文章类型：论文|刊号（ISSN）：2972-4112(P) / 2972-4120(O)

基于图像处理的网络安全入侵检测方法研究

徐东　张旭华
陕西能源职业技术学院
DOI:10.32629/pe.v3i6.18031

[摘　要] 随着网络规模扩大以及业务类型的多样化,网络攻击变得隐蔽性更强、类型更多样也更为长期,传统基于规则或统计特征进行入侵检测的方法,面临复杂攻击环境下的检测不准确性和泛化能力受限等问题。基于此,本文针对现有网络入侵检测对异常行为描述能力不足的问题,借鉴图像处理思想将高维度抽象、实时变化的网络流量转化为可识别的图像表示形式,构建了基于图像特征的网络入侵检测方法体系框架；并借助流量图像构造、图像特征提取以及图像分类器设计,达到了对不同攻击类型进行有效区分的目的,其具有较高的精确度及鲁棒性,为网络入侵检测方法的研究提供了一个新思路。
[关键词] 网络入侵检测；图像处理；异常行为识别
中图分类号：TP751　文献标识码：A

Research on Network Security Intrusion Detection Method Based on Image Processing

Dong Xu　Xuhua Zhang
Shaanxi Energy Vocational and Technical College

[Abstract] With the expansion of network scale and the diversification of business types, network attacks have become more concealed, more diverse in type and more long-term. Traditional intrusion detection methods based on rules or statistical features are facing problems such as inaccurate detection and limited generalization ability in complex attack environments. Aiming at the problem that the existing network intrusion detection has insufficient ability to describe abnormal behaviors, drawing on the idea of image processing, the high-dimensional abstract and real-time changing network traffic is transformed into a recognizable image representation form, and a framework of the network intrusion detection method system based on image features is constructed. By means of traffic image construction, image feature extraction and image classifier design, the purpose of effectively distinguishing different attack types has been achieved. It has high accuracy and robustness, providing a new idea and direction for the research of network intrusion detection methods.
[Key words] Network Intrusion Detection; Image processing; Network traffic analysis; Abnormal behavior recognition

引言

在现代网络环境中,随着信息技术的迅猛发展与广泛应用,网络安全问题日益严峻,入侵检测成为确保系统安全的重要手段。传统入侵检测技术已难以应对复杂多变的攻击模式和日益增长的数据量。网络安全入侵检测作为信息安全领域的关键技术,其核心目标是识别并响应网络系统中未经授权的访问或恶意行为。该过程涉及对网络活动的持续监控,通过分析网络流量、系统日志等数据,检测异常或可疑模式,及时发现并阻止潜在的安全威胁。本文尝试将网络流量数据转化为图像形式,引入图像特征分析方法,构建基于图像处理的网络入侵检测模型,并通过实验验证其有效性与可行性。

1 网络入侵检测与图像处理技术基础

1.1网络入侵检测方法的基本原理与发展现状

网络入侵检测目的是监控网络通信和系统的运作状况,以找出任何异于常规的行为或者恶意操作。基本理念是构建并应用一种标准化行为模板来对比实时信息。依据不同检测策略,这种方法可以分为两类。一是利用预先定义好的攻击特征进行匹配的技术；二是基于行为统计模型发现异常的方法。随着网络空间日益动态化、多变化,入侵检测由单一特征检测向混合式特征检测发展,这也给这两组数据的表现形式及分析方法提出了更高要求。

1.2网络流量数据的结构特征与可视化基础

由于网络流量通常具有高维特征、强时序性和较强的非线性程度,其蕴含的关键信息有可能分散在诸如协议类型、端口

号、数据包长度、时间间隔等多个特征上,而直接使用数值或者字符串表示的方法则很难对其整体进行把握,进而影响了对复杂关系的发现。采用可视化的方法将上述多种多样的流量特征映射为二元或多维的可视对象,有助于数据分布形式及变化更容易被观察,也提供了一种新的视角去审视异常行为[1]。合适的可视化设计可在不丢失原始数据信息的前提下,揭示网络流量活动的整体结构特点,有利于后续研究的开展。

1.3图像处理方法在安全数据分析中的适用性

基于图像处理技术,在特征提取以及分类识别方面有着很大优势,可以从空间结构与形态变化中分析出蕴含的数据内在规律性。将网络安全的信息转化为图像形式后,复杂的多维速度信息可以被转化为具有空间分布特性的可视对象,入侵行为可以在图像中表现为特殊的结构或者纹理图案[2]。这样的描述方式有助于降低直接使用高维度数字带来的分析困难,并且能够更好地描述异常行为的整体特征信息。影像运算方法在边缘检测、区块分割以及特征提取等方面有成熟的应用基础,对网络流量中所包含的噪声及扰动具有一定的容忍能力,适用于对复杂网络环境下的网络安全信息进行分析。应用图像处理的思想能够为网络攻击探测提供稳定而可扩展的分析方法。

2 基于图像处理的入侵检测方法构建

2.1网络流量数据的采集与图像化表示方式

采用基于图像处理的方法进行入侵检测的前提条件是采集到规范化的网络流量信息,在实际网络环境中,流量信息是由镜像端口、探针设备及日志服务器获取的,这些信息中包含了数据包时间戳、源地址、目的地址、源端口号、目标端口号、使用的协议类型、数据包长度等要素。在进行后续分析之前,需要清洗噪声、冗余数据,并将连续的时间窗口划分为标准形式的特征序列。而在图像表示阶段,将选取几个重要的流量属性并将其投影到二维空间中,在像素点上以灰度值或者亮度值的形式展现该属性的数量变化,这样时间性和性质性便在图像中生成可识别的空间形式。常见做法是将时间窗口内的特征值归一化后填充为图像矩阵,其映射关系可表示为:

$$I(i,j)=\frac{F(i,j)-F_{\min}}{F_{\max}-F_{\min}} \tag{1}$$

其中,I(i,j)表示图像中第i行第j列像素值,F(i,j)为对应的网络流量特征值。通过该方式,抽象的网络流量数据被转化为具有结构特征的图像,为后续特征提取与入侵识别奠定基础。

2.2入侵行为图像特征的提取与表达方法

在完成网络流量数据可视化表示后,从图像中抽取能够表征正常行为和异常行为的特征是十分重要的一步。通常来说,攻击性行为在图像中的表现形式会与正常行为流量分布不同,如亮度较高、纹理不连续或分布位置不规律等,因此需要关注图像的变化及整体趋势。常用方法包括基于灰度统计提取特征的方法,分析纹理特性反映流量活动的空间分布规律以及突出边界的区域结构特征的重要性。灰度特征能够体现流量大小的整体起伏变化趋势,纹理特征便于描述各类流量活动的空间分布特征,边界和区域特征更适合表现异常流量突现性和集聚性的图示特征[3]。特征表示阶段,将获取到的二维图像特征进行归一化整理形成有序的特征向量,以便于后期分类器的整体操作,复杂攻击动作被转化为具有判别意义的特征字符,进而提高鉴别精度。

2.3基于图像特征的入侵识别模型设计

获得结构化图像特征向量后,为保证正常流量和其他各类入侵类型能被正确区分而建立的入侵检测模型的核心过程,主要包括标记、输入、分类以及输出四个环节。考虑到入侵检测类别不平衡性和样本差异性等特点,可采用“两次识别”方法。先进行二值识别,区分是行为还是非行为;再对识别结果中的非行为进行细粒度的攻击类别识别,以降低误报并提升多态性识别性能。在模型选取上,传统分类器如SVM和RF适合于中等甚至较低维的特征,其具有较低的培训成本并更适合于小规模的数据集。但是,当图像特征维度很大或纹理结构较为复杂的情况下,则可以使用卷积特征提取和分类单元相结合的方法进行实现,并将局部纹理信息以及全局结构信息共同融入决策过程中。为了避免模型发生过拟合现象,需要交叉验证以及正则化约束来作为培训的一部分,并且还要使用网格搜索对于关键的超参数配置来进行训练,这样才能确保模型能以稳定的方式运行在不同网络环境上。最终输出不仅提供入侵预测,而且还能提供置信度等级阈值和警报级别,实现面向实际防护的可用性设计[4]。

2.4检测流程与系统整体架构实现

基于图像处理方法的入侵检测系统既要考虑处理效率又要保证检测准确率,其流程包括数据采集、预处理、图像建模、特征提取、入侵判断以及入侵结果汇报六个阶段。首先采用流量捕获装置进行数据获取,接着进行清洗、规范化以及窗口定时,使得录入的数据格式统一,再由图像建模模块将整理后的流速属性转化为图像形式,供后续使用。该环节中,特征提取单元将其中可区分性表示信息提取出来,发送至分类单元进行分类判断。系统架构设计为模块化,各功能模块之间相互独立并且以通用接口传递信息,方便后期系统维护及功能扩展[5]。报警和日志模块用来产生所有检测到的异常行为的信息,以便展示并存储在数据库内。这种整体架构在保证检测精度的基础上,提高了系统的鲁棒性及适应性,满足实际网络环境中的部署需求。

3 实验设计与检测性能分析

3.1实验环境与数据集构建说明

为验证基于图像方法进行网络安全监测的有效性,在实验室内搭建模拟实验平台,采用常规的局域网拓扑结构。由采集信息的服务器、中心管理机构以及连接不同节点的交换机组成,这些部分可以模仿正常的商业活动和各种异常访问模式。在这个阶段,连续捕捉网络流量,会获得包含多个协议、多个接口和不同流量强度的数据样本。在创建数据集中,第一步是清理原始的网络流数据,去除重复或缺少的信息,然后根据时间窗重新组织,得到结构相同的网络流样本,然后对每一个样本进行标注来

区分正常流量及攻击流量，并以一定比例划分为训练集以及测试集，以保证实验评估结果的有效性及客观性。

3.2检测性能评价指标与测试方法

为全面评价基于图像识别方法的安防监控系统性能，设计了基于混淆矩阵的分类结果导向型的评价指标体系。主要采用混淆矩阵作为评价工具，通过对各类别判别结果统计，定量分析模型效果。选取的主要评价指标有准确率、误检数量和漏检数量。可以分别体现整体系统辨识性能、对合法流速误判情况及漏检可疑攻击动作的情况。在实验方案设计上，采用在固定数据集内，以脱离真实应用场景的方法进行离线检测流程；将构建的数据集分为训练样本和测试样本两个部分，随后采用相同的设置完成模型学习及性能测试；为了消除随机因素对实验的影响，将多次重复实验所得平均数作为最终得分，并结合不同参数组合作出的表现差异，对检测方法的稳定性进行分析。

3.3实验结果与对比分析

在完成实验测试后，对基于图像处理的入侵检测方法与传统检测方法的性能进行对比分析，以验证所提方法的有效性。结果表明，对复杂入侵行为采用图像特征进行表示优于直接使用原始流速度数据，不仅可以提高检测率而且还能降低误报和漏检的概率。相对于单一流速特征的方法而言，该算法在对异常流量进行识别时稳定性更强，在混合不同种类的攻击场景下其识别性能相对稳定一些。为评估各方法的表现情况，基于相同的测试样本集以精确度、误检率以及漏检率作为指标开展评测工作。实验结果显示，基于图像特征的方法在综合性能指标上整体优于对比方法，验证了图像处理思路在入侵检测中的应用价值。具体结果见表1。

表1 不同入侵检测方法性能对比结果

检测方法	准确率(%)	误报率(%)	漏报率(%)
传统特征匹配方法	89.6	6.8	3.6
基于统计特征的异常检测方法	91.2	5.9	2.9
基于图像处理的入侵检测方法	95.4	3.1	1.5

从对比结果可以看出，基于图像处理的入侵检测方法在各项指标上均取得较优表现，验证了其在复杂网络环境中的应用潜力。

3.4检测效果分析与结果讨论

综合实验结果可以看出，图像化入侵检测方法整体检测性能稳定，在不同网络流量特征变化下，均可取得良好检测效果。图像化表征形式提升了入侵行为的特征空间可区分性，有利于异常流量的识别并减少漏检率。这种算法在混合型攻击仿真场景中，仍能较好地检测出混合攻击行为，说明其在实际网络环境中具备一定的适用性。但是，也应该看到图像化建模过程以及特征提取过程受参数设置以及样本数量影响较大，当网络流量特征出现较大变化时，检测性能仍可能受到影响。后续研究可致力于增强表征特性的能力以及模型自适应性，以增强方法在动态复杂网络环境下的稳定性和普适性。

4 结语

基于图像处理的网络入侵检测方法将流量信息映射为图像，形成完整的特征提取、特征模板生成以及检测流程，并能有效识别异常行为。实验结果表明，该方法具有良好的准确率和稳定性，在一定程度上弥补了传统查验技艺面对复杂攻击过程中的不足之处。相关分析显示，将图像处理思想引入网络安全领域，可增强入侵行为特征描述能力以及对入侵检测技术提供新的实现思路。但在实际应用中，仍无法摆脱因网络环境差异性和数据规模变化的影响而出现的局限性。后续工作可围绕其核心特征解释性的增强及扩展应用范围等内容进行研究，以增强其应用于复杂网络的实际意义。

[项目基金]

(1)2025年陕西能源职业技术学院校级科研基金“基于图像感知与分析的管道内部缺陷智能检测技术研究”(编号：2025KYZRP01)；(2)2022年陕西能源职业技术学院校级科研基金“基于我校一卡通数据挖掘的贫困生资助评价模型研究”(编号：2022KY11KJP)。

[参考文献]

[1]胡萍.基于图像处理的城市轨道交通线路异物检测与识别[J].自动化与仪器仪表,2022(7):23-27.

[2]康恺,毛一凡,周钢泉.电力变电站图像识别与入侵检测系统设计[J].信息与电脑,2024,36(16):95-97.

[3]刘联海,黎汇业,毛冬晖.基于图像凸包特征的CBAM-CNN网络入侵检测方法[J].信息网络安全,2024(9):1422-1431.

[4]李伟.基于深度学习的网络安全入侵检测与防御技术研究[J].电脑乐园,2023(3):31-33.

[5]栾宁.计算机网络安全的入侵检测技术研究[J].微型计算机,2024,(7):3-6.

作者简介：

徐东(1997--),男,汉族,陕西渭南人,硕士,助教,研究方向：网络安全。

张旭华(1987--),女,汉族,山西临汾人,硕士,副教授,研究方向：计算机应用。