过程的自动化执行。当检测到入侵行为并确定风险等级后，系统可以自动触发相应的响应脚本，无需人工干预即可完成阻断网络连接、发送警报信息等操作。这不仅大大缩短了响应时间，还能够避免因人工操作失误而导致的响应不及时或不准确的问题。此外，建立响应效果评估机制对每次响应行动的效果进行评估和分析。通过收集响应过程中的各种数据，如响应时间、攻击阻断情况、系统恢复时间等，评估响应策略的有效性。根据评估结果调整响应策略，不断优化响应机制，使其能够更好地应对不断变化的网络攻击。

3.3 系统架构优化

为了解决现有入侵检测与响应系统集中式架构存在的问题，本文设计一种分布式架构。该架构将入侵检测与响应功能分散到多个节点上，每个节点负责监测和处理本地的安全事件。节点可以部署在电力信息系统的不同位置，如发电厂、变电站、调度中心等，对各自区域内的网络流量、主机状态等进行实时监测。节点之间通过高速网络进行通信和协作，实现信息的共享和协同响应。当一个节点检测到安全事件时，它可以及时将相关信息发送给其他节点，其他节点可以根据这些信息调整

自己的监测策略或提供协助。例如，如果一个节点检测到针对某个变电站的攻击，它可以将攻击的特征信息发送给其他节点，其他节点可以加强对类似攻击的监测和防范。分布式架构具有诸多优点。一是提高了系统的可靠性和可用性，避免了单点故障风险。由于检测和响应功能分散在多个节点上，即使某个节点出现故障，其他节点仍然可以正常工作，保证系统的整体运行不受影响[3]。二是增强了系统的可扩展性，能够方便地添加新的节点以适应系统的扩展需求。随着电力信息系统规模的不断扩大，可以轻松地在系统中添加新的检测节点，提高系统的检测能力和覆盖范围。三是提高了检测和响应的效率，由于检测和响应任务在本地节点上完成，减少了数据传输延迟。本地节点可以快速对本地发生的安全事件做出反应，无需将数据传输到中心节点进行处理，能够更快地发现和阻止入侵行为，保障电力信息系统的安全稳定运行。

4 实验验证与分析

4.1 实验环境搭建

为了验证优化后的入侵检测与响应机制的有效性，搭建了一个高度模拟电力信息系统的实验环境。该环境包括多个服务器、工作站和网络设备，模拟了电力系统的发电、输电、配电等业务场景。服务器模拟电力系统的核心控制设备，如调度服务器、监控服务器等，负责电力系统的调度、监控和管理等关键业务。工作站则模拟电力系统的操作终端，供工作人员进行日常操作和数据处理。网络设备包括路由器、交换机等，用于构建电力信息系统的网络架构，实现各个设备之间的通信和数据传输。在实验环境中部署了优化前后的入侵检测与响应系统，优化前的系统采用传统的集中式架构和单一的检测技术，优化后的系统则采用本文提出的分布式架构和混合检测模型。同时，使用专业的网络攻击工具模拟各种常见的网络攻击，如 DDoS 攻击、SQL 注入攻击、木马攻击等，以全面测试系统的性能。

4.2 实验结果分析

通过对实验数据的收集和分析，对比优化前后入侵检测与响应系统的性能指标，全面评估优化机制的有效性。在检测准确率方面，优化后的系统表现出了显著的优势。对未知攻击的检测能力明显提高，能够更及时、准确地发现那些未在已知特征库中的新型攻击。同时，误报率和漏报率显著降低。误报率的降低得益于混合检测模型中关联分析技术的应用，通过综合分析不同来源的检测信息，避免了单一检测信息的误判。漏报率的降低则归功于深度学习算法对未知攻击特征的挖掘和学习能力，使得系统能够识别更多类型的攻击行为。在响应时间方面，基于风险评估的主动响应机制发挥了重要作用。该机制能够根据攻击的风险等级迅速制定响应策略，并通过自动化响应技术快速执行。实验结果表明，优化后的系统平均响应时间较优化前缩短了30%，能够更快地对入侵行为做出反应，及时阻止攻击的进一步蔓延，减少系统受损的程度。在系统可靠性和可扩展性方面，分布式架构的优化系统表现出了更好的性能。在面对节点故障时，其他节点能够迅速接管故障节点的工作，保证系统的整体运行不受影响，避免了集中式架构中单点故障导致的系统瘫痪问题。在系统扩展方面，当添加新的节点时，优化后的系统能够快速集成新节点的信息，实现无缝扩展，满足电力信息系统大规模、分布式的发展需求。实验结果表明，优化后的入侵检测与响应机制能够有效提升电力信息系统的安全防护能力，为电力系统的稳定运行提供有力保障。

结束语

电力信息系统的安全防护是一个不断发展和变化的领域，随着网络攻击技术的不断创新和电力行业的数字化转型加速，未来还将面临更多新的安全挑战。因此，未来的研究可以进一步探索更加先进的检测技术和响应策略，如利用人工智能和区块链技术提升系统的智能化水平和安全性；加强电力信息系统与其他行业信息系统的安全协同防护，构建更加完善的网络安全生态体系。同时，还应注重安全人才的培养和安全意识的提升，从多个层面保障电力信息系统的安全稳定运行。

参考文献

[1]陈新和. 探讨入侵检测技术在电力信息网络安全中的应用[J]. 通讯世界,2014,01:67-68.

[2]顾春晖. 基于云计算的电力信息系统安全技术讨论[J]. 电子技术与软件工程,2014,09:227.

[3]林云威. 基于故障树和DSET的电力控制系统信息安全风险评估[D].华东理工大学,2014.