

# 基于 DCA 算法的微博虚假信息检测

杨超<sup>1,2</sup>, 项振辉<sup>1</sup>, 李涛<sup>3</sup>

(1. 湖北大学 计算机与信息工程学院, 武汉 430062;

2. 湖北省教育信息化工程技术研究中心, 武汉 430062;

3. 武汉科技大学 智能信息处理与实时工业系统湖北省重点实验室, 武汉 430065)

**摘要:** 通过对微博虚假信息的分析, 基于 DCA 算法的思想, 提出一种检测微博虚假信息的方法; 以新浪微博为例, 从虚假信息发布者的用户属性和虚假信息评论的文本内容两个方面进行分析; 从用户方面选取用户的特征属性, 如是否认证、有无简介、地址信息是否详细、关注数、粉丝数等, 从评论内容方面选取评论与微博内容的相关性、评论的支持性及其置信度等特征属性, 将以上属性的分析结果作为区别虚假信息与真实信息的特征信号, 并基于树突状细胞算法 (Dendritic Cells Algorithm, DCA) 实现新浪微博虚假信息的识别; 使用新浪微博真实数据对算法有效性进行了验证和对比实验, 结果表明该方法能够有效检测出新浪微博中的虚假信息, 具有较高的检测准确率。

**关键词:** 微博; 虚假信息; 人工免疫; 危险理论; 树突状细胞算法

## Micro-blog Misinformation Detection Based on Dendritic Cells Algorithm

Yang Chao<sup>1,2</sup>, Xiang Zhenhui<sup>1</sup>, Li Tao<sup>3</sup>

(1. School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China;

2. Hubei Education Information Engineering Technology Research Center, Wuhan 430062, China;

3. Hubei Provincial Key Lab of Intelligent Information Processing and Real-Time Industrial Systems,

Wuhan University of Science and Technology, Wuhan 430065, China)

**Abstract:** By the comprehensive analyzing of misinformation on micro-blog, applied the idea of Dendritic Cells Algorithm provided a method to test the misinformation on micro-blog, took the Sina micro-blog as an example, analyzed the information from two sides, one side was the property of misinformation publisher, the other side was the comment content of the misinformation, selected the user's properties, such as, identified whether the publisher was certified, had brief introduction, had detailed address, number of attention, number of fans etc. selected the comments' properties, such as the relativity between the content of micro-blog and comment, the support and confidence of comment etc. took the above property analyzing results as property signals to identify the misinformation and real information, and realized the identification of false information based on the Dendritic Cells Algorithm (DCA) on Sina micro-blog. We did the comparison experiment and test the effectiveness of the algorithm by using the real data on Sina micro-blog, the result shows that this method can test the false information on Sina micro-blog effectively, has high test accuracy rate.

**Keywords:** micro-blog; misinformation; artificial immunity; danger theory; dendritic cells algorithm

## 0 引言

微博, 又称“微博客”(Microblog), 是一种基于用户关系的信息分享、传播以及获取平台<sup>[1]</sup>。近几年微博迅速发展, 已经渗透到人们生活的各个方面, 成为人们获取信息的重要渠道之一。截至 2017 年 6 月, 微博用户规模达 29017 万, 手机微博用户规模 24086 万, 用户使用率 35.7%, 人均单日访问次数持续快速增长, 其中新浪微博人均单日访问次数达到 2.8 次<sup>[2]</sup>。由于微博用户数的爆炸性增长、信息传播的门槛低、缺乏有效的监督管理平台, 使

得微博中虚假信息盛行。例如: 2018 年 6 月中旬, 一篇微博称 12306 网站密码可能泄露, 引起了大量用户对 12306 关于信息安全方面的质疑, 后经过核查, 发现该网站并未发生用户信息泄露事件。恶意的虚假信息可能严重侵犯当事人合法权利, 造成社会恐慌, 煽动群体性事件, 甚至引发信任危机, 这对国家的发展尤为不利<sup>[3]</sup>。因此, 进行虚假信息检测的研究工作迫在眉睫。

基于对微博虚假信息的分析, 当前的研究可主要分为三类。

(1) 基于内容特征和用户特征: 内容特征包括博文的符号特征、链接特征、关键词分布特征和传播特性等特征, 用户特征包括发布者的粉丝数量、朋友数量、是否为认证用户等特征。如 Dayani 等人<sup>[4]</sup>选取提取用户特征和内容特征, 采用 K 最近邻 (K-Nearest Neighbors, KNN) 分类器以及 NB 分类器检测 Twitter 中的谣言。Gupta 等人<sup>[5]</sup>选取

收稿日期: 2018-09-02; 修回日期: 2018-09-20。

基金项目: 国家自然科学基金(61170306); 智能信息处理与实时工业系统湖北省重点实验室开放基金项目(znxx2018MS05)。

作者简介: 杨超(1982-), 男, 湖北武汉人, 博士, 副教授, 主要从事信息安全和人工免疫系统方向的研究。

用户特征和一些内容特征，基于决策树分类来检测 Twitter 上的虚假图片。但是这些方法只是简单的分析了文本的表面特征，并没有对文本的语义进行深入分析，并且随着网络的复杂化，虚假信息不再具有显著的识别的特征。因此，简单的基于内容特征和用户特征已不能有效的识别虚假信息。

(2) 基于信息传播过程：通过微博信息在传播过程中转发和评论者的把关行为来实时的更新微博信息的可信度来进行虚假信息的检测，如谢柏林等人<sup>[6]</sup>利用模型状态持续时间概率为 Gamma 分布的隐半马尔可夫模型来刻画信息转发者和评论者对流行的真实信息的把关行为，基于此进行虚假信息的在线检测。Liu 等人<sup>[7]</sup>在 Twitter 上进行实时的谣言检测，选取了两个实时谣言跟踪网站 (snopes.com 和 emergent.info)，结果显示该方法能将检测延迟减少 25% 和 50%。但该方法需要大量时间对虚假信息进行跟踪，处理效率较低。

(3) 基于评论特征：包括对文本情感分析<sup>[8]</sup>、倾向性分析<sup>[9]</sup>以及内容相关性分析。如段大高等人<sup>[10]</sup>从评论的角度出发，选取微博评论对博文内容的置信度、支持性以及评论与博文之间的内容相关性作为特征对评论进行 SVM 分类，通过统计微博下的异常评论的比例，判定其是否为微博虚假信息。该方法能较好的识别微博网络环境下的虚假信息，但其只对微博评论进行了深入的分析，没有考虑用户特征和虚假信息的传播特性方面的特征。

微博客中的信息往往具有一定的时效性和随意性，所以现有的虚假信息检测方法难以通过检测微博内容本身来判断是否虚假，大多是通过选取虚假信息的发布者特征和评论特征，训练分类器，然后用训练好的分类器进行微博虚假信息的检测。但是这些研究往往选取局部的、单一方面的特征进行检测，并没有全面的分析和挖掘影响微博虚假信息的各方面的特征。同时社交网络中的虚假信息检测问题与人体免疫系统中所遇到的问题有很大的相似性，如利用人工免疫危险理论中的树突状细胞算法 (Dendritic Cell Algorithm, DCA) 进行垃圾邮件群发检测<sup>[11]</sup>和服务器异常检测<sup>[12]</sup>等。

受此启发，本文通过对微博虚假信息的分析，选取了微博发布者的用户属性，微博评论两个方面的特征，将人工免疫系统中危险理论的原理和信号机制应用在社交网络中虚假信息的分析检测中，使用危险理论中的 DCA 算法实现微博虚假信息的检测。

## 1 树突状细胞 (DCA) 算法概述

1994 年, Polly Matzinger 提出了危险理论的思想, 认为“危险”才是引发免疫响应的关键<sup>[13]</sup>。2002 年英国诺丁汉大学的 Uwe 研究小组, 在文献 [14] 中首次提出可以考虑将机体免疫系统中的危险理论引入计算机安全领域。2007 年, Greensmith J 等人<sup>[15]</sup>设计并提出了基于危险理论

的树突状细胞算法 (Dendritic Cell Algorithm, DCA)。随后的研究中, DCA 算法普遍被应用于入侵检测<sup>[16-17]</sup>领域中。

在生物免疫系统中, 树突状细胞 (dendritic cells, DC) 是来自于骨髓内的髓样前体细胞, 构成了人体对抗入侵者的第一道防线的一部分<sup>[18]</sup>。DC 细胞收集组织中的抗原并进行提呈。未成熟的 DC 细胞 (immature DC) 暴露在有抗原存在的环境下的安全信号 (Safe Signals 信号, 以下简称 SS 信号) 和危险信号 (包括 Danger Signals 信号、PAMPS 信号和 Inflammatory CKS 信号, 以下分别简称 DS 信号、PAMP 信号和 IS 信号) 下, 根据两种信号的占比分化成为成熟 DC 细胞 (mature DC) 和半成熟 DC 细胞 (semi-mature DC) 两种, 最终由成熟抗原占总抗原的比重来决定是否产生了危险<sup>[19]</sup>。如图 1 所示, 未成熟 DC 细胞暴露在安全信号下会成为半成熟 DC, 暴露在危险信号下会成为成熟 DC。

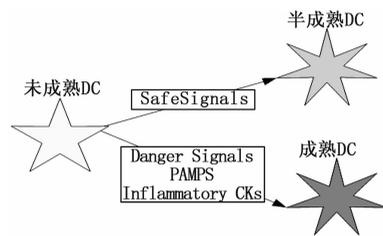


图 1 DC 成熟和分化所需信号的抽象视图

DCA 算法主要是模拟作为抗原呈递细胞的树突细胞的功能所提出的<sup>[20]</sup>, 其输入信号包括 4 种: (1) PAMP 信号 (病原体相关分子模式); (2) DS 信号 (危险信号); (3) SS 信号 (安全信号); 细胞正常死亡产生的信号, 代表系统中的正常行为; (4) IS 信号 (致炎信号)。对输入信号通过相关函数及权值矩阵进行融合处理后, 输出以下 3 种信号: (1) CSM (costimulatory molecules) 协同刺激分子: 该值用来判断未成熟 DC 细胞何时开始分化, 当  $CSM >$  迁移阈值时, 未成熟 DC 开始分化为半成熟 DC 或成熟 DC; (2) 半成熟 DC 细胞 (semi-mature): 表示当前细胞环境的安全程度, 同时该 DC 摄取到的所有抗原提呈为安全抗原; (3) 成熟 DC 细胞 (mature) 表示当前细胞环境的危险程度, 同时该 DC 摄取到的所有抗原提呈为危险抗原。当抗原达到判别次数时, 计算出代表该抗原异常程度的成熟环境抗原值 MCAV ( $MCAV = \text{抗原标记为危险抗原的次数} / \text{抗原被标记的总次数}$ )。如果 MCAV 值大于异常阈值, 则表明该抗原为异常抗原, 反之则为正常抗原。

DCA 算法具有自适应性强, 效率高等优点。基于以上内容, 本文将微博网络环境抽象为生物机体, 针对社交网络中微博发布者的用户属性, 微博评论特征、信息传播等特征进行分析定义, 将其映射为危险信号, 与 DCA 算法模型进行匹配, 并使用 DCA 算法设计一种新的微博虚假信息检测方法。本文涉及到的生物免疫系统中的七种信号及其

抽象定义详见文献 [21]。

## 2 基于 DCA 算法的微博虚假信息检测

### 2.1 微博虚假信息特征选取

微博上虚假信息的发布者个人信息和其评论内容有较为显著的特征,本文以目前国内用户规模最大的新浪微博平台作为研究对象,通过对近几年虚假信息特征变化的主流研究,结合相关文献的观点,得出如下分析结论。(1)从微博发布者的角度:①微博上虚假消息的发布者通常缺乏完善的用户简介、是否认证、所在地等个人信息。②虚假信息的发布者所发布的信息通常都带有一定的目的性,而其有价值的微博数少且影响力弱,造成其关注数远高于粉丝数<sup>[22]</sup>。(2)从虚假信息的评论内容:虚假信息下面的评论普遍支持性较弱,负面词汇多,语气的不确定性较强,且评论内容与原微博的内容相关性也较弱<sup>[23]</sup>。(3)从微博的传播角度:影响力大的用户对源消息的转发及评论会促进虚假信息的传播。

基于以上分析,本文从这三个角度总共选取了12个特征:(1)基于用户的特征:微博发布者的粉丝数、关注数、互相关注数、是否认证、有无简介、地址信息是否详细等6种特征;(2)基于文本内容的特征:用户的评论内容对微博的内容相关性、支持性以及置信度等3种特征;(3)基于传播特性的指标:选取评论用户所发微博的收藏数、转发数、点赞数等3种特征。选取并将其融合成6种能够区分虚假信息和真实信息的重要属性,具体的融合方法见2.2节中的定义1~6。

### 2.2 抗原信号选取

基于上述微博虚假信息的特点,分析一定时间段内的微博虚假信息情况,采取以下指标作为抗原信号,并通过多次对比实验和经验总结,确定定义公式中各项指标的权重系数。

定义1:用户身份评价(IE)。涉及多个属性变量,分别为有无简介(I)、是否认证(C)和地址信息详细程度(G),给各个属性的权重分别为0.3、0.4、0.3,计算方式如公式(1)所示。

$$IE = 0.3I + 0.4C + 0.3G \quad (1)$$

定义2:用户的粉丝关注比(FF)。即每个用户的粉丝数(Fans)与关注数(Followers)的比值,比值越小,则用户异常的可能性越大。计算方法如公式(2)所示。

$$FF = Fans / Followers \quad (2)$$

定义3:评论内容相关性(CR)。即评论内容与源微博信息之间的内容相关程度,本文通过对微博内容(U)和评论内容(C)进行词法分析<sup>[24]</sup>,统计文本的基本词得出构成微博及其评论的关键词集合,评论中出现的源微博的关键词越多,则评论内容与源微博信息之间越相关,即评论内容相关性越大。评论内容相关性的计算方法如公式(3)所示。

$$CR_i = \frac{|U \cap C_i|}{|U|} + \frac{|U \cap C_i|}{|C_i|} \quad (3)$$

其中:CR<sub>i</sub>表示当前微博下第i个评论与微博的内容相关性,U表示当前微博的关键词集合,C<sub>i</sub>表示当前微博下的第i个评论的关键词集合,|U|和|C<sub>i</sub>|分别表示微博和评论的关键词数量。

定义4:评论内容置信度(FP)。置信度是评论内容本身语气不确定性程度的刻画,置信度越大,则评论内容的不确定性越小。本文通过调用神箭手的自然语言处理API中的接口,得出每个评论内容的置信度FP。

定义5:评论内容支持性(SUP)。支持性即评论用户的观点对微博内容的支持程度,若评论中含有大量的负面词汇(假的,怀疑,造谣…)则评论内容对微博的支持程度低。本文通过对评论内容进行情感分析<sup>[25]</sup>,得出每个评论内容的情感正向比重(SUP<sub>POS</sub>)和情感负向比重(SUP<sub>NEG</sub>)。每个评论的内容支持性的计算方法如公式(4)所示。

$$SUP = SUP_{POS} - SUP_{NEG} \quad (4)$$

定义6:评论用户影响力(CI)。涉及多个属性变量,涉及多个属性变量,分别为评论数(J),转发数(R)和收藏数(C),即评论用户所发微博的被评论数、被转发数和被收藏数,各个属性的权重分别为0.3、0.2、0.5,计算方式如公式(5)所示。

$$CI = 0.3J + 0.2R + 0.5C \quad (5)$$

### 2.3 微博虚假信息检测算法实现

#### 2.3.1 信号映射

针对前文提到的微博虚假信息各项指标数据进行预处理,统一将其进行规格化处理。定义规格化函数f(x)如公式(6)所示。

$$f(x) = \begin{cases} \frac{x}{n-m} * 10, & x \in [m, n] \\ 10, & x > n \end{cases} \quad (6)$$

其中:x是原始信号值,当x∈[m,n]时,对信号值进行规格化处理,当时x∈[n,∞),信号最大值为10。

现将检测新浪微博虚假信息的相关属性进行如下映射。

(1)病原体相关分子模式PAMP:表明微博信息异常,存在虚假信息的特征,定义PAMP={⟨IE, FF, SUP⟩}

(2)危险信号DS:表明微博信息异常的可能性较高,也可能是真实的信息,但存在虚假信息的可能,定义DS={⟨CR, FP⟩};

(3)安全信号SS:表示微博信息真实的可能性较高,并处于正常状态,定义SS={⟨CR, FP, SUP⟩};

(4)致炎因子IS:表明微博信息总体上存在虚假的可能,起到放大PAMP、DS、SS信号的作用,定义IS={⟨CI⟩}。

#### 2.3.2 权值矩阵

如前文所述,DC收集组织中的抗原和信号,对输入信

号 (PAMP、DS、SS、IS) 进行计算处理, 输出三个信号: 协同刺激信号 (CSM)、半成熟信号 (SEMI) 与成熟信号 (MAT)。DCA 算法中输入信号对输出信号的影响如图 2 所示。

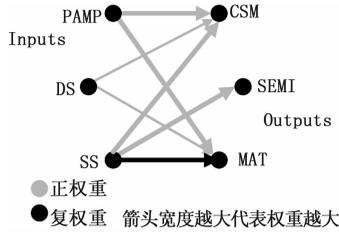


图 2 DC 信号处理抽象图

其中 PAMP 和 DS 对 CSM 信号及 MAT 信号有正影响, 起促进作用, 且 DS 信号的影响要比 PAMP 信号弱。SS 对 CSM 信号和 SEMI 信号值的具有正影响, 对 MAT 信号则具有负影响。由输入信号值到输出信号值的转换权值矩阵如表 1 所列。

表 1 DCA 信号转换权值矩阵

W(权值)	CSM	SEMI	MAT
PAMP	8	0	8
DS	3	0	4
SS	3	1	-4

表 1 中的权值矩阵中权值大小根据实验结果进行调整并确定最后的数值, 表示输入信号对输出信号的影响程度, 权值越大表明其对相应信号的输出的影响程度越大, 权值为负值即代表其对相应信号的输出为负影响。输入信号值转换为输出信号值的计算如公式 (7) 所示。其中 (1+IS) 为放大信号,  $W_p$ 、 $W_D$ 、 $W_s$  是根据表 1 中得出的计算输出信号是 PAMP 信号、DS 信号和 SS 信号所占的权重, 如计算时,  $W_p=8$ ,  $W_D=3$ ,  $W_s=3$ 。

$$C_{[CSM, SEMI, MAT]} = \frac{(W_p \times C_p) + (W_D \times C_D) + (W_s \times C_s)}{|W_p| + |W_D| + |W_s|} \times (1 + IS) \quad (7)$$

如前文所述, 当 CSM 信号达到迁移阈值时, 比较当前 DC 细胞中 SEMI 和 MAT 的大小。若  $SEMI \geq MAT$  时, DC 迁移为半成熟 DC 细胞, 同时标记当前抗原为正常抗原一次; 反之, DC 迁移为成熟 DC 细胞, 同时标记当前抗原为异常抗原一次。当抗原的判别次数达到抗原判别阈值, 计算出当前抗原的 MCAV 值。通过 MCAV 值与抗原异常阈值之间大小的判断, 标记该抗原为异常或正常。

### 2.3.3 算法流程描述

根据文献 [15] 的描述, 本文应用到微博虚假信息检测中的 DCA 算法流程如图 1 所示。

## 3 实验

### 3.1 数据获取

本文实验数据集选自文献 [10], 其数据采集来自新浪

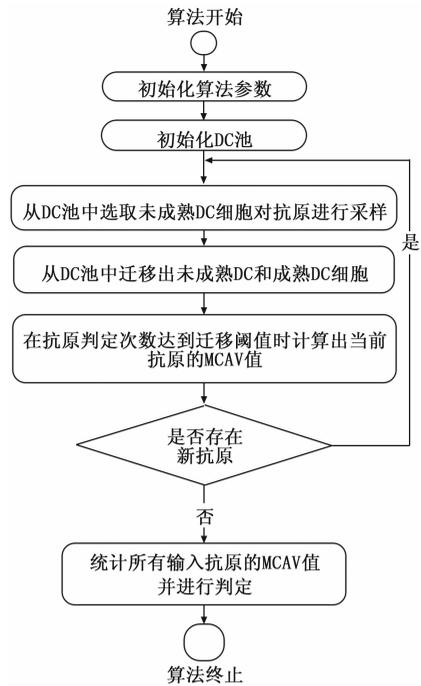


图 3 DCA 算法流程

算法伪代码如下:

```

Begin
初始化抗原池采集数目, 初始化DC细胞种群
FOR 每个DC
  IF CSM<迁移阈值Then
    在抗原池中随机采集未被标记的抗原, 并收集
    PAMP、DS、SS和IS信号, 依据权值矩阵计算
    CSM、SEMI和MAT信号并进行累加;
  END IF;
  If CSM>=迁移阈值Then
    比较semi和Mat的大小,DC发生迁移并标记该
    DC采集的抗原状态;
  END IF;
  If 抗原判定总次数=抗原判别阈值Then
    计算MCAV=抗原被判为异常次数/抗原判定总
    次数, 比较MCAV与异常阈值的大小;
  If MCAV>=N then抗原标记为异常;
  Else 抗原标记为正常;
  End If; End If;
End FOR;
If DC采集抗原次数>=DC生命周期Then
  抛弃该DC;
End If;
    
```

图 4 算法伪代码

微博社区管理中心和新浪微博 API 接口获取的热门微博, 包含 100 个谣言和 100 个非谣言, 谣言微博以微博官方辟谣为依据, 经过筛选与数据处理得到的数据集统计信息如表 2 所示。

表 2 数据集统计信息

	微博数	总评论数
真实微博	100	25386
虚假微博	100	41706

### 3.2 评价指标

算法结果评估包括查准率 ( $P$ )、查全率 ( $R$ ) 以及  $F1$  值等评价指标。其中查准率和查全率用来评价实验准确性,  $F1$  值对实验综合表现的评价指标。各指标的详细定义如下。

(1) 查准率  $PR$  的定义如公式 (8) 所示。

$$P = \sqrt{\text{class}^+ \times \text{class}^-} \quad (8)$$

式中,  $\text{class}^+ = TP / (TP + FP)$ ,  $\text{class}^- = TN / (TN + FN)$ , 分别表示分类器对虚假信息 and 真实信息的分类准确率, 其中:  $TP$  是被正确识别为虚假信息的微博数,  $FP$  是被错误识别为虚假信息的微博数,  $TN$  是被正确识别为真实信息的微博数,  $FN$  是被错误识别为真实信息的微博数。  $PR$  表示分类器平均准确率。平均准确率  $PR$  的高低由  $\text{class}^+$ 、 $\text{class}^-$  两者值的高低共同决定。

(2) 查全率  $R$  的定义如公式 (9) 所示。

$$R = TP / (TP + FN) \quad (9)$$

(3)  $F1$  值的定义如公式 (10) 所示。

$$F1 = (2P * R) / (P + R) \quad (11)$$

### 3.3 实验结果与分析

为了验证基于人工免疫危险理论的虚假信息检测算法的有效性, 本文通过对微博虚假信息的特征分析, 与前文所提及的文献 [10] 提出的基于 SVM 的分类方法进行了对比实验, 其中基于 SVM 的分类方法按 8:2 的比例随机划分数据集, 即数据集的 80% 作为训练集, 余下的 20% 作为预测集。在实验结果中比较了查准率、查全率及  $F1$  值等 3 个指标。实验抽取上述数据集的数据作为样本, 使用两种识别方法分别进行实验, 对比结果如图 5 所示。实验结果表明, 基于 DCA 算法微博虚假信息检测对比 SVM 分类方法有较好的适用性和较高的准确率。

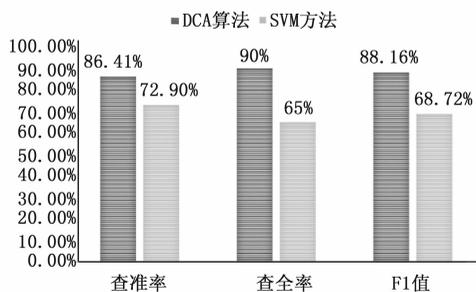


图5 实验结果对比

## 4 结束语

本文借鉴生物免疫系统的思想, 采用 DCA 算法进行微博虚假信息的检测。通过分析新浪微博中虚假信息的特征, 根据微博真实信息与虚假信息在发布者用户属性, 评论特征和信息传播等特征表现上的差异, 判断微博信息是否虚假。实验结果表明, 该方法的检测准确率较高, 是检测微博虚假信息的一种有效方法。但是本文微博虚假信息检测方法依赖于微博评论的数量, 当微博评论增多时, 说明虚假信息的危害已经产生, 未来应该将重点放在虚假信息的

预测上, 拟采用更复杂的特征, 通过实现微博虚假信息提前检测以减少其造成的危害和不良影响。

### 参考文献:

- [1] 蒋盛益, 陈东沂, 庞观松, 等. 微博信息可信度分析研究综述 [J]. 图书情报工作, 2013, 57 (12): 136-142.
- [2] 佚名. CNNIC 召开第 40 次《中国互联网络发展状况统计报告》发布会 [J]. 中国信息安全, 2017 (8): 25-25.
- [3] 祖坤琳, 赵铭伟, 郭凯, 等. 新浪微博谣言检测研究 [J]. 中文信息学报, 2017, 31 (3): 198-204.
- [4] Dayani R, Chhabra N, Kadian T, et al. Rumor detection in twitter: An analysis in retrospect [A]. IEEE International Conference on Advanced Networks and Telecommunications Systems [C]. IEEE, 2016: 1-3.
- [5] Gupta A, Lamba H, Kumaraguru P, et al. Faking Sandy: characterizing and identifying fake images on Twitter during Hurricane Sandy [A]. Proceedings of the 22nd international conference on World Wide Web companion. International World Wide Web Conferences Steering Committee [C]. 2013: 729-736.
- [6] 谢柏林, 蒋盛益, 周咏梅, 等. 基于把关人行为的微博虚假信息及早检测方法 [J]. 计算机学报, 2016, 39 (4): 730-744.
- [7] Liu X, Nourbakhsh A, Li Q, et al. Real-time Rumor Debunking on Twitter [J]. 2015: 1867-1870.
- [8] 赵妍妍, 秦兵, 刘挺. 文本情感分析 [J]. 软件学报, 2010, 21 (8): 1834-1848.
- [9] Liu B. Sentiment analysis and subjectivity [A]. In: Indurkha N, Damerau FJ, eds. Handbook of Natural Language Processing [C]. Boca Raton: CRC Press, 2010. 627-666.
- [10] 段大高, 王长生, 韩忠明, 等. 基于微博评论的虚假消息检测模型 [J]. 计算机仿真, 2016, 33 (1): 386-390.
- [11] 杨超, 李子怡. 基于树突状细胞算法的垃圾邮件群发检测 [J]. 传感器与微系统, 2015 (10): 133-136.
- [12] 王新新, 梁意文. 树突状细胞算法在 Web 服务器异常检测中的应用 [J]. 计算机工程与应用, 2016, 52 (24): 148-152.
- [13] Matzinger P. Tolerance, Danger and the Extended Family [J]. Annual Review of Immunology, 1994, 12 (1): 991-1045.
- [14] Aickelin U, Cayzer S. The Danger Theory and Its Application to Artificial Immune Systems [A]. In Proceedings of the 1st Internat Conference on ARTificial Immune Systems (ICARIS-2002) [C]. Canterbury, UK, 2002: 141-148.
- [15] Greensmith J, Aickelin U. The Dendritic Cell Algorithm [J]. Revista Clínica Espanola, 2007, 202 (10): 552-554.
- [16] 王亚芹, 梁意文, 刘赛. 基于树突状细胞算法的应用层 DDoS 攻击检测 [J]. 计算机工程与设计, 2015 (4): 841-845.
- [17] 王舒洋, 慕晓冬, 张力. 基于粗糙集的改进树突状细胞算法 [J]. 计算机工程与应用, 2016, 52 (23): 172-175.
- [18] Gu F, Greensmith J, Aickelin U. The Dendritic Cell Algorithm for Intrusion Detection [J]. Computer Science, 2012: 84-102.