计算机网络安全防护中入侵检测技术的应用

张维峰

河北赛克普泰计算机咨询服务有限公司 河北 石家庄 050000

【摘　要】：随着互联网技术飞速发展，网络攻击手段不断翻新，数据泄露、恶意入侵事件频发，计算机网络安全防护面临严峻挑战，入侵检测技术应用迫在眉睫，本文深入探讨计算机网络安全防护中入侵检测技术的应用。阐述入侵检测技术原理、分类，分析基于主机、网络及分布式入侵检测系统特点，研究其在网络安全防护各场景的具体应用及面临挑战与发展趋势，旨在为提升计算机网络安全防护水平提供理论与实践参考。

【关键词】：计算机网络安全；入侵检测技术；网络防护

DOI:10.12417/2705-0998.26.10.090

在数字化浪潮席卷而来的今天，计算机网络已经成为社会运转，经济发展以及信息交互的核心。在企业数据管理、个人隐私保护、金融交易安全、关键基础设施运行等方面，网络安全都具有十分重要的意义。但是黑客攻击，恶意软件传播和数据窃取等安全威胁不断出现，传统防护技术已经很难满足人们越来越复杂的安全需求。入侵检测技术是网络安全防护体系中的一道重要防线，可以对异常行为及潜在攻击进行实时监控、识别，对风险预警和防御起到至关重要的作用。深入进行应用研究，对于健全网络安全防护体系，确保网络空间安全有着十分现实的意义。

1 入侵检测技术综述

1.1 定义和概念

入侵检测技术（简称 IDS）是保障计算机网络安全的关键技术之一，旨在实时监测网络环境中违反安全策略或存在潜在威胁的行为。其通过对网络流量，系统日志，用户行为等多源数据进行采集与分析，按照设定的规则或者算法识别出未经许可的接入，恶意攻击或者异常操作，对网络安全防护体系的动态监测和预警能力。入侵检测系统就像网络中的“免疫系统”，能对安全威胁进行及时的发现和反应，和防火墙这种静态防护手段相辅相成，共同筑起网络安全防线[1]。

1.2 基本原理

通过布设于网络中关键节点或者主机的传感器采集网络数据包，系统调用记录和用户登录信息。接下来，我们采用了基于误用（特征匹配）或异常（行为基线对比）的分析方法，对收集到的数据进行了深入的处理。根据错误使用情况进行检测，并与已知攻击特征库进行匹配，确定威胁；在异常基础上进行检测，然后通过构建正常行为模型来确定偏离模型是否存在异常。最后当发现潜在威胁时，系统会立即启动报警机制按照预设策略进行响应，如阻断连接和隔离主机以达到及时处理安全事件。

2 入侵检测技术在计算机网络安全防护的价值

2.1 主动防御能力增强

传统的网络安全防护更多是被动防御，依靠事先制定好的访问控制规则来抵抗攻击，利用入侵检测技术，由被动防御变为主动防御，可以对网络活动进行实时监控，对可能存在的威胁进行主动识别，当攻击还没有造成实质上的损害时就会进行预警和应对，从而有效地减少了攻击的成功概率[2]。入侵检测系统通过不断地对攻击特征库进行学习和更新，能够及时地发现新的攻击手段并为网络安全防护争取到有价值的反应时间，显著增强了网络主动防御能力。

2.2 安全事件准确溯源

当网络安全事件爆发时，精准的事件溯源对于识别攻击来源，分析攻击路径，评估损失以及制定后续防护策略至关重要。入侵检测系统因其出色的数据收集和记录能力，能够在攻击过程中完整地保存所有关键信息，这包括攻击的时间、源 IP 地址、攻击的种类以及涉及的系统资源等。这些翔实数据对安全事件进行深度分析和精准溯源，有助于安全人员迅速定位攻击源头并阻断攻击链路，同时对攻击规律进行了总结，以期对后续的安全防护起到经验借鉴。

2.3 网络安全态势感知

入侵检测技术对大量网络数据进行分析和处理，可以实时感知网络安全态势。其不仅能够对单个攻击事件进行识别，而且能够通过关联分析发现攻击事件之间潜在的关联，从而构造出网络安全威胁全景图。

作者简介：张维峰（1981—），男，汉族，河北安国人，大专学历，研究方向为网络安全。

安全管理人员可以通过可视化显示网络安全态势来直观地了解整个网络的安全状况、及时发现潜在风险区域并对安全防护策略实施效果进行评价，为网络安全决策、实现全局把控和动态管理提供科学依据。

2.4 合规性和风险管控

企业和机构网络安全管理，符合行业规范和法律法规的要求是一个重要的目标。入侵检测系统对网络活动进行连续监控，以保证网络行为满足设定的安全策略和合规要求，从而为企业通过审查合规性提供了强有力的支撑。与此同时，还可以对网络安全风险进行有效的识别和量化，有利于企业对风险等级进行评估，有针对性地制定风险管控措施以减少安全事件造成的经济损失和声誉损害，确保企业业务持续平稳经营。

3 入侵检测技术在计算机网络安全防护的方法

3.1 机器学习检测法

在计算机网络安全防护中，机器学习检测法由于其具有较强的自学习和智能分析能力，而成为入侵检测技术发展的一个重要趋势，传统的以规则匹配为核心的入侵检测方式很难处理新型和变种攻击，机器学习算法可以自动地从大量网络数据中进行特征提取和模式识别，本发明打破了人工定义规则限制，明显提高了入侵检测精度和适应性，监督学习算法对于入侵检测起到了至关重要的作用，该算法通过对已知的正常和异常的网络行为数据进行标注并构造训练模型可以学习到攻击行为和正常行为之间的特征差异[3]。决策树和支持向量机这样的算法能够对新的输入数据进行精确的分类和预测，能够准确地识别出与已知攻击模式类似的潜在威胁。以决策树为例，该算法可以通过网络流量源 IP，目的端口和数据传输频率多维度特征的层级划分来迅速判断有无恶意行为发生。半监督学习方法主要适用于某些标记数据的场景。在有限的已知攻击样本的基础上，结合了大量的未标记数据来进行模型的训练，从而深入挖掘可能的攻击模式，并有效地满足对未知攻击的检测需求，无监督学习算法从一个不同的角度为入侵检测提供了支持，该类算法不需要事先对数据进行标注，利用聚类分析和异常点检测来检测出数据是否存在异常模式。在对网络流量进行监控时，无监督学习算法能够依据数据包大小和传输时间间隔的特点对类似的流量行为进行聚类，发现与正常聚类存在偏差的异常流量并及时发现隐蔽攻击。深度学习算法，例如卷积神经网络（CNN）和循环神经网络（RNN），因其出色的特征抽取和序列分析功能，在处理复杂的网络数据时表现出了不可替代的优越性。CNN 能够有效地提取网络流量图像化之后的空间特征，而 RNN 适合对有时序性攻击行为进行分析，两者结合可以更加综合地发现网络攻击。机器学习检测法不断地对算法模型和训练数据进行优化，不断地提高检测精度和检测效率，从而为网络安全防护工作提供智能化技术支持。

3.2 数据融合检测

数据融合检测通过对多源异构数据进行融合来深入发掘数据之间的潜在联系，从而增强入侵检测的准确性和可靠性，在复杂网络环境下，单一数据源信息通常存在局限性，很难综合反映网络的安全状态，数据融合技术则是通过针对不同种类、通过对不同源数据的全面分析可以克服这一不足，构造出更加全面的网络安全态势视图，在数据融合检测中，网络流量数据、系统日志数据和用户行为数据作为主要数据源[4]。网络流量数据中包括数据包传输方向，协议类型和流量大小，可以直观地反映网络通信状态；系统日志是对系统运行中各种事件的记录，如用户登录和程序调用，可用来在系统层面上发现异常运行情况；从用户的操作习惯和访问频次等多个维度出发，用户行为数据揭示了用户行为的不正常波动。整合这些数据可以实现对网络行为安全性在多维度上的交叉验证，实现数据融合检测时需要采取适当的融合策略。特征级融合就是把不同数据源中抽取出来的特征融合在一起组成一个新特征向量然后分析检测。在识别分布式拒绝服务（DDoS）攻击的过程中，通过将网络流量的峰值特性与系统日志的资源使用特性进行整合，我们可以更为精确地确定攻击的具体行为。在决策级的融合过程中，首先对不同的数据源进行独立的分析和决策，然后对这些决策结果进行整体评估。当发现病毒入侵后，可以综合根据网络流量分析和根据文件特征扫描两种方法进行投票和加权，从而得到最后的结论以减少误报率和漏报率。另外，在物联网和工业互联网蓬勃发展的背景下，设备状态数据和传感器数据等新数据源逐步融入融合范围中，数据融合检测应用界限得到进一步扩展。通过数据融合检测可以有效地弥补单一数据源存在的缺陷，提高入侵检测系统对复杂攻击的鉴别能力，从而为网络安全防护工作提供更加全面的保证。

表 1 数据融合检测

数据源类型	数据内容	描述
网络流量数据	数据包传输方向、协议类型、流量大小	反映网络通信状态
系统日志数据	用户登录、程序调用等事件记录	发现系统层面上的异常运行情况
用户行为数据	操作习惯、访问频次等	揭示用户行为中的不正常波动

3.3 云环境下的分布式检测

云环境的资源动态分配，服务弹性扩展和多租户共享的特点使得传统的集中式入侵检测方式已经很难满足其复杂的架构和海量数据处理的要求。云环境下的分布式检测技术，通过在众多节点上分散完成检测任务来实现云环境下网络安全的有效和准确监控，已成为确保云服务安全的重要技术途径，云

环境下的分布式架构，决定入侵检测系统需要采取与其相适应的分布式部署方式[5]。在基础设施即服务（IaaS）的层次上，可以在虚拟主机、虚拟网络设备等资源中部署轻量级的检测代理，以实时收集虚拟机的系统日志、网络流量和其他数据以及向中央管理节点发送关键信息。在平台即服务（PaaS）和软件即服务（SaaS）这两个层次上，我们需要对云平台的服务接口和用户的访问习惯进行深入的监控。通过将分布式检测节点部署到不同服务层次上，实现了云环境下全链路数据覆盖获取和分析，分布式检测以数据协同处理和智能分析为核心内容。每个检测节点对本地采集到的数据做初步过滤和特征提取以降低数据传输的压力，然后把关键信息上传到中央管理节点。中央管理节点利用分布式计算框架，例如 Hadoop、Spark 等，对多节点数据进行分布式存储和并行处理，从而快速分析数据之间的关系。当检测到对云数据库有攻击行为时，可以综合多种数据库实例访问日志和流量数据进行分布式关联分析来确定异常访问模式。同时采用分布式机器学习技术对每个节点上的检测模型进行自主训练，通过模型参数同步机制进行全局模型优化以增强云环境下新攻击检测能力。另外云环境下的分布式检测需要兼顾数据隐私和安全，并通过加密传输和访问控制来保证数据在检测时的保密性和完整性，从而保护了用户的数据权益，同时也保证了云服务的安全性。

3.4 物联网的轻量检测

物联网具有设备多，资源有限，通信协议种类繁多等特点，使得传统的入侵检测技术很难直接运用到物联网场景中。通过优化算法和架构设计来减少检测系统资源消耗、实现物联网设备和网络高效安全防护的物联网轻量检测技术已成为破解物联网安全难题的重要手段。

物联网设备一般计算能力较弱，存储容量较低，能量受限，需要在算法层面上对轻量检测技术加以优化，在物联网设备中很难直接操作传统的复杂机器学习算法，因此出现了轻量级的机械学算法。通过简化模型结构和压缩模型参数等措施，减少了对计算和存储的要求，同时保证了检测精度。通过决策树剪枝和模型量化，使得机器学习模型可以在资源有限的物联网设备中快速工作，从而达到实时发现设备中存在异常行为。另外，规则化轻量检测方法在物联网场景中得到了广泛的应用。通过提取物联网特定协议（如 MQTT、CoAP）的特征规则，对设备通信数据进行快速匹配检测，能够有效识别协议层面的攻击行为，架构设计中物联网轻量检测使用分层协同方式，边缘层设备承担着本地收集到数据的初步加工和筛选工作，只把可疑数据上传到网关或者云端。网关是物联网和外部网络之间连接的枢纽，可以部署有一定处理能力的检测模块来进一步解析边缘设备上传数据，实施一些响应策略比如屏蔽恶意连接等。云端主要负责对大量数据进行深入的分析和全局的安全态势感知，通过整合各种网关数据，能够识别出跨越不同设备和区域的攻击行为。与此同时，在物联网中进行轻量检测也需要综合考虑设备异构性和通信协议多样性所带来的各种挑战，并通过对通用数据采集和分析接口的设计来实现对不同种类设备和协议的兼容，以保证检测系统可扩展性和适用性。通过物联网轻量检测技术实现了物联网安全威胁有效保护，确保了物联网生态系统平稳运行，同时不会加重设备负担。

4 结语

入侵检测技术对计算机网络安全防护具有显著效果，但是随着网络环境的改变和攻击手段的演变，仍然面临许多挑战。需要不断探索和创新，促进技术的智能化发展和多技术的融合发展，提高检测的准确性和效率，从而为计算机网络安全的实现提供更加强有力的保障。

参考文献：

[1] 党林.电力系统网络安全维护中入侵检测技术的应用分析[J].电子技术与软件工程,2022,(21):225-228.

[2] 史海丽.入侵检测技术在电力信息网络安全中的应用[J].科技经济导刊,2020,(21):15-18.

[3] 王先培,熊平,李文武.防火墙和入侵检测系统在电力企业信息网络中的应用[J].电力系统自动化,2022,26(05):60-63.

[4] 伍晖平,金亚民,蔡青有.入侵检测技术在电力信息网络安全中的应用[J].电力安全技术,2020,(10):38-40.

[5] 费强.基于大数据时代防火墙和入侵检测技术在网络安全中的运用分析[J].网络安全技术与应用,2022,(06):10-11.