doi :10.3969/j.issn.1671-1122.2020.09.007

无监督机器学习在游戏反欺诈领域的应用研究

徐瑜，周游，林璐，张聪
（杭州浮云网络科技有限公司，杭州 310000）

摘　要：随着在线游戏市场不断壮大，互联网游戏“薅羊毛”事件日渐增多，这对网络游戏资产平衡，特别是游戏发行商的利益，造成严重影响。文章提出一种基于无监督机器学习的游戏机器人检测方法，该方法专注于发现游戏机器人与人类玩家在行为上的区别，引入 word2vec 思想对事件类型向量进行处理，通过聚类分析发现游戏机器人及新的欺诈模式。将无监督机器学习应用于在线游戏反欺诈引擎后，在线游戏机器人检测准确率提升约 8%，极大地提高了检测的准确率。

关键词：无监督机器学习；时间序列；游戏机器人；游戏反欺诈

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2020）09-0032-05

中文引用格式：徐瑜，周游，林璐，等 . 无监督机器学习在游戏反欺诈领域的应用研究 [J]. 信息网络安全，2020，20（9）：32-36.

英文引用格式：XU Yu，ZHOU You, LIN Lu, et al. Applied Research of Unsupervised Machine Learning in Game Anti-fraud[J]. Netinfo Security, 2020, 20(9): 32-36.

Applied Research of Unsupervised Machine Learning in Game Anti-fraud

XU Yu, ZHOU You, LIN Lu, ZHANG Cong
(*Hangzhou Fuyun Network Technology Co., Ltd., Hangzhou* 310000, *China*)

Abstract: As the online game market continues to grow, there are more and more events of "get a deal" happen in the online game, which has had a serious impact on the balance of game assets, especially the interests of game publishers. This paper proposed a game bot detection method based on unsupervised machine learning, this method focused on discovering the differences in behavior between game bots and human players, introduced the word2vec idea to process the event type vector, discovered game bots and new fraud patterns through cluster analysis. After applied unsupervised machine learning to the online game anti-fraud engine, the accuracy of online game bot detection increased by about 8%, greatly improve the detection accuracy rate.

Key words: unsupervised machine learning; time series; game bot; game anti-fraud

0 引言

随着在线游戏用户群体的增加，虚拟经济与真实货币之间的界限逐渐模糊，游戏公司已成为欺诈分子获利对

收稿日期：2020-7-16
作者简介：徐瑜（1987—），男，浙江，硕士，主要研究方向为网络安全、自然语言处理；周游（1975—），男，浙江，硕士，主要研究方向为大数据、人工智能、区块链技术；林璐（1995—），女，福建，硕士，主要研究方向为数据挖掘、人工智能；张聪（1988—），男，吉林，硕士，主要研究方向为数据挖掘、人工智能。
通信作者：林璐 lu@fuyuncn.com

象之一。游戏欺诈逐渐表现出专业化、系统化、隐蔽化的特征，甚至形成完整的黑灰产业链，给游戏反欺诈带来全新挑战。

游戏机器人是一种模仿人类玩家游戏行为的自动程序[1]，是游戏欺诈者常用的工具之一。欺诈者使用游戏机器人的目的分为两种：一种是个人玩家使用游戏机器人，自动精准地进行游戏内活动，从而获取便利；另一种是有组织的“羊毛党”利用游戏机器人不停运行，快速积累游戏金币和物品的活动。游戏欺诈者利用游戏机器人加速耗尽游戏资源，破坏游戏平衡，使得游戏运营有效用户留存率急剧下降，导致玩家对游戏失去兴趣甚至离开，给游戏发行商造成巨大损失[2]。

增加网络游戏安全性的目的是保护游戏发行商和游戏玩家的资产不被欺诈者侵犯。利用反欺诈技术快速识别游戏机器人，有效挖掘欺诈模式成为了当今游戏行业重大挑战之一。

1 反欺诈技术研究现状

反欺诈技术应用分为数据采集、数据分析和应对机制3个阶段[3]，本文主要研究数据采集与数据分析阶段的反欺诈技术。

1.1 数据采集阶段反欺诈技术

在反欺诈系统中，大数据是基础建设之一。基于大数据的反欺诈技术效率高且结果精准，得到广泛应用。相关部门利用大数据技术，将数据采集形成的自动化实时报告中的数据信息提交给数据分析平台，进行反欺诈决策。数据采集过程要严格遵循法律法规和监管要求，获得用户授权方可进行合法合规的数据采集。

1.2 数据分析阶段反欺诈技术

在游戏领域中，基于数据分析技术的游戏机器人检测分为数据挖掘、统计分析、网络理论、相似度分析和图灵测试[2]。使用数据挖掘技术从游戏日志中发现游戏机器人特殊行为模式是游戏发行商青睐的方法，该方法依赖预设的检测算法，不会对玩家游戏造成干扰。

机器学习技术被广泛应用到异常行为检测系统[4,5]，以满足海量数据高效准确的检测要求。通过机器学习挖掘潜在联系，可针对相关数据进行有效监管[6]。无监督机器学习通过分析用户行为数据来识别可疑集群，并在高维特征空间对用户进行聚类，以发现未知的欺诈威胁、提前检测未知攻击，具有很强可解释性[7]。

2 基于无监督机器学习的反欺诈方法

2.1 业务背景及方法流程

目前，业内普遍采用有监督机器学习模型进行风险控制，但有监督机器学习仅能识别部分游戏机器人，本文引入无监督机器学习方法，实现自动识别游戏机器人以发现新的“薅羊毛”行为模式。无监督机器学习流程如图1所示，其难点在于特征选择和相似度计算，后续会对这两部分进行说明。

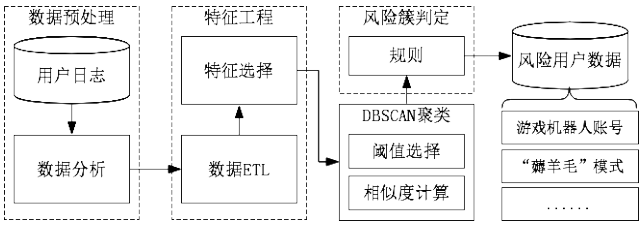

图 1 无监督机器学习流程

2.2 特征工程

用户数据特征可分为统计特征、短文本特征和时间序列特征3类。统计特征包括金币变化统计特征、游戏时长统计特征和签到行为统计特征等；短文本特征包括用户昵称、用户账号等；时间序列特征包括金币变化事件时间序列特征、点击事件变化时间序列特征、游戏切换事件时间序列特征等。统计特征除基础统计信息外，复合比率特征（如签到率、用户投入产出比等）也尤为重要。时间序列特征分为数值型和枚举值型，数值型时间序列特征可通过时间序列趋势图观察。比较图2、图3发现，同一时间段内人类玩家游戏行为更加频繁，且人类玩家游戏时长分布区间较大。

枚举值型时间序列特征较为复杂，需借助光谱图对其进行观察[8]。图4是根据在线游戏用户日志数据绘制的人类玩家（Human）和游戏机器人（Bot）同一时

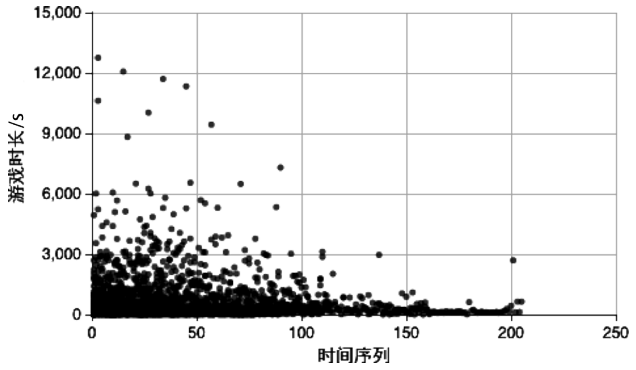

图 2 人类玩家游戏时长时间序列

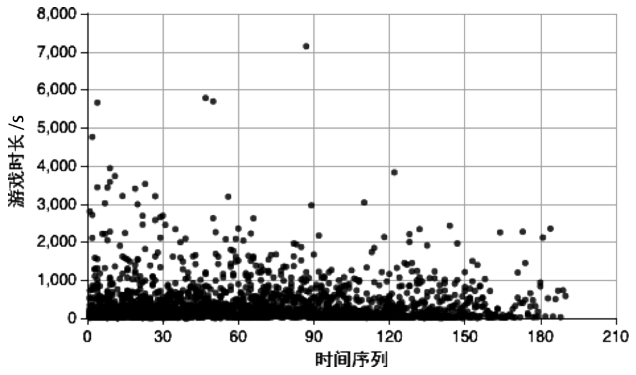

图 3 游戏机器人游戏时长时间序列

间段内金币变化事件时间序列光谱图，每条光谱代表1个用户时间段内金币变化事件，不同事件分配不同光谱。图4深色部分代表游戏引起的金币变化，由图4可知正常用户游戏行为更加频繁，游戏机器人金币变化事件切换更加频繁且存在“空窗期”。这说明游戏机器人的目标可能是阶段性运营活动。人类玩家和游戏机器人的行为都非常复杂，如何准确区分人类玩家和游戏机器人是难点之一。

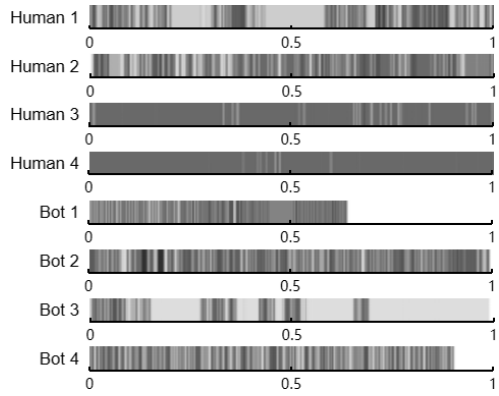

图 4 金币变化事件时间序列光谱图

2.3 模型和算法

2.3.1 基本假设

在“游戏机器人的行为趋于相似，而人类玩家的行为较为随机”的假设下对用户进行聚类，理论上，游戏机器人更容易聚成一类。本文选用DBSCAN算法进行聚类，该算法难点在于相似度的度量。

2.3.2 不同类型特征相似度计算方法

对于统计特征，本文采用用户数据归一化之后的标准差作为相似度的度量。部分游戏机器人的账号或游戏昵称存在规律性，Levenshtein距离能够很好地度量这种相似性，因此，对于短文本特征，如账号、昵称等，使用Levenshtein距离来度量[9]；对于时间序列特征，使用DTW距离来衡量相似性。

2.3.3 事件类型时间序列特征相似度计算

在处理事件类型时间序列特征时，事件用自然数表示后，DTW距离的计算结果不能很好表征其真实距离。因此，本文参考word2vec思想对事件类型时间序列特征进行处理[10]。将用户操作的1个事件当作1个单词，一系列事件形成的时间序列相当于1句话，事件与事件的联系，即单词与单词的上下文联系。事件的任意组合不能代表有意义的一系列事件时间序列，而用户操作形成的一系列事件必定是有意义的。可将用户操作形成的一系列事件抽取出来，根据CBOW架构（图5），参照word2vec来训练事件向量。这个预训练过程定义为event2vec。

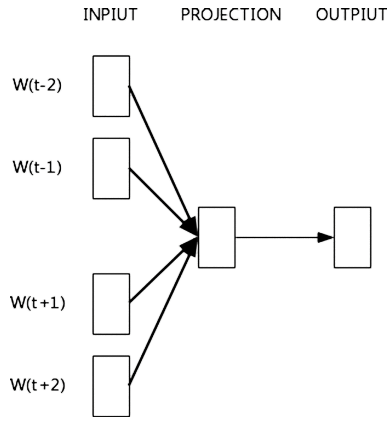

图 5 CBOW 架构

预训练过程需先把事件向量进行独热编码，然后按照word2vec方式训练事件向量，根据事件的含义来确定事件向量维度。例如，金币变化事件时间序列影响因素较多，可用16维向量进行表征；点击事件变化时间序列采用3维向量进行表征，其中两个维度代表界面上的坐标关系，一个维度代表前后操作关联关系。事件向量表征成多维向量后，即可计算事件类型时间序列特征DTW距离，计算过程如图6所示。

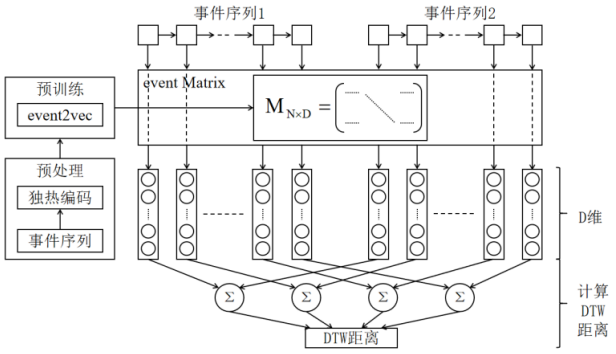

图 6 事件类型时间序列特征 DTW 距离计算过程

2.3.4 混合特征相似度计算

多种类型特征混合时，相似度的度量需要调整不同特征之间的比重。例如，将统计特征和时间序列特征混合进行相似度计算时，统计特征计算出的标准差和时间序列计算出的DTW距离，需经过加权计算才能得出最终的相似度，典型的加权模式如下：

$$T_{score}=\alpha\cdot N_{std}+\beta\cdot P_{std}+\gamma\cdot N_{le}+\varepsilon\cdot\min(R_{\%}+RT_{\%}) \quad (1)$$

其中，α, β, γ, ε 是系数，T_{score} 表示总距离，N_{std} 表示金币等相关统计特征，P_{std} 表示游戏行为相关统计特征，N_{le} 表示文本相关 Levenshtein 距离，$R_{\%}$ 表示金币投入产出比，$RT_{\%}$ 表示金币获取时间效率比。

2.3.5 超参数调整

超参数调整主要包括DBSCAN聚类的领域半径、最小包含点数以及加权用到的系数和模式，加权模式主要根据业务来确定。由于处理各个特征的相似度时，已把数值映射到0~1之间，因此加权后得到的相似度也是0~1之间的数值，因此领域半径只需在0~1之间调节即可。根据实践，最小包含点数在5~20之间调节，会有较为明显的变化。

2.4 游戏机器人判定

根据相似度把用户聚成若干类后，下一步即可判定哪些类是由游戏机器人聚成。人类玩家也可能由于某些相似性（如游戏行为相似、游戏偏好相似、地理位置相似等）聚成一类，因此，需结合业务场景采用特定规则对该类是否由游戏机器人聚成进行判定。

2.5 实验结果

本文从在线游戏用户日志中提取数据进行实验，通过对特征进行相似度计算、与验证集进行验证，得到如表1所示效果对比。金币值和游戏时长本身是非离散的连续数值，此处不做向量化验证。

表 1 时间序列特征间的效果对比

	非向量化			向量化		
特征	准确率	召回率	误封率	准确率	召回率	误封率
游戏切换事件时间序列	60.70%	39.00%	1.01%	62.70%	44.75%	1.07%
金币变化事件时间序列	59.49%	37.63%	1.03%	62.50%	41.88%	1.01%
点击事件变化时间序列	77.78%	66.50%	0.76%	80.99%	69.75%	0.66%
金币值变化时间序列	59.39%	31.63%	0.87%			
游戏时长变化时间序列	85.73%	75.88%	0.51%			

由表1结果可知，非向量化游戏时长变化时间序列和向量化点击事件变化时间序列效果较好，后续实验将对这两个特征和统计特征、短文本特征以及混合特征进行比较。其中，短文本特征字段较少，单独训练效果不理想，需与统计特征组合训练，结果如表2所示。

表 2 混合特征效果对比

特征	准确率	召回率	误封率
统计特征 + 短文本特征	84.93%	88.75%	0.63%
向量化点击事件变化时间序列特征	80.99%	69.75%	0.66%
游戏时长变化时间序列特征	85.73%	75.88%	0.51%
统计特征 + 短文本特征 + 向量化点击事件变化时间序列特征	81.48%	95.13%	0.87%
统计特征 + 短文本特征 + 游戏时长变化时间序列特征	85.16%	90.38%	0.63%

从表2结果可知，各特征的误封率与准确率相差不大，召回率的差异最为显著。以“统计特征+短文本特征”为参照，仅使用向量化点击事件变化时间序

列特征或游戏时长变化时间序列特征，结果都不理想。而向量化点击事件变化或游戏时长变化时间序列特征分别与统计特征及短文本特征混合后，表现均有所提升。其中，统计特征、短文本特征与向量化点击事件变化时间序列特征结合表现最优，召回率可达95.13%。

3 实际应用

在线游戏的实际业务中，在线游戏机器人识别主要基于特定规则和有监督机器学习模型进行。无监督机器学习使用统计特征、短文本特征与向量化点击事件变化时间序列特征相结合的方式训练，召回尽可能多的游戏机器人样本，规则校验和人工审核后，用以补充有监督机器学习样本。完整的反欺诈引擎架构如图7所示。

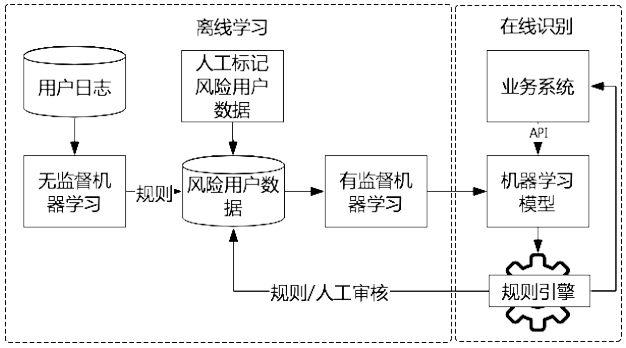

图 7 反欺诈引擎架构

截至目前，较未使用无监督学习补充样本，使用无监督学习补充样本数据后，在线识别游戏机器人有监督模型在测试集上准确率提升约3%，召回率提高约8%。加入无监督学习后，反欺诈引擎能自动检测到新的“薅羊毛”模式，提升反欺诈效率，降低游戏平台被“薅羊毛”的风险。

4 结束语

本文采用无监督机器学习发现异常用户，引入word2vec思想对事件类型的时间序列进行处理。在未来工作中，可参考doc2vec思想，用更稠密的向量直接表达整个事件时间序列[11]。此外，完整的反欺诈系统除了能够有效识别欺诈行为，还需在防范过程中提供相应的反制措施和手段，防止误伤真实玩家，保护用户和平台的利益不受损失。（责编 姜丽辉）

参考文献：

[1] KANG A R, WOO J, PARK J, et al. Online Game Bot Detection Based on Party-play Log Analysis[J]. Computers & Mathematics With Applications, 2013, 65(9): 1384-1395.

[2] XUE Hongyan, CHEN Ruoping. Strengthen Marketing Offenses and Defenses to Completely Contain the "Wool Party"[J]. Internet Economy, 2017, 17(12): 26-31.
薛洪言，陈若平. 加强营销攻防全面围堵“羊毛党”[J]. 互联网经济，2017，17（12）：26-31.

[3] HAO Guanghao. Application of Digital Fraud and Fintech Anti-fraud[J]. Taxation and Economy, 2019, 19(6): 40-47.
郝光昊. 数字化欺诈与金融科技反欺诈的应用 [J]. 税务与经济，2019，19（6）：40-47.

[4] CHEN Sheng, ZHU Guosheng, QI Xiaoyun, et al. Custom User Abnormal Behavior Detection Based on Depth Neural Network[J]. Computer Science, 2019，19(S2): 442-445.
陈胜，朱国胜，祁小云，等. 基于深度神经网络的自定义用户异常行为检测 [J]. 计算机科学，2019，19（S2）：442-445.

[5] PING Ping, LI Jianhua, MAO Yingchi, et al. Image Encryption Based on Chaotic Mapping and Bit Reorganization[J]. Journal of Image and Graphics, 2017, 22(10): 1348-1355.
平萍，李健华，毛莺池，等. 混沌映射与比特重组的图像加密 [J]. 中国图象图形学报，2017，22（10）：1348-1355.

[6] WU Baogui. Exploration of the Ways to Apply Artificial Intelligence to the Field of Financial Supervision[J]. Modern Economic Information, 2019, 19(18): 273-274.
武宝贵. 人工智能应用于金融监管领域的途径探索 [J]. 现代经济信息，2019，19（18）：273-274.

[7] DataVisor. Using Automated AI Technology to Combat Intelligent Network Fraud[J]. Security & Informatization, 2019, 19 (10): 42.
维择科技 . 运用自动化 AI 技术打击智能化网络欺诈 [J]. 网络安全和信息化，2019，19（10）：42.

[8] TAO J, XU J, GONG L, et al. NGUARD: A Game Bot Detection Framework for NetEase MMORPGs[C]//ACM. The 24th ACM SIGKDD International Conference, August 19-23, 2018, London, United Kingdom. New York: ACM, 2018: 811-820.

[9] KEOGH E, RATANAMAHATANA C A. Exact Indexing of Dynamic Time Warping[J]. Knowledge and Information Systems, 2005, 7(3): 358-386.

[10] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient Estimation of Word Representations in Vector Space[EB/OL]. https://arxiv.org/abs/1301.3781, 2013-6-15.

[11] LE Q V, MIKOLOV T. Distributed Representations of Sentences and Documents[C]//IMLS. 31st International Conference on Machine Learning, June 21-26, 2014, Beijing,China. MA: MIT Press, 2014: 1188-1196.