入侵检测系统的识别机制探索分析

樊亚娟

湖南信息职业技术学院，湖南 长沙 410203

摘　　要： 入侵检测系统作为信息安全行业中检测网络数据流量异常的机制，是防护网络攻击不可忽视的组成部分。入侵检测特征库目前主要有基于异常和误用两种识别和判断方式，在这两种方式固定识别特征的情况下，就会造成非法数据的利用给系统造成一定的损失。本文主要通过分析入侵检测传统机制的检测过程发现其应用弊端，并且尝试建立新的理论检测模型来提升检测机制的精确度和全面性。

关 键 词： 入侵检测；差分网络；对抗网络

中图分类号： TN915.08　　**文献标识码：** A　　**文章编码：** 2023040191

Exploration and Analysis of Recognition Mechanism of Intrusion Detection System

Fan Yajuan

Hunan College of Information, Hunan, Changsha 410203

Abstract: Intrusion detection system as a mechanism for detecting network data traffic anomalies in the information security industry is an integral part of protection against network attacks that cannot be ignored. Intrusion detection feature library is currently based on anomalies and misuse of two identification and judgment methods, in the case of these two ways to fix the identification of features, it will result in the use of illegal data to the system causing certain losses. This paper mainly analyzes the detection process of the traditional mechanism of intrusion detection to find out the disadvantages of its application, and tries to establish a new theoretical detection model to improve the accuracy and comprehensiveness of the detection mechanism.

Key words: intrusion detection; differential network; adversarial network

入侵检测系统（简称 IDS）是一种专门用于检测网络数据中是否存在异常或者违规行为的安全防御技术，目前它的实现原理主要通过收集和分析网络流量数据，然后根据自己特征库的策略和规则进行特征识别和对比，确定其网络数据流量是否处于正常状态，在这个对比过程中，如果特征库匹配上数据流量特征属于非正常流量的话，那么这种检测机制称为基于误用的检测匹配机制；如果特征库规则没有匹配数据流量特征被判定为属于正常流量，则这种检测机制称为基于异常的检测匹配机制。

一、入侵检测系统概述

异常检测技术也被称为基于行为的入侵检测技术，它主要通过将收到的数据与存储在特征库里面的正常行为的数据进行对比，判断收到的数据是否偏离正常行为来进行异常的评估检测，从另外一个方面来看，这种方式不依赖于发生异常的具体行为，所以很可能会导致很多未知的正常行为也会被识别为异常行为（比如系统故障、人为失误等操作）。这种类型的检测技术对入侵行为和攻击行为的防御性很强，适用于已知攻击类型很少或者攻击行为难以预测的情况，最典型的适用场景是内部攻击，但是在实际应用中，正常数据的行为基线没有办法做到永久或者长期不变，所以异常的检测机制很大概率会出现大量数据被误报的可能性，因此这种对于正常行为的模型建立是入侵检测系统很大的一个挑战，需要不断的对特征库进行调节，并且很需要人力和时间。

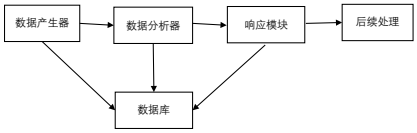
误用检测技术也被称为基于知识的入侵检测技术，它的特征库里面所记录的是已知的数据类型和攻击类型，主要通过将收到的数据和特征库的攻击数据类型进行对比来实现入侵检测的功能，这种检测方法的实现过程是规则匹配的过程，能够有效的降低数据的误报率，快速的发现已知类型的攻击行为，适用于已知攻击类型很多的情况或者攻击者的行为比较容易预测的情况（比如蠕虫病毒、端口扫描等）。但是由于该检测方法的特征库只能加入已知攻击的数据特征，所以如果出现了未知攻击并且不知道其特征的情况下，那么入侵检测系统将无法识别，对此类数据也不会进行异常警告，也很可能对系统网络造成一定的损害。

综上所述，传统的入侵检测机制不管是基于异常或者基于误用的检测，都必然会存在误报或者漏报的情况，最根本的原因还是特征库无法根据攻击的行为特征或者正常行为的特征进行及时的更新和识别，如果可以做到自动更新和识别学习的情况下，或许识别的精确度就会又上一个阶梯。

二、基于深度学习的入侵检测技术

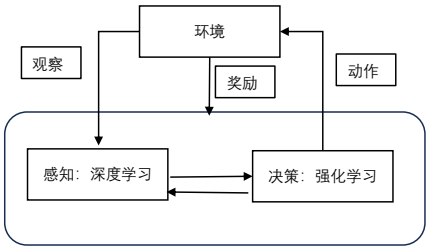
2010年，Sommer提出一个在入侵检测系统中应用机器学习的概念，也称为基于机器学习的入侵检测模型，这个模型通过机

器学习算法学习正常的网络数据和网络行为，不再是固定的检测已知的攻击类型或者已知的正常行为，在此之后大量的数学算法都被研究者尝试融入到入侵检测模型中，在这样的背景下，更加突出了机器学习在入侵检测领域的重要性，尽管传统机器学习的方法在网络入侵检测方面突出了一定的作用，但是由于传统特征库需要花费大量的时间和人力去判断特征是否合适，而且一旦遇到大规模的数据流量检测时检测效率就极其低下，所以在各种学术算法都考虑应用到入侵检测领域后，也一步步在开始证明深度学习技术在网络入侵检测方面的精确度和超强表现力，以下是入侵检测模型的系统架构。



> 图1 入侵检测系统架构

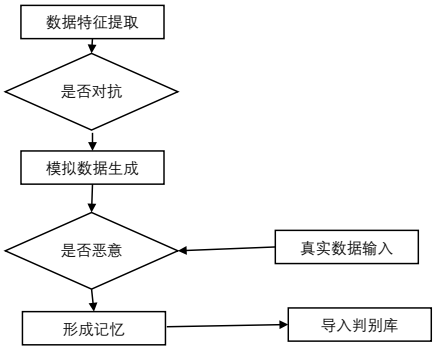
在基于深度学习的入侵检测技术的研究成果越来越丰富之后，很多学者进行了测试和实验，实验数据表明基于深度学习的入侵检测模型在建模时精确度越高，模型的参数就越多，会导致在模拟学习的时候训练的时间很长，而在现实环境中，由于许多异常检测样本都没有标签，所以又需要人工标注标签，这也会间接导致成本增高，所以学者们又在基于深度学习的基础知识提出了基于强化学习的入侵检测模型，这个模型提出来也会在一定程度上缓解了入侵检测模型的耗时和耗力问题，学习架构如下图所示：



> 图2 深度强化学习框架

三、基于对抗网络的入侵检测模型

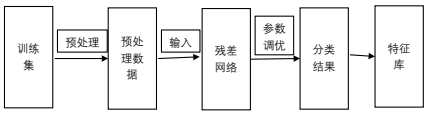
2007年张琨于则指出了针对传统机器学习在入侵检测机制所存在的问题，并且选择了以特征为导向的入侵检测策略进行建模。对抗网络作为深度学习神经网络的模型之一，很早就被称为生成领域“20年来机器学习领域最酷的想法”。在U gan将高斯噪声加入到生成对抗网络的判别器后，判别器的判断精确度就被大大的提高，在Beaulieujones B K将差异隐私训练纳入深度神经网络后，生成器的所生成的模拟数据也越来越接近于真实数据，为利用该模型的相关领域提高了强有力的测试保证。Fiore U利用对抗网络做过对恶意软件的检测实验，结果表明在增强集上训练的分类器性能优于在原始数据上训练的相同分类器，产生了有效欺诈检测机制。与此同时很多学者在K- means 聚类算法的基础上，与真实网络环境相结合实现了对网络数据信息的聚类分析，从而进一步完善了网络入侵检测系统。将对抗网络应用到入侵检测系统的架构如下：



> 图3 对抗网络应用到入侵检测系统架构

四、基于残差网络的入侵检测技术

残差网络是一种通过残差模块来构建深层网络的手段，这种网络架构不仅容易优化而且能够通过增加深度来不断提高准确率，如果可以在入侵检测系统加入残差网络用于特征识别的话，那么识别的精确度将会被大大提升。残差模块用于入侵检测任务时，可能会存在无法有效处理入侵检测数据的特性，主要原因是因为残差模块着重于提取局部特征比较优秀，但是对不具有图像的空间结构数据处理能力比较弱，所以可以进一步考虑在残差网络中融入注意力机制，该机制可以模拟大脑对捕捉的数据进行深度学习，可以提升残差模块在处理复杂数据的能力和识别度。其中残差网络的实现原理如下图所示：



> 图4 残差网络数据处理架构

五、总结

综上所述，入侵检测系统的检测机制识别精确度低是行业内一直在不断完善和改进的问题，目前关于将新技术融入到入侵检测机制的理论模型很多，但是实际应用案例却屈指可数，根据国内外相关的实验表明，融入对抗网络功能提升入侵检机制精确度，也很有可能是预防人工智能应用中的AI诈骗的一直重要手段。

参考文献

[1]王琛灿，徐杨斌，范乙戈等·计算机网络安全防御系统的实现及关键技术探析［J］. 网络安全技术与应用，2021（5）：20-22.

[2]冯亚丽. 计算机网络技术的应用及安全防御策略研究［J］. 电子元器件与信息技术，20215（3）：131-132,135.

[3]张蕾，崔勇，刘静，等. 机器学习在网络空间安全研究中的应用［J］. 计算机学报，2018,41(9):1943-1975.