Operations Research and Fuzziology 运筹与模糊学, 2024, 14(2), 1315-1322
Published Online April 2024 in Hans. https://www.hanspub.org/journal/orf
https://doi.org/10.12677/orf.2024.142228

Hans汉斯

基于网络多入侵行为识别的数学建模分析研究

肖丽丽

南京邮电大学理学院，江苏 南京

收稿日期：2024年2月9日；录用日期：2024年2月29日；发布日期：2024年4月30日

摘　要

在互联网飞速发展的同时，网络的安全性也越来越突出。网络入侵行为对信息系统和数据安全构成了严重威胁，因此网络入侵行为的识别和分析成为了网络安全领域的重要研究方向之一。本文以网络多入侵行为识别为研究对象，通过对入侵行为的数学建模分析，旨在提高网络安全防护水平。本文对网络入侵行为进行了分类和定义，明确了入侵行为的特征和类型。基于已有的入侵行为数据集，采用数学建模的方法对入侵行为进行了分析和建模。通过对入侵行为的数据特征提取和模式识别，建立了入侵行为的数学模型，并提出了相应的识别算法。在数学建模分析的基础上，本文还对网络多入侵行为的识别技术进行了探讨和研究。通过对入侵行为的特征提取和数据挖掘技术的应用，提出了一种基于网络流量和行为分析的入侵行为识别方法，并进行了实验验证和性能评估。研究指出了网络多入侵行为识别技术的意义和应用前景，为进一步提高网络安全防护水平提供了理论和技术支持。

关键词

多入侵行为识别，信任度计算，深度学习，建模仿真

Research on Mathematical Modeling and Analysis of Network Multi-Intrusion Behavior Recognition

Lili Xiao

College of Science, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu

Received: Feb. 9th, 2024; accepted: Feb. 29th, 2024; published: Apr. 30th, 2024

Abstract

With the rapid development of the Internet, the security of the network is also becoming more and

文章引用: 肖丽丽. 基于网络多入侵行为识别的数学建模分析研究[J]. 运筹与模糊学, 2024, 14(2): 1315-1322.
DOI: 10.12677/orf.2024.142228

more prominent. Network intrusion poses a serious threat to information system and data security, therefore, it is an important task to identify and analyze network intrusion. This paper takes the recognition of network intrusion behavior as the research object, and aims to improve the level of network security protection through the mathematical modeling and analysis of intrusion behavior. In this paper, the network intrusion behavior is classified and defined, and the characteristics and types of intrusion behavior are defined. Based on the existing intrusion behavior data set, the intrusion behavior is analyzed and modeled by mathematical modeling method. Based on the data feature extraction and pattern recognition of intrusion behavior, the mathematical model of intrusion behavior is established, and the corresponding recognition algorithm is proposed. On the basis of mathematical modeling analysis, this paper also discusses and researches the recognition technology of network multi-intrusion behavior. Through the application of feature extraction and data mining technology of intrusion behavior, this paper presents a new approach to IDS based on network flow and behavior analysis, and verifies it and evaluates its performance. The research points out the research significance and application prospect of network multi-intrusion behavior identification technology, and provides theoretical and technical support for further improving the level of network security protection.

Keywords

Multi-Intrusion Behavior Recognition, Trust Calculation, Deep Learning, Modeling and Simulation

1. 引言

随着互联网的快速发展和普及，网络安全问题日益引起人们的关注。网络入侵行为作为一种威胁信息系统和数据安全的行为，给个人、企业甚至国家的信息安全带来了严重的挑战。因此，网络入侵行为的识别和分析成为了网络安全领域的重要研究课题之一。在当前的网络环境下，传统的安全防护手段已经难以满足对抗复杂入侵行为的需求。因此，基于数学建模分析的研究成为了提高网络安全防护水平的重要途径之一。

近年来，近年来，针对网络安全的入侵检测系统(IDS)的研究和开发日益受到关注。这些系统旨在识别和识别网络中的异常行为，目的是防止未经授权的访问和潜在的网络攻击。提高 IDS 有效性的一种方法是通过使用数学建模和分析，这可以提供对网络行为和潜在入侵的更全面的理解。祝毅鸣，刘莹[1]研究提出：“对高度伪装的网络入侵行为优化识别，是保护网络安全的重要手段。随着网络入侵行为伪装性的不断增强，传统的入侵检测方法，主要通过对网络入侵行为特征进行识别的，需要根据疑似入侵特征的相似性，进行迭代计算，一旦伪装程度较高，需要多次计算，效率偏低。”该方法通过对网络行为进行多尺度分析，提高了入侵检测的准确性和可靠性。同样，李辉，蔡忠闽等[2]人研究的一项研究强调了多传感器集成在入侵检测中的重要性，这可以提供对网络态势感知的更全面理解。另一个研究领域集中在使用机器学习和深度学习方法进行入侵检测。正如几位作者所讨论的，这些方法(谈帅昕[3]；余淋[4]；王蓉、马春光[5]；陈傲晗、杜建斌[6])在提高入侵检测系统的准确性和效率方面表现出了希望。此外，基于神经网络的深度学习技术已广泛应用于各种研究领域，包括医疗保健、情感分析和自然语言处理(张婷婷、汪红利[7]；陈先昌[8]；高强、靳其兵[9]；李睿凡[10])。此外，还需要对网络中多入侵行为的分析进行研究。这对于识别和识别多步攻击尤其重要，正如美国陆军(2022 年)所强调的那样。研究多重入侵行为需要对

网络安全态势感知有全面的了解，这可以通过使用先进的数学建模和分析技术来实现(Zhong, Lin, and He, 2023)。因此，本项目拟对多源入侵行为进行建模与解析，以提升 IDS 的效能。本项目拟采用先进的数学模型与分析方法，深入理解网络行为与可能的攻击方式，从而达到更加可靠、精确的入侵检测。

本研究旨在通过对网络多入侵行为的数学建模分析，探讨入侵行为的特征和规律，提出相应的识别和防范策略，为网络安全领域的研究和实践提供理论和技术支持。本文将从网络入侵行为的分类和定义出发，通过数学建模的方法对入侵行为进行分析和建模，探讨网络多入侵行为的识别技术，并对研究结果进行实验验证和性能评估。希望通过本研究能够为网络安全领域的进一步发展和实践提供有益的参考和借鉴。

2. 入侵行为的分类和定义

网络入侵行为是指未经授权的个人或实体通过网络渗透、破坏或获取未授权的信息的行为。根据入侵行为的性质和目的，可以将网络入侵行为分为以下几类，具体见下表 1 所示。

Table 1. Classification of network intrusion behavior
表 1. 网络入侵行为分类

类型	内容
木马和后门	通过植入木马程序或后门程序，使攻击者能够远程控制受感染的计算机系统，获取敏感信息或进行破坏。
拒绝服务攻击(DDoS)	攻击者会不断地向目标系统发出大量的请求，造成系统过载，导致正常用户不能使用系统。
数据窃取	攻击者通过各种手段获取目标系统中的敏感数据，如个人信息、财务数据等，用于非法牟利或其他目的。
网络钓鱼	攻击者通过虚假的网站或电子邮件等手段诱骗用户输入个人敏感信息，如账号密码、银行卡信息等。
恶意软件	包括病毒、蠕虫、间谍软件等，通过植入计算机系统或网络中，用于破坏系统、窃取信息或监视用户活动。
网络扫描和渗透	攻击者通过扫描目标系统的漏洞并利用其进行渗透，获取系统权限或进行其他恶意行为。

针对不同类型的入侵行为，需要采取相应的防范和应对措施，以保障网络安全。

3. 网络多入侵行为的危害

网络多入侵行为的危害十分严重，网络中蕴含大量的敏感信息，包括个人隐私、财务信息、商业机密等，这些信息一旦落入攻击者手中，可能被用于非法牟利、恶意勒索或其他违法活动。拒绝服务攻击(DDoS)等网络多入侵行为可能导致目标系统或网络服务的中断，影响正常的业务运作，给用户和组织带来不便和损失。网络多入侵行为可能导致系统数据的损坏、篡改或丢失，给组织和个人的财产造成损失。当一个企业遭受多重入侵时，它会损害企业的信誉，降低顾客与合作者的信任，从而损害企业的品牌形象。网络多重入侵暴露了系统及网络的安全缺陷，增加了对未来攻击的脆弱性。在某些国家或地区，一旦遭受多重攻击，将面临严重的法律后果，尤其是在某些国家或地区，因不能有效地保护使用者的个人信息及个人信息而被追究法律责任。如何有效地防范和应对网络攻击，是当前迫切需要解决的问题。

4. 模型仿真信任度计算

为保证信息系统的安全，应以信任度为评价指标。通过信任度评估，可以更好地识别和管理网络中的实体，从而降低网络风险和增强安全性。在网络系统中，可以通过信任度评估来验证用户的身份。

通过分析用户的历史行为、社交关系等因素，系统可以更准确地判断用户是否可信，从而提高身份验证的准确性和安全性。在企业网络或云计算环境中，可以根据设备或用户的信任度来实施访问控制策略。对于信任度较低的设备或用户，可以采取更严格的访问限制，以防止未经授权的访问和操作。在跨组织或跨系统的数据交换中，可以通过信任度评估来确定数据接收方的可信度。只有信任度较高的接收方才能获得敏感数据，从而保护数据的安全性和隐私性。在集成第三方服务或组件时，可以通过信任度评估来选择合作伙伴。只有信任度较高的第三方服务提供商才能被允许接入系统，以降低系统受到恶意攻击或数据泄露的风险。引入信任度作为评判标准可以帮助提高网络安全水平，降低网络风险，保护用户数据和系统安全。通过信任度评估，可以更精确地识别和管理网络中的实体，从而有效应对各种安全威胁。

研究模型信任度相关定义见下表 2 所示。

Table 2. Definition of trust degree
表 2. 信任度相关定义

序号	定义
定义 1	信任可以用来对网络中的用户进行可信评价，从而确定节点的身份。
定义 2	信任评价准则采用可信程度－可信程度对其进行评估。
定义 3	由结点间的联系来获得直接的信任度。
定义 4	在此基础上，提出了一种基于其他节点的可信推荐方法。
定义 5	假设节点 n_i 对节点 n_j 的推荐信任度为 $N\left(n_i,n_j,t\right)$；节点 n_i 对节点 n_j 在 t 时刻的信任度为 n_i,n_j，$G\left(n_i,n_j,t\right)$；节点 n_i 对节点 n_j 的直接信任度为 $M\left(n_i,n_j,t\right)$，具体如式(1)所示 $$G\left(n_i,n_j,t\right)=M\left(n_i,n_j,t\right)+N\left(n_i,n_j,t\right) \quad (1)$$ 信任度值的求解，需在式(1)中添加权值 α 完成求解，信任度值如式(2)所示 $$G\left(n_i,n_j,t\right)=\left(1-\alpha\right)\cdot M\left(n_i,n_j,t\right)+\alpha\cdot N\left(n_i,n_j,t\right)0<\alpha<1 \quad (2)$$
定义 6	在上式中权值 α 选取可降低 M、N 对信任度影响度。整合全部节点的直接信任表，对各节点 n：生成二维矩阵，节点 n_i 对节点 n_j 的直接信任度为 $R\left(n_i,n_j\right)$，直接信任度如式(3)所示 $$M\left(n_i,n_j,t\right)=R\left(n_i,n_j\right)\cdot \mathrm{e}^{-\left(t-t_{ij}\right)}t-t_{ij}\geq 0 \quad (3)$$ 为更好地反映伴随时间降低网络节点的直接信任度值会发生变化，通过导入 $\mathrm{e}^{-\left(t-t_{ij}\right)}t-t_{ij}\geq 0$ 表示时间衰减函数。
定义 7	设置网络推荐节点用 P 描述，网络节点用 S 描述，两者节点集合用 A = {A¡, A_2, …, A„}描述。各节点的平均回馈评分组成矢量分别为 SA = [V, VΩ, …, V„]、PA = [V„, Vp2, …, Vμ]，其内节点 i 对节点 j 的平均反馈评分为 v。矢量的夹角的 0 余弦值为 $\theta=\cos'\left(SA\cdot PA\right)$，其中 $0^\circ\leq\theta\leq 180^\circ$。通过各节点评分评估推荐信任度 $N\left(n;,n;,t\right)$。两个矢量相似满足 0 小于阈值 ε 条件，因此推荐信用度如式(4)所示。 $$N\left(n_i,n_j,t\right)=\cos\theta=\sum_{\forall A_i\in A\pi_i\cdot\pi_j}\left(V_{\pi_i\cdot A_i}\times V_{\pi_j\cdot A_j}\right) \quad (4)$$ 其中：矢量用 nA、n，A 分别为节点 n，何节点 n；平均回馈评分。 为减少不诚实推荐对信任评估结果的影响，通过构建矢量空间模型实现。
定义 8	$\forall n_i\in\left\{\text{Grid-Node}\right\}$，其属性为 $a_1,a_2,\cdots,a_n$ 述，属性集为 $A\left(ni\right)=\left\{a_1,a_2,\cdots,a_n\right\}$ 描述。

续表

定义 9　对于 $\forall n_i \in \{\text{Grid-Node}\}$，$n$，与 n；的信任度用式(5)描述:

$$G = G_a + G_d \tag{5}$$

其中：G_d 为动态信任度，G_a 为静态信用度，G_a 值一般不变，

通过式(2)决定 G_d 值，其与时间和网络节点的情况有关。

本项目拟构建一种基于公式(5)的动态可信性和静态可信性模型，以解决因动态可信性下降而引起的可信性评价精度不高的问题。在此基础上，提出了一种新的基于时变的可靠性模型。在此基础上，将随时间变化的节点可信性作为可信元素，以此来确定多个网络入侵。

5. 多重入侵识别的深度学习神经网络模型

基于深度学习神经网络的多入侵识别数学建模在此过程中，我们将采集到海量的网络数据，其中既有常规的网络业务，也有多种入侵行为。然后对数据进行预处理，包括数据清洗、特征提取等。接下来，利用深度学习神经网络技术，构建用于多入侵识别的模型。目前广泛使用的深度神经网络有卷积神经网络、递归神经网络、长短时记忆网络等。在此基础上，采用 BP 神经网络学习方法，对所建模型的参数进行持续优化，从而提升模型对扰动的识别精度。练完成后，需要对模型进行评估，通常使用测试数据集进行验证模型的性能。一旦模型表现良好，就可以部署到实际的网络系统中进行入侵识别。利用深度学习网络建立多元 IDS 模型，可以更好地刻画入侵行为的复杂性，提升其识别精度与鲁棒性，是当前网络安全研究的热点。获取网络节点的可信度特征，并对其进行预处理，包括数据清洗、特征提取等。在此基础上，提出一种新的基于神经网络的多类入侵检测方法，并利用该方法对不同类型的入侵行为进行识别。在多入侵识别数学建模中，采用包括 M 个神经元的输出层和 K 个神经元的输入层组成自适应特征映射的神经网络结构。每个节点的权值用 W 描述，其中 $i \in [1, K]$，$j \in [1, M]$。

具体算法步骤为：

步骤 1：对权值 W 进行初始化，并设置训练数据集 $\left(x', x^{1/2}, \cdots, x\right)$，其中 $l \in [1, N]$。

步骤 2：在 t 时刻内从矢量集中选取 K 维矢量 $Y(t)$，并使用欧氏距离来衡量每个输出节点的距离。

$$d_j = \sum_{i=1}^{K} \left(Y_i^l(t) - W_{ij}(t)\right)^2 \tag{6}$$

步骤 3：神经元的选取是通过计算 M 个欧氏距离，然后选取距离最小的神经元作为最终的选择。在这个过程中，当其他权值被固定时，需要调节领域 N 和节点 g 的权值，以便根据具体的情况得出式(7)。这个过程可以被视为一种优化过程，通过调节领域 N 和节点 g 的权值，使得神经元的选取更加准确和有效。这样的调节过程可以帮助神经网络更好地适应不同的输入数据，并提高多入侵识别的准确性和鲁棒性。

$$W_{ij}(t+1) = W_{ij}(t) + \lambda(t)\left(Y_i^l(t) - W_{ij}(t)\right) \tag{7}$$

步骤 4：使用式(8)激活函数。

$$f(n) = \frac{1}{1 + e^{-n}} \tag{8}$$

为了保证模型的精确性，可以使用负差梯度法对权值进行修正，减少了误差。本项目拟通过对信号源的分析，利用混沌理论中的相空间重建方法，对多阵元干涉信号进行检测，并对其进行处理。在此基础上，选取滥用与异常行为两种类型，研究信用程度函数，建立基于深度神经网络的多源干扰辨识数学

模型。

在这个过程中，利用算法误差的负梯度调整权值是为了最小化模型的预测误差，从而提高模型的准确度。同时，通过混沌理论中的相空间重构技术进行预处理检测，可以有效地处理复杂的网络数据，为后续的入侵识别提供更可靠的基础。此外，结合误用检测和异常检测，分析信用度特征，并利用深度学习神经网络构建信用度特征多入侵识别数学模型，可以更全面地识别多种入侵行为，提高入侵识别的准确度和鲁棒性。

6. 实验分析

为了检验所提出的方法的正确性与可行性，论文以企业网络为研究对象，运用 MATLAB 软件对所提出的方法进行了模拟。在不受时间影响的条件下，分别对 150 次、250 次不同权值 α 和 β 尺度的试验进行了仿真，得到了准确的多次穿透识别率 ρ。共收集 2000 份网路网络资料，其中，从网络的资料中，随机挑选出 1000 个做为训练资料，其他的则为测验资料。实验对比的方法包括文献狄婷、谷良[11]提出的基于灰狼算法的入侵识别方法，以及文献任家东、刘新倩、王倩等[12]人提出的基于 KNN 离群点的入侵识别方法通过这些实验，可以验证本文方法在入侵识别方面的精确性和可行性，并与其他方法进行对比，从而评估其性能和有效性。这样的实验设计可以为深入研究多入侵识别提供重要的实验数据和结果。

在对多个入侵行为进行分析的过程中，只需对输出的流量进行幅度进行辨识即可实现对多个入侵行为的辨识。试验设定了 10~20 ms 内出现多个侵入的情况，并用三种模拟的方式来辨识网络的输出幅度。如图 1 所示。

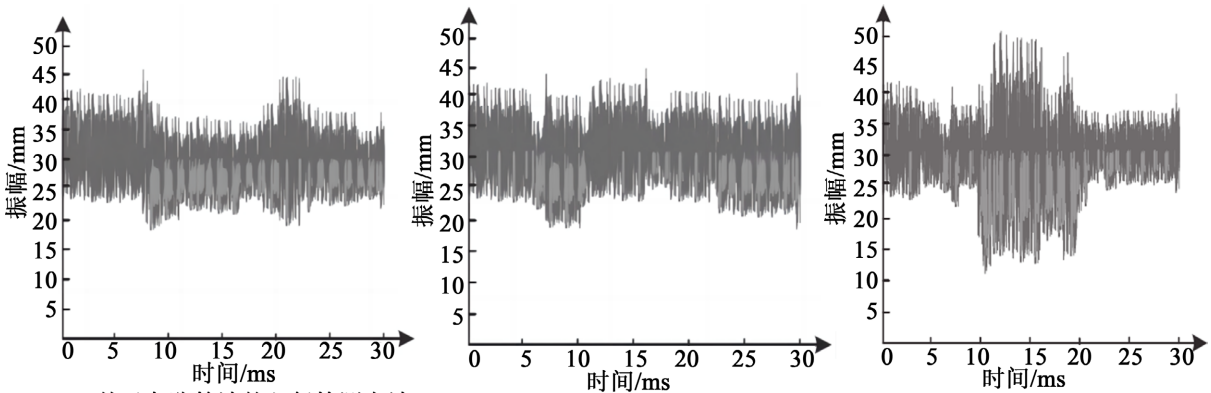

Figure 1. Results of multiple intrusion detection
图 1. 多入侵检测结果

从图 1 可以看出，在多重入侵情况下，本项目所提出的算法能够实现对多个入侵行为的快速检测，并在 10~20 毫秒范围内实现对多个入侵行为的检测。而其他两种方法的振幅变化不显著，在 10~20 ms 时网络振幅波动较小，因此检测效果不佳。

最后，将所提出的算法应用于多种入侵行为的识别，并与已有的算法进行比较，评价算法的效果和精度。通过本项目的研究，将为多重入侵识别问题的研究提供重要的试验依据，并为今后的网络安全研究提供借鉴。

本项目针对现有多入侵行为辨识方法不能对网络中多个入侵行为进行有效辨识，造成传统方法识别结果起伏较小、识别结果失真等问题，以信任度计算为基础，研究多源入侵辨识的数理建模与模拟方法。本项目提出的方法辨识出的网络业务数据幅值发生明显变化，辨识结果与真实情况一致，且存在一个稳

定的区间，可有效提升网络多重入侵辨识能力，合理规避网络风险。

7. 未来发展展望

随着网络上的网络安全软硬件设施的应用越来越多，例如防火墙、安全路由器、入侵检测系统、主机安全系统、防毒系统和桌面安全系统等，都会生成海量的报警和日志等安全事件数据，它们的数据冗余巨大、分散独立、错漏混杂，命中率低、响应滞后，难以将其作为触发事件进行精确的安全响应。安全事件关联分析技术是通过对安全事故数据的全面分析与处理，揭示其隐含的逻辑关系，挖掘攻击者真实意图，进而防范与应对网络攻击，达到对整体信息安全态势监测的目的。参考温辉、徐开勇等[13]人的研究，杜鹏[14]的论述，再结合写者自己的思考，本项目将针对安全事件关联分析中存在的问题，将其划分为：聚集性关联(同类、相似事件之间关联)、交叉关联(安全事件与上下文知识之间关联)、多阶段攻击关联(多步攻击各阶段之间关联)、关联结构与关联细节等。其中，基于多阶段攻击关联技术，旨在重构攻击场景并挖掘攻击意图，是一个十分重要的研究方向。但是，现有的多步骤攻击关联分析方法还存在对先验信息依赖性太强、关联规则要求太高、不能有效地进行场景碎片化挖掘、新型攻击发现困难、实时性不能有效保障等问题。

近年来，神经网络在图像、语音、文字等多个方面得到了广泛的应用。在多入侵识别领域，深度学习神经网络可以通过学习大量的入侵行为数据，自动提取特征并进行分类识别，从而提高入侵检测的准确性和效率。

未来，随着深度学习模型的不断优化和硬件计算能力的提升，多入侵识别数学建模将会更加精确和快速。同时，结合其他技术如强化学习、迁移学习等，可以进一步提高入侵识别系统的鲁棒性和适应性，使其能够更好地适应不断变化的入侵行为。

此外，随着物联网、智能家居等领域的快速发展，对多入侵识别的需求也将不断增加，这将进一步推动多入侵识别数学建模技术的发展和应用。因此，可以预见，基于深度学习神经网络的多入侵识别数学建模在未来将会成为安全领域的重要技术，并在各个领域发挥重要作用。

8. 结论

本研究以基于网络多入侵行为识别的数学建模分析为主题，通过对入侵行为的分类和定义、数学建模分析、识别技术探讨等方面展开了深入研究。通过对网络入侵行为的分类和定义，明确了入侵行为的特征和类型，为后续的数学建模分析奠定了基础。基于已有的入侵行为数据集，采用数学建模的方法对入侵行为进行了分析和建模。通过对入侵行为的数据特征提取和模式识别，建立了入侵行为的数学模型，并提出了相应的识别算法。在识别技术方面，本研究探讨了基于网络流量和行为分析的入侵行为识别方法，并进行了实验验证和性能评估。结果表明，所提出的识别方法在多入侵行为的识别方面具有一定的有效性和可行性。本研究为网络安全领域的研究和实践提供了理论和技术支持，对于提高网络安全防护水平具有一定的指导意义。然而，网络入侵行为的形式和手段日益复杂多样，未来的研究仍需进一步深入，不断完善和优化网络安全防护技术，以应对不断变化的网络安全威胁。

参考文献

[1] 祝毅鸣, 刘莹. 高伪装网络入侵行为的辨识方法优化仿真[J]. 计算机仿真, 2016, 33(9): 296-300.

[2] 李辉, 蔡忠闽, 韩崇昭, 管晓宏. 基于信息融合的入侵检测模型与方法[J]. 小型微型计算机系统, 2003, 24(9): 1602-1606. https://doi.org/10.3969/j.issn.1000-1220.2003.09.008

[3] 谈帅昕. 基于深度学习的入侵检测方法[D]: [硕士学位论文]. 武汉: 中南民族大学, 2019.

[4] 余淋. 基于深度置信网络的入侵检测研究[D]: [硕士学位论文]. 北京: 北京工业大学, 2019.

[5] 王蓉, 马春光, 武朋. 基于联邦学习和卷积神经网络的入侵检测方法[J]. 信息网络安全, 2020, 20(4): 47-54.

[6] 陈傲晗, 杜建斌, 景鑫淼. 基于焦点损失函数的物联网入侵检测深度学习方法[J]. 互联网周刊, 2023(18): 28-31.

[7] 张婷婷, 汪红利, 刘黎, 周菡晓, 严斌宇. 基于大数据与神经网络深度学习技术的学生评价系统综述[J]. 长江丛刊, 2020(32): 94-96.

[8] 陈先昌. 基于卷积神经网络的深度学习算法与应用研究[D]: [硕士学位论文]. 杭州: 浙江工商大学, 2014. https://doi.org/10.7666/d.Y2531769

[9] 高强, 靳其兵, 程勇. 基于卷积神经网络探讨深度学习算法与应用[J]. 电脑知识与技术: 学术版, 2015(13): 169-170.

[10] 李睿凡. 探索神经网络深度学习的教学[J]. 计算机教育, 2014(19): 77-79. https://doi.org/10.3969/j.issn.1672-5913.2014.19.022

[11] 狄婷, 谷良, 安毅, 等. 一种基于互信息与灰狼提升算法的网络入侵检测方法[P]. 中国专利, CN202210799416.9, 2022-11-04.

[12] 任家东, 刘新倩, 王倩, 何海涛, 赵小林. 基于 KNN 离群点检测和随机森林的多层入侵检测方法[J]. 计算机研究与发展, 2019, 56(3): 566-575.

[13] 温辉, 徐开勇, 赵彬, 汪滨. 网络安全事件关联分析及主动响应机制的研究[J].计算机应用与软件, 2010, 27(4): 60-63. https://doi.org/10.3969/j.issn.1000-386X.2010.04.020

[14] 杜鹏. 网络安全事件关联分析与态势评测技术研究[J]. 数字技术与应用, 2016(7): 191-193.