文章编号: 1006-2475(2020) 06-0089-06

基于深度 Q 网络的垃圾邮件文本分类方法

景栋盛,薛劲松,冯仁君

(国网江苏省电力有限公司苏州供电分公司,江苏 苏州 215004)

摘要: 电子邮件广泛应用于人们的工作生活中。然而,充斥着虚假信息、恶意软件和营销广告等内容的垃圾邮件也以电子邮件为载体进行传播。这不仅给人们带来不便,而且也占用和耗费大量的网络资源,甚至严重地威胁信息安全。因此,有效地识别、过滤垃圾邮件是一项重要的工作。目前,垃圾邮件过滤方法主要包括基于邮件来源的识别和基于内容的识别,但大部分方法效果不佳且效率不高,并且需要耗费大量的人力标注特征,也跟不上垃圾邮件内容和形式等的改变。近年来,有研究人员将深度强化学习用在自然语言处理上并取得了重大的成果,鉴于此,本文提出基于深度 Q 网络的垃圾邮件文本分类方法。该方法在对邮件文本进行预处理、分词以及用 Word2vec 模型得到词向量的基础上用深度 Q 网络对垃圾邮件进行过滤,充分利用 Word2vec 中的 CBOW 模型得到邮件文本中的每个分词对应的词向量,直接用深度 Q 网络对得到的词向量集进行处理,无需提取邮件的特征,避免了由于特征提取的偏差带来的负面影响,提高了垃圾邮件过滤的效率和精确率。实验结果验证了本文方法的有效性。

关键词: 电子邮件; 深度 Q 网络; Word2vec 模型; 文本分类
中图分类号: TP393 **文献标识码:** A **doi:** 10.3969/j.issn.1006-2475.2020.06.014

Spam Text Classification Method Based on Deep Q-network

JING Dong-sheng, XUE Jing-song, FENG Ren-jun

(Suzhou Power Supply Branch, State Grid Jiangsu Electric Power Limited Company, Suzhou 215004, China)

Abstract: Electronic mail is widely used in people's daily life. It also serves, however, as a carrier for the proliferation of spam mails filled with false information, malicious software and undesired advertisements. Spam mails not only bring inconvenience but also unnecessarily consume a lot of network resource and even pose a huge threat to their information safety. Therefore, it remains an important task to effectively identify and filter spam mails. Current filtering methods are mainly based on identifying the source and content of mails, which are not effective and require a large amount of artificial labeling and are not sensitive to the changes of spam mails' content or format. In recent years, researchers have applied deep reinforcement learning to the natural language processing and obtained good results. Therefore, this paper presents a classification method for identifying spam mails based on deep Q-network. The mail text first is preprocessed, then is segmented and is transformed into word vectors using Word2vec model. The deep Q-network is used to filter spam mails based on these word vectors in order to improve efficiency and accuracy. The method makes full use of the CBOW model in Word2vec to obtain the word vector corresponding to each participle in the mail text, and directly processes the obtained word vector with the deep Q-network, without extracting the features of the mail, so as to avoid the negative impact caused by the deviation of feature extraction. The experiment results verify the effectiveness of the method.

Key words: electronic mail; deep Q-network; Word2vec; text classification

0 引 言

电子邮件是一种便捷的交流工具,在人们的日常生活中起着重要的作用,具有使用成本低廉、信息传播迅速等优点。但电子邮件的这些特点却被垃圾邮件的制造者所利用来传播垃圾邮件。广义上讲,垃圾

收稿日期: 2019-09-20; **修回日期:** 2019-11-22
基金项目: 国家自然科学基金资助项目(61303108) ; 江苏省高等学校自然科学研究重大项目(17KJA520004)
作者简介: 景栋盛(1981-) ,男,江苏苏州人,高级工程师,硕士,研究方向: 机器学习,网络安全,智能化信息系统,E-mail: jds19810119@163.com; 薛劲松(1977-) ,男,江苏常熟人,高级工程师,学士,研究方向: 网络安全,智能化信息系统,E-mail: 6802569@qq.com; 冯仁君(1989-) ,男,江苏盐城人,工程师,硕士,研究方向: 网络安全,智能化信息系统,E-mail: frj1989@126.com。

邮件是指含有虚假或不良信息、恶意链接以及营销广告等内容的电子邮件。垃圾邮件中可能包含木马、病毒,因此垃圾邮件会浪费社会资源,泄露隐私信息,造成无法挽回的损失[1],对互联网的发展带来不利影响[2]。

研究人员提出了各种识别和过滤垃圾邮件的方法,主要包括:基于黑白名单的过滤、基于规则的过滤以及基于邮件内容的过滤方法[3]。基于黑白名单的过滤方法虽然简单、快速,内存消耗低,并在邮件发送成功之前就可识别出邮件是否为垃圾邮件,但是这种过滤方法不能识别所有的邮件,并且需要耗费大量的人力建立黑白名单,也可能会错误地将正常邮件拦截[4]。基于规则的邮件过滤方法需要人工挖掘邮件的特征,而垃圾邮件的特征词库会随着邮件数量的增多而不断改变,这需要花费大量的人力建立特征词库[5],然而仍然会在很多情况下识别不出垃圾邮件。基于邮件内容的过滤方法是对已经标记好的邮件文本使用机器学习方法进行训练[6]。常用的机器学习算法主要有支持向量机[7]、朴素贝叶斯[8]和逻辑回归[9]等算法,机器学习算法可以根据历史数据进行主动学习和预测,这使得垃圾邮件的识别成为主动的预防识别[10]。

基于邮件内容的垃圾邮件过滤方法不再局限于邮件的协议和网络,而是根据邮件的内容来过滤垃圾邮件。王青松等人[11]更改以词为文本的特征项单位的方式,采用短语作为正文文本的特征项单位在朴素贝叶斯模型上进行分类,提出了基于短语的贝叶斯中文垃圾邮件过滤方法,该方法提高了垃圾邮件的分类精度;于洪霞[12]提出了基于支持向量机的中文垃圾邮件过滤方法,该方法采用分词方法对特征提取方法进行改进,然后在支持向量机分类器中对邮件进行分类,该方法提高了邮件分类的精度和速度;李培国[13]在人工神经网络的基础上设计了中文垃圾邮件过滤器,该方法采用 ICTCLAS 系统进行中文分词,在 BP 分类器中对邮件进行分类,该方法提高了垃圾邮件分类的精度和稳定性;Wang 等人[14]采用卷积神经网络和支持向量机来提取垃圾邮件中图像的特征,在邮件分类中取得了良好的效果;李艳涛等人[15]提出了一种采用动态函数使 Dropout 随着迭代次数而逐渐减小的方法,并在堆叠式降噪自编码中应用该方法,以及在英文邮件上进行实验,实验结果表明该方法有效地提高了邮件的分类精度,分类效果具有更好的稳定性。

虽然垃圾邮件过滤方法取得了一定的成绩,但是在准确率的提高上依然有很大的上升空间,同时也存在着很多问题。例如,现有的垃圾邮件过滤方法人工标注成本高,并且效率低下,垃圾邮件的内容、形式更新快,传统的人工方法无法与之匹配。近几年,深度 Q 网络被提出并在实验和应用中取得了更好的效果,深度 Q 网络应用在垃圾邮件的过滤上通过“试错式”学习对邮件进行分类。由于特征提取影响识别效果,甚至会降低垃圾邮件的过滤准确率,为避免这一问题,本文充分利用 Word2vec 中的 CBOW 模型得到邮件文本分词集对应的词向量集,再训练深度 Q 网络对邮件分类,可以有效地忽略特征提取这一步骤,解决了邮件文本特征提取困难的问题,进而降低成本。并且强化学习是终生学习,可以边学习边改进,能有效地应对垃圾邮件的更新问题。为解决垃圾邮件过滤过程中遇到的问题,本文提出基于深度 Q 网络的垃圾邮件文本分类方法。该方法需要首先对原始邮件文本数据预处理和分词,并采用 Word2vec 方法对文本进行向量化处理,实现在深度 Q 网络上的垃圾邮件文本的分类。通过比较正确率、精确率、召回率和 F1 值可知,本文所提出的基于深度 Q 网络的垃圾邮件文本分类方法能提高垃圾邮件过滤的高效性和精确性。

1 相关工作

1.1 文本预处理和分词

文本预处理是指将原始数据处理成实际应用所需要的文本格式[16]。因为数据集的来源不同,导致数据源中可能含有大量非法或无意义的字符,这些字符可能是标点或乱码等非文本分类需要的字符,需要将其去除。并且在邮件文本分类中,需要把文本编码方式统一转换成可以识别的编码方式。

分词是指按照一定的规则将句子切分成一组词的过程[17]。在英文文本中,空格是词与词之间的分割符号,然而,在中文文本分词中,句子包含的词与词之间没有明确的分割符号,因此,比较而言中文分词具有一定的困难性[18]。中文分词中最常见的几类分词算法有基于字符串匹配的分词方法[19]、基于理解的分词方法[20]、基于统计的分词方法[21]和基于词与词性相结合的分词方法[22],基于词与词性相结合的分词方法考虑了词还具有词性的问题[23]。基于统计的分词方法是目前最常用的中文分词方法,该方法在分词的过程中将词的词性进行人为标注并统计了中文词出现的次数这一统计特征,通过模型学习标注的文本数据,得出各种情况下每个词出现的概率,选择最可能出现的分词结果。该方法考虑到了词出现的频率和文本词的上下文的含义,在中文分词中展示了

很好的效果[24]。

1.2　Word2vec 模型

因为计算机只能识别数学符号,所以邮件中的邮件文本必须转化为数学的形式才能够被识别。因此,需要将文本中的词转化为数学中向量的形式。文本向量化表示是指将文本中的词转化成实数向量,并用于后续模型的计算。将邮件文本中的词转化为数学向量形式的主要方法有独热表示(One-hot Representation)和词向量表示(分布式表示(Distributed Representation))[25]。

Word2vec 模型是一个 n 元语法模型,目的是使计算机理解自然语言,方法是通过对自然语言进行假设和建模[26]。Word2vec 模型在语义维度上推动了文本分析的进程,该模型主要包括连续词袋模型(Continuous Bag-of-Words, CBOW)和 Skip-gram 模型[27]。

连续词袋模型是根据输入的相关 $n-1$ 个词预测中心词本身,在训练的过程中,首先给出中心词的一个邻域半径内的所有单词,然后预测输出单词是给出的中心词的概率[28]。Skip-gram 模型将 CBOW 的因果关系进行颠倒,根据给定的当前中心词预测上下文的内容[27]。Word2vec 模型的网络结构包含输入层、投影层和输出层 3 个层次。Word2vec 的 2 种模型又各有 2 种策略,故一共有 CBOW 加层次的网络模型、Skip-gram 加层次的网络模型、CBOW 加抽样的网络模型和 Skip-gram 加抽样的网络模型[26]。使用 Word2vec 模型得到的词向量会考虑上下文,通用性强。

1.3　强化学习

强化学习(Reinforcement Learning, RL)是指智能体处于一个未知的环境中,通过与环境不断交互的试错式学习来获得最大回报,并学得最优策略的过程,强化学习是一种机器学习方法[29]。强化学习是基于马尔可夫决策过程的。在强化学习中,智能体周期性地根据观察到的随机动态系统做出序贯决策,这个过程连续执行,一直到智能体得到最大回报值后结束。Q-learning[30]是一种异策略(off-policy)强化学习算法,在状态 s 下根据 Q 值择优选择并执行动作 a,从环境中获得奖赏 r,进入下一个状态 s'。Q 值的更新方式为:

$$Q(s,a) \leftarrow Q(s,a) + \alpha\delta \tag{1}$$

其中,s 表示智能体所处的状态,a 表示智能体在状态 s 下所采取的动作,α 是学习率,δ 是时间差分误差(Temporal Difference Error, TD-error)[31],计算方法为:

$$\delta = r + \gamma \max_{a'} Q(s',a') - Q(s,a) \tag{2}$$

其中,r 表示奖赏,γ 是折扣因子。Q-learning 算法学习得到的动作值函数 Q 直接逼近最优动作值函数,并不依赖于智能体选择的策略,简化了算法的分析。

1.4　深度 Q 网络

深度强化学习(Deep Reinforcement Learning, DRL)是将深度学习和强化学习相结合,融合了二者的感知能力和决策能力来解决系统中的感知决策问题[32]。深度 Q 网络(Deep Q-network, DQN)作为第一种深度强化学习算法,高效地缓解了用非线性函数逼近器表示值函数时算法的不稳定性问题[33]。

深度学习(Deep Learning, DL)是基于人工神经网络(Artificial Neural Network, ANN)的,基本算法是反向传播(Back Propagation, BP)算法,深度学习模型的经典范例是多层感知器(Multi-layer Perceptron, MLP),其由多层隐藏层构成,与浅层网络相比较,多层感知器具有更强的特征表达能力[34]。

Mnih 等人[35]在 Q-learning 算法和深度卷积神经网络的基础上提出了深度 Q 网络算法,该算法使用了经验回放机制和目标网络方法,DQN 的结构示意图如图 1 所示。

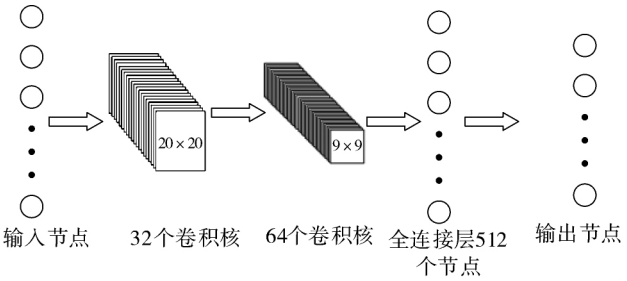

图 1　深度 Q 网络结构示意图

深度 Q 网络使用当前值网络和目标值网络这 2 个独立的 Q 网络,用 θ 表示当前值网络的参数,该参数是实时更新的,θ^- 表示目标值网络的参数,该参数在每过 L 步后由 θ 复制得到[36]。当前值网络的输出表示为 $Q(s,a;\theta)$,目标值网络的输出表示为 $Q(s,a;\theta^-)$,损失函数由目标值函数和当前值函数的均方误差决定:

$$L(\theta) = E[Y - Q(s,a;\theta))^2] \tag{3}$$

$$Y = r + \gamma \max_{a'} Q(s',a';\theta^-) \tag{4}$$

其中,s 代表当前智能体所处的状态,a 代表智能体在状态 s 下执行的动作,s' 表示智能体所处的下一个状态,a' 表示智能体处于下一状态时执行的动作。式(4)作为监督学习的标签,近似地表示了值函数的优化目标。为了求解得到最小化损失函数,对式(3)中参数 θ 求导得到:

$$\nabla_\theta L(\theta) = (r + \gamma \max_{a'} Q(s',a';\theta^-) - Q(s,a;\theta)) \nabla_\theta Q(s,a;\theta) \tag{5}$$

在上述公式中,参数 θ 的更新采用随机梯度下降

法(Stochastic Gradient Descent, SGD)方式进行。

深度 Q 网络通过贪心策略更新动作值函数,用 ε-贪心策略(ε-greedy)方法选择动作。

2 数据处理与算法描述

2.1 数据描述与处理

本文使用的数据来自于 ECML/PKDD 2006 Discovery Challenge[6] 中任务 A 的数据,数据分为带标签的培训数据和测试数据。其中,带标签的培训数据一共有 4000 条,包括 50% 的垃圾邮件和 50% 的非垃圾邮件。测试数据来自不同的多个邮箱,每个邮箱有 2500 条数据。提供的数据不是电子邮件的原始文本,而是用向量空间表示的向量并采用 SVMlight 使用的稀疏数据格式存储数据。属性是单词的词频,并且删除了数据集中计数少于 4 的单词,最终数据集中大约有 150000 个单词。数据集中每一行代表一封电子邮件,每一行的第 1 个标记是类标签,+1 表示垃圾邮件,-1 表示非垃圾邮件,0 表示没有标签的测试数据。标签之后的每一对标记表示单词的 ID 和其词频,词频按升序排列。

如训练数据集中的某一条数据为:1 9:3 94:1 109:1 163:1,这表示是一条垃圾邮件数据,有 4 个单词,第 1 个单词的 ID 是 9,该单词在这封邮件中出现了 3 次。

2.2 算法描述

在深度 Q 网络被训练之前,通过对数据进行预处理,过滤掉文本中的非法字符和无意义字符等,并通过对邮件文本分词来获得数据长度统一的邮件文本,每一封邮件对应一个有顺序的分词集,最后用 Word2vec 中的 CBOW 模型得到邮件文本分词集对应的词向量集。处理后的每一封邮件的文本内容对应一个词向量集,词向量是数值向量的形式,不需要对邮件进行特征提取,词向量集作为深度 Q 网络的输入状态。为提高垃圾邮件过滤的效率和精确度,本文提出基于深度 Q 网络的垃圾邮件文本分类方法。用于垃圾邮件检测的深度 Q 网络学习算法中,状态 s 是词向量集,s = { 词向量集 | 用 Word2vec 中的 CBOW 模型得到邮件文本对应的词向量集}。在当前状态下,智能体执行分类动作 a,a = { 是垃圾邮件,不是垃圾邮件},判断词向量集是否属于垃圾邮件,若判断正确,则得到奖励值,该奖励值设置为一个正数,若判断错误,则得到惩罚值,惩罚值设置为一个负数。智能体依次从状态空间 S 中选择状态词向量集,一直到训练结束。网络训练好后可以用于垃圾邮件的文本分类。在应用的过程中,首先对获得的邮件文本预处理,过滤掉文本中的非法字符和无意义字符等,并通过对邮件文本分词来获得数据长度统一的邮件文本,最后用 Word2vec 中的 CBOW 模型得到邮件文本对应的词向量集。词向量集作为训练好的深度 Q 网络的输入状态,输出结果为该邮件是否为垃圾邮件。基于深度 Q 网络的垃圾邮件文本分类方法示意图如图 2 所示。

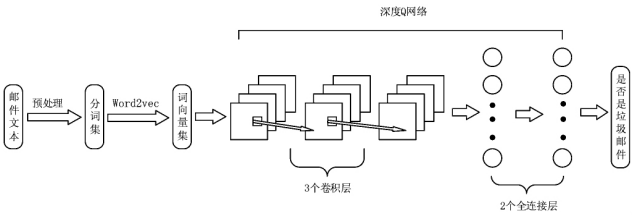

图 2 基于深度 Q 网络的垃圾邮件文本分类示意图

用于垃圾邮件检测的深度 Q 网络学习算法(Deep Q-network for Spam Detection, DQNSD)描述如算法 1。

算法 1 用于垃圾邮件检测的深度 Q 网络学习算法。

输入:迭代轮数 T,状态特征维度 n,动作集 A,步长 α,衰减因子 γ,探索率 ε,Q 网络结构,批量梯度下降的样本数 m。

输出:Q 网络参数。

1. 对邮件文本进行预处理,用分词软件对邮件文本进行分词,每封邮件对应一个词按顺序排列的分词集

2. 用 Word2vec 中的 CBOW 模型得到分词集对应的词向量集 s

3. 随机初始化 Q 网络的所有参数 ω

4. 基于 ω 初始化所有的状态和动作对应的 Q 值

5. 清空经验回放集合 D

6. for i from 1 to T

7. 初始化 s 为当前状态序列的第 1 个状态

8. 在 Q 网络中使用 s 作为输入,得到 Q 网络的所有动作对应的 Q 值

9. 用 ε - 贪婪法在当前 Q 值输出中选择对应的动作 a

10. 在状态 s 执行当前动作 a,得到新状态 s' 及其对应的奖励 r 和是否是终止状态 is_end

11. 将五元组{s, a, r, s', is_end} 存入经验回放集合 D

12. $s = s'$

13. 从经验回放集合 D 中采样 m 个样本{s_j, a_j, r_j, s_j', is_end$_j$},$j = 1, 2, \cdots, m$,计算当前目标 Q 值 y_j

14. 使用均方差损失函数,通过神经网络的梯度反向传播来更新 Q 网络的所有参数 ω

15. 如果 s' 是终止状态,当前轮迭代完毕,否则转到步骤 6

Return Q 网络参数

3 实验及分析

基于深度 Q 网络的垃圾邮件文本分类方法首先

对邮件文本进行预处理、分词,然后用 Word2vec 模型得到邮件文本的词向量集表示,最后用深度 Q 网络对垃圾邮件进行过滤,提高了垃圾邮件过滤的效率和精确率。实验的对比方法有朴素贝叶斯、决策树、支持向量机、TextCNN 和 TextRNN。

3.1　评价标准

本文实验的评价标准有正确率、精确率、召回率和 F1 值。当分类类别是二分类时,TP 的含义是真正类(True Positives) ,表示在所有正样本中,分类器可以正确识别为正样本的样本个数; FP 的含义是假正类(False Positives) ,表示在所有的负样本中,被分类器误分类为正样本的样本个数; FN 代表的是假负类(False Negatives) ,表示在所有的正样本中,分类器把正样本错误地识别为负样本的样本个数; TN 表示的是真负类(True Negatives) ,表示在所有的负样本中,分类器把负样本正确地识别为负样本的样本个数[38] 。

正确率[38] (accuracy) 也称作准确率,代表在正确分类的情况下,正样本和负样本占所有样本的比例,也就是在所有的样本中被分类器正确识别的正负样本数所占的比例,准确率越高越好,计算公式如下:

$$\text{accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{FP} + \text{TN}} \tag{6}$$

精度[38] (precision) 也称作精确率,代表被分为正样本的数据中同时也是正样本的样本个数占所有被分为正样本的比例,计算公式如下:

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{7}$$

召回率[38] (recall) 是用来度量覆盖面的,等同于灵敏度(sensitive) ,代表所有被分为正样本的数据中被正确识别的样本个数占所有正样本的比例,计算公式如下:

$$\text{recall} = \text{sensitive} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{8}$$

F1 值[38] 亦称为平衡 F 分数,同时反映了模型的精确率和召回率,其取值范围在 0 ~ 1 之间,是精确率和召回率加权平均的一种评价标准形式。计算公式如下:

$$\text{F1} = \frac{2 \cdot \text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \tag{9}$$

3.2　实验结果及分析

深度 Q 网络以词向量集作为输入,在训练的过程中,如果将每封邮件分类正确,可以得到 10 的奖励值,分类错误得到 - 10 的奖励值。Q 网络在追求长期累积回报值最大化的过程中不断更新计算得到最大 Q 值,并用梯度的反向传播更新神经网络的参数 ω,不断地减小通过经验回放得到的目标 Q 值和通过 Q 网络计算的 Q 值。ω 收敛后,得到近似的 Q 值计算方法和贪婪策略,训练结束。

深度 Q 网络在训练时利用的邮件样本数量 mini-batch 设置为 32,由 3 个卷积层提取特征,最后经过 2 个全连接层处理得到输出,网络更新的学习率 α 被设置为 0.05,奖赏折扣率 γ 被设置为 0.99,探索因子 ε 设置为 0.1。表 1 给出了朴素贝叶斯、决策树、支持向量机、TextCNN、TextRNN 和深度 Q 网络的性能对比。

表 1　不同模型与深度 Q 网络的性能对比

模型	正确率/%	精确率/%	召回率/%	F1 分数
朴素贝叶斯	78.30	76.91	79.97	0.7839
决策树	78.96	79.57	78.13	0.7883
支持向量机	80.10	80.19	79.41	0.7980
TextCNN	82.03	80.70	83.71	0.8213
TextRNN	83.62	81.39	84.07	0.8301
DQN	85.91	84.04	87.93	0.8598

决策树方法采用分类与回归树(Classification and Regression Tree, CART) 方法,支持向量机采用的是高斯径向基函数分类器,对应的核函数是高斯核函数,公式如下:

$$K(x,z) = \exp\left(-\frac{\|x - z\|^2}{2\sigma^2}\right) \tag{10}$$

其中,z 是核函数中心,σ 为函数的宽度参数,控制函数的径向作用范围。

由表 1 可知,基于深度 Q 网络的垃圾邮件文本分类方法与以往的方法相比较效果有所提高,但仍然存在误分类的情况,这是由于深度 Q 网络在分类的过程中仍然会有一个很小的概率选择其他的行为,探测是否有可能获得更大回报值的行为。实验结果表明基于深度 Q 网络的垃圾邮件文本分类方法提高了垃圾邮件的识别正确率,可以避免由于误分类造成不必要的影响和损失,提高了垃圾邮件过滤的效率。

4　结束语

垃圾邮件的传播降低了人们办公的效率,占用和浪费了网络公共资源,危害了信息安全,是亟需清除的“毒瘤”。传统的垃圾邮件过滤方法需要依赖大量的人力,且效果并不理想,可能会不能正确地区别正常和垃圾邮件。为解决上述问题,本文提出了基于深度 Q 网络的垃圾邮件文本分类方法。该方法首先对原始邮件文本数据预处理和分词,得到邮件文本对应的分词集,然后采用 Word2vec 方法对文本的每个分词进行向量化处理,最后在深度 Q 网络上实现了垃圾邮件文本的分类。实验结果验证了该方法有效地

提高了垃圾邮件过滤的效率和精确率。

参考文献:

[1] 胡小娟,刘磊,邱宁佳. 基于主动学习和否定选择的垃圾邮件分类算法[J]. 电子学报,2018,46(1):203-209.

[2] 翟军昌,车伟伟. 一种基于条件熵的垃圾邮件过滤算法[J]. 计算机与现代化,2014(2):129-132.

[3] 杜猛. 反垃圾邮件技术分析和发展研究[J]. 电子技术与软件工程,2015(16):34.

[4] 赵静凯,张佳,卜宏,等. 基于信件源的垃圾邮件过滤[J]. 计算机工程与应用,2004,40(9):139-142.

[5] 汤金波,孙力. 基于规则的垃圾邮件过滤算法比较研究[J]. 网络安全技术与应用,2016(6):57-58.

[6] 赵晓丹,徐燕. 垃圾邮件分类技术对比研究[J]. 信息网络安全,2014(2):75-80.

[7] 石铁峰. 支持向量机在电子邮件分类中的应用研究[J]. 计算机仿真,2011,28(8):156-158.

[8] 李书全. 基于贝叶斯分类算法的中文垃圾邮件过滤技术的研究[D]. 合肥:合肥工业大学,2008.

[9] 韩敏,李秋锐. 基于 KNN 算法的垃圾邮件过滤方法分析[J]. 计算机光盘软件与应用,2012(7):179-180.

[10] 翟军昌,秦玉平,车伟伟. 应用特征词分类贡献的垃圾邮件过滤研究[J]. 计算机工程与应用,2012,48(34):116-119.

[11] 王青松,魏如玉. 基于短语的贝叶斯中文垃圾邮件过滤方法[J]. 计算机科学,2016,43(4):256-259.

[12] 于洪霞. 基于 SVM 的中文垃圾邮件过滤[D]. 哈尔滨:哈尔滨工程大学,2009.

[13] 李培国. 基于人工神经网的中文垃圾邮件过滤器的设计与实现[D]. 广州:暨南大学,2007.

[14] WANG A L, WANG Y, CHEN Y S. Hyperspectral image classification based on convolutional neural network and random forest [J]. Remote Sensing Letters, 2019, 10(11):1086-1094.

[15] 李艳涛,冯伟森. 堆叠去噪自编码器在垃圾邮件过滤中的应用[J]. 计算机应用,2015,35(11):3256-3260.

[16] 王永昌,朱立谷. 面向 Twitter 情感分析的文本预处理方法研究[J]. 中国传媒大学学报(自然科学版),2019,26(2):31-38.

[17] 韩冬煦,常宝宝. 中文分词模型的领域适应性方法[J]. 计算机学报,2015,38(2):272-281.

[18] 梁喜涛,顾磊. 中文分词与词性标注研究[J]. 计算机技术与发展,2015,25(2):175-180.

[19] 常建秋,沈炜. 基于字符串匹配的中文分词算法的研究[J]. 工业控制计算机,2016,29(2):115-116.

[20] 施询之,孙宁远,李骋罡. 基于微博信息库和文本分词的人机对话模型设计[J]. 计算机与现代化,2013(11):207-209.

[21] 马金娜,田大钢. 基于 SVM 的中文文本自动分类研究[J]. 计算机与现代化,2006(8):5-8.

[22] 郭振,张玉洁,苏晨,等. 基于字符的中文分词、词性标注和依存句法分析联合模型[J]. 中文信息学报,2014,28(6):1-8.

[23] 刘遥峰,王志良,王传经. 中文分词和词性标注模型[J]. 计算机工程,2010,36(4):17-19.

[24] 路金泉,徐开勇,戴乐育. 基于文本过滤的贝叶斯分类算法的改进[J]. 计算机与现代化,2016(9):100-103.

[25] LAI S W, LIU K, HE S Z, et al. How to generate a good word embedding? [J]. IEEE Intelligent Systems, 2016, 31(6):5-14.

[26] 杨楠,李亚平. 基于 Word2vec 模型特征扩展的 Web 搜索结果聚类性能的改进[J]. 计算机应用,2019,39(6):1701-1706.

[27] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient estimation of word representations in vector space [J]. arXiv preprint arXiv:1301.3781, 2013.

[28] 朱书眉. 基于词袋模型和关联规则的医学图像分类研究[D]. 南京:南京邮电大学,2016.

[29] SUTTON R S, BARTO A G. Reinforcement Learning: An Introduction [M]. Cambridge: MIT Press, 2018.

[30] WATKINS C J C H, DAYAN P. Technical Note: Q-learning [J]. Machine Learning, 1992, 8(3-4):279-292.

[31] SCHAUL T, QUAN J, ANTONOGLOU I, et al. Prioritized experience replay [J]. arXiv preprint arXiv:1511.05952, 2016.

[32] 刘全,翟建伟,章宗长,等. 深度强化学习综述[J]. 计算机学报,2018,41(1):1-27.

[33] 朱斐,吴文,刘全,等. 一种最大置信上界经验采样的深度 Q 网络方法[J]. 计算机研究与发展,2018,55(8):1694-1705.

[34] 尹宝才,王文通,王立春. 深度学习研究综述[J]. 北京工业大学学报,2015,41(1):48-59.

[35] MNIH V, KAVUKCUOGLU K, SILVER D, et al. Human-level control through deep reinforcement learning [J]. Nature, 2015, 518(7540):529-533.

[36] 朱斐,吴文,伏玉琛,等. 基于双深度网络的安全深度强化学习方法[J]. 计算机学报,2019,42(8):1812-1826.

[37] GALLAGHER B, ELIASSI-RAD T. Classification of HTTP Attacks: A Study on the ECML/PKDD 2007 Discovery Challenge [R]. Livermore: Lawrence Livermore National Laboratory, 2009.

[38] 王莹. 基于深度学习的文本分类研究[D]. 沈阳:沈阳工业大学,2019.