文章编号:1671-4598(2019)04-0088-04 DOI:10.16526/j.cnki.11—4762/tp.2019.04.021 中图分类号:TP301.6 文献标识码:A

智能设备网络虚假信息行为识别与控制技术研究

吴 珊,李跃新
(湖北大学 计算机与信息工程学院,武汉 430062)

摘要:传统智能设备网络虚假信息行为识别技术识别范围小,准确性低,在识别后不能快速地采取控制手段进行控制,导致事态进一步恶化;针对上述问题,研究了一种新的智能设备网络虚假信息行为识别与控制技术,设定虚假信息模型,由神经网络和BP网络构成,通过互联网控制,通过检测触发词、信息分类、虚假信息识别完成精确识别工作,控制模型由演示平台、网络中心组成,能够针对不同类型的虚假信息给出不同的控制手段;与传统技术进行实验研究,结果表明,给出的智能设备网络虚假信息行为识别技术能够完成更大范围的识别,提高识别准确率,在识别后对应的控制技术会快速采取有效手段控制虚假信息的散布。

关键词:智能设备;网络虚假信息;行为识别;行为控制技术

Research on False Information Behavior Recognition and Control Technology in Intelligent Device Network

Wu Shan, Li Yuexin
(School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China)

Abstract: The traditional intelligent device network false information behavior recognition technology has a small recognition range and low accuracy. It cannot be quickly controlled by control after identification, which leads to further deterioration of the situation. Aiming at the above problems, this paper studies a new intelligent device network false information behavior recognition and control technology, and sets up a false information model, which is composed of neural network and BP network. It is controlled by the Internet and detects trigger words, information classification and false information. The precise identification work is completed. The control model is composed of a demonstration platform and a network center, and can provide different control means for different types of false information. Experimental research with traditional techniques shows that the intelligent information network false information behavior recognition technology can complete a wider range of recognition and improve the recognition accuracy. After the identification, the corresponding control technology will quickly take effective measures to control the false information. spread.

Keywords: intelligent device; network false information; behavior recognition; behavior control technology

0 引言

网络时代极大方便了人们的日常交流,移动设备和智能设备能够以非常快速的方式接入网络。网络信息具有自由性、交互性、多元性等特点,为信息的传递带来更便捷的方式,信息获取规模也在不断扩大。相较于其它信息传播媒介,网络媒体规模更大、传播速度更快,每一个网民都可以在网络上发布自己的言论,使网络信息传播实时性更强。近年来社交网络越来越丰富,微博、BBS论坛、贴吧等形式的出现让更多的网民参与话题的探讨中,人们可以随心所欲地在网络上抒发感情[1]。

但是由于人们在网上发表言论不需要承担任何责任,所以虚假信息很容易被散布,这些虚假信息左右着大众的情感和判断,甚至对社会造成威胁。人们很容易盲目相信网络的一些不实言论和过激言论,并大肆传播,而网民自身对这些言论的真假是没有准确判断的,他们只是为了抒发个人情绪[2]。不法分子利用网络的开发性引导舆论,危害公众,破坏政府形象,一些恐怖信息的散布甚至会影响社会的安定,造成社会动荡不安。

综上所述,及时识别虚假信息,并对虚假信息进行控制对于社会安全稳定的发展具有重大意义。网络信息量大,传统的识别技术和控制技术在实现时有很大的局限性,实时性差,识别效率低,控制效果不好。本文研究了一种新的识别技术和控制技术,能够将调查信息结构化,再统一放入到数据库中,提高识别效率,加强控制效果[3]。

1 智能设备网络虚假信息行为识别技术

网络虚假信息可以划分成两个元素,分别为触发词和散布时间,触发词和虚假信息的其它组成词不一样,它是最具代表性的词,能够准确地描述所发生事件,散布时间指的是虚假信息发送的最初时间。人们在调查虚假信息时,要在对社会有破坏、损坏和危害的信息中查找,将可能存在虚假的信息提取出来,分布在各个文本中,主要的文本有4类:攻

收稿日期:2019-01-02; **修回日期**:2019-01-26。
基金项目:湖北省科技厅科技支撑项目(2014BAA089)。
作者简介:吴 珊(1998-),女,陕西咸阳人,大学本科生,主要从事图像处理和实体关系抽取方向的研究。
通讯作者:李跃新(1958-),男,武汉人,博士,教授,主要从事人工智能与知识工程、智能控制系统、嵌入式技术方向的研究。

击行为文本、受伤行为文本、死亡行为文本和拘捕行为文本。在寻找出网络虚假信息后，对信息进行简要识别。简要识别过程主要有三步：首先设定 LDA 模型，将可能存在虚假信息的舆情文档统一到一起，对其进行识别，在不同阶段识别不同的文档事件，并进行针对性操作，逐层处理，每次处理的数量都要减小，提高针对性；然后对没有虚假信息的舆情进行过滤，将所有的异常句子集合到一起，利用 ACE 标准识别，寻找特征向量，再通过分类器识别；最后构建共建网络，通过可视化的方法识别整个信息。

网络虚假信息识别模型如图 1 所示。

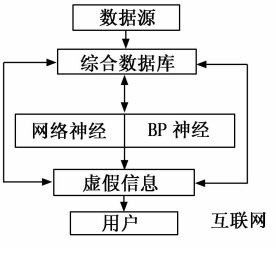

图 1　网络虚假信息精确识别模型

智能设备包括的类型很多，每天有大量信息在智能设备中流传，必须要采取统一的管理手段，本文设定的网络虚假信息识别模型以互联网为中心网络，采用统一控制端控制识别工作的进行。识别模型中拥有匹配模板，匹配模板中含有神经网络，可以处理一些复杂的信息，增加识别的种类，神经网络不会损失、损坏信息，使信息造成畸变，同时能够加强运行速度，提高适应能力，增强分辨率。网络虚假信息识别模型对图像识别和文字识别采用统一的识别原理，对信息能够预处理，从原始数据中剔除无用信息[4]。图像识别要相比文字识别更加复杂一些，特征值也更加复杂，因此要设定目标图像，根据目标图像进行识别。除了神经网络外，模型中还加入了 BP 网络，能够自动对被识别的样本进行训练，分析样本的敏感度，使网络陷入局部最小点，BP 网络可以对网络信息做归一化处理，通过构建的坐标图像完成识别。坐标图像具有平移、缩放和旋转的能力，识别率很高，差距能够达到 30 个点。系统在工作时会产生一定的噪声，因此必须要加入一定的降噪技术，提高识别率，使识别效果趋于稳定[5]。

虚假信息在做出简要识别后，要进行精确识别，精确识别要比简要识别复杂得多，网络虚假信息精确识别流程如图 2 所示。

第一步：检测触发词。网络舆情数据量大，开放性强，如果全部分析的话，将会浪费大量时间，分析无用信息和干扰数据也会投入更高的成本，降低系统的工作性能，检测触发词是一种很好的识别手段。触发词检测能够自动做去噪处理，剔除无用数据，使系统能够高效稳定运行。检测触发词对于分析虚假信息有很重要的意义，通常不含有触发词的句子，就不含有虚假信息，可以直接将其剔除。触发词是最能表现出事件的词语，但是有的虚假信息中不

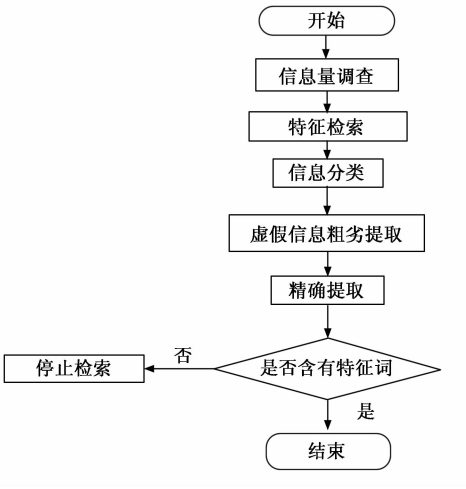

图 2　网络虚假信息精确识别流程

含有触发词，所以要检测与触发词类似的词[6]。

第二步：信息分类。分类检测是识别虚假信息最重要的步骤之一，本文设计的分类检测器为 SVM 检测器，通过非映射识别手段将高维空间样本降低成低维空间样本，使其能够通过线性手段处理[7]。SVM 检测器采用平面检测的方法识别网络虚假信息，能够将分类信息的风险降到最低，从而获得更好的信息。SVM 检测器对于异常信息的检测能力很强，即使信息量很少，它也能够逐层检测到信息，识别到关键特征，然后进行分类。

第三步：智能设备网络虚假信息识别。通过建立虚假信息识别网络对分类后的信息进行识别。虚假信息识别网络是一种大规模网络。网络结构如图 3 所示。

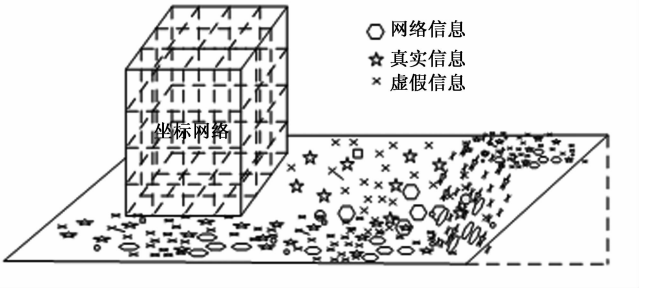

图 3　虚假信息识别网络

图 3 中的虚假信息识别网络的每个点都是实体点，记录大量人名、地名和组织名，再将这些实体点以特定的方式连接起来，形成实体网络。在实体网络中分析异常行为以及是否出现虚假信息。虚假信息识别网络拥有多个拓扑节点，节点和节点之间的距离以及角度都是识别的重要要素。

2　智能设备网络虚假信息行为控制技术

智能设备包含的信息非常多，用户在阅读、评论或者是转发这些信息时，既是消费者，也是把关者[8]。用户自己要使用有效的检测方法识别信息。由于网络使用者的生活经验、个人水平不同，所以对于虚假信息的识别能力也

不同，通常识别度越高的人，越能通过正确的方式识别网络信息。不同的人在识别到虚假信息时采取的态度也是不同的，绝大多数人对虚假信息都是持否定态度的，但是也有人对虚假信息部分人对虚假信息持中立态度，甚至有些人在得知该信息是虚假信息后还支持其继续传播，因此必须要及时采取有效手段对虚假信息进行控制。智能设备网络虚假信息识别与控制是息息相关的，对网络信息要尽早检测，检测结束后及时进行控制，防止虚假信息进一步扩大，危害他人的利益，造成社会的动荡。

本文使用的控制技术会根据得到的智能设备网络虚假信息虚假程度分成不同等级。对于不同类型的网络虚假信息处理方式不同，一些虚假信息由于最初没有及时制止传播，在网上大量传播，得到网民多次转载和评论，这时就要采取强制手段控制智能设备网络虚假信息的传播[9]。找到散发该信息的根源以及大量散布这些信息的人，提取相关人的特征值，将这些人分成不同簇，通过人工检验和筛选的方式，将每一个簇的人都编辑上编号，分析发布人和散发人的资料，对应分类。对于行为恶劣的可以依法加入刑事处罚，对于行为较轻的人采取警告处分。

对于一些刚刚被散发出来，还没有在网上大肆传播的网络虚假信息，要将这些信息集成不同的数据集，对这些数据集进行预处理，建立观测值，按照虚假信息真实度作为观测序列。训练控制模型，寻找模型参数值，控制虚假参数。

以马尔可夫模型控制虚假信息，控制模型如图 4 所示。

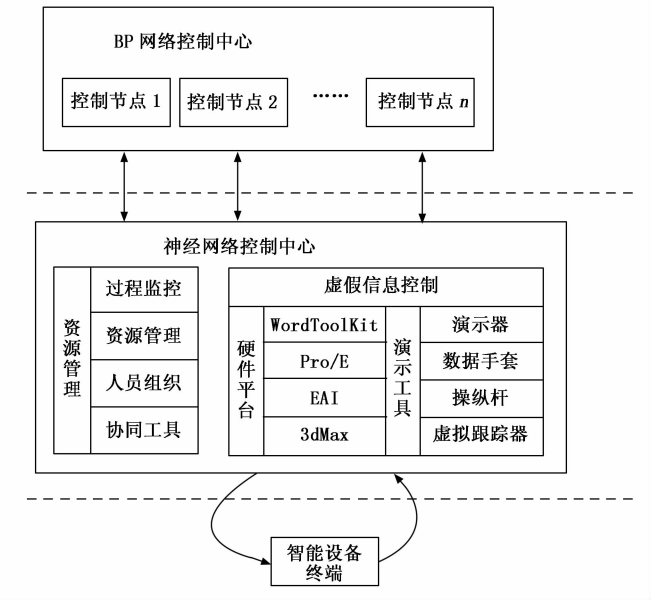

图 4 网络虚假信息控制模型

图 4 的虚假信息控制模型具有自然分割的能力，模型内部又有红外探测仪，能够将虚假信息和正常信息分离开，通过增强虚假信息的对比度控制虚假信息的传播。提取虚假信息分量，通过训练原始数据，找到最佳维权系数，提高控制效果。智能设备网络虚假信息的具体控制过程如图 5 所示。

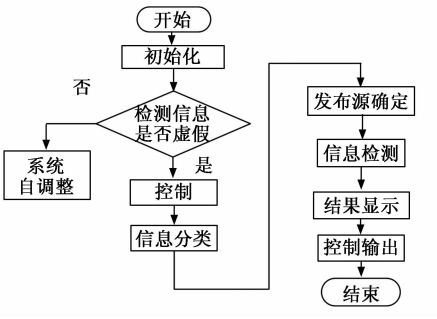

图 5 虚假信息控制过程

工作人员要仔细了解网络发布的信息，对发布的信息进行审核。同时对网民诚信度进行排名，设定诚信度排行榜，对于诚信度不高的网民发布的信息要重点排查，以道德水准的标准评估网络信息是否真实。由于网络信息的开放性，所以控制起来十分困难，工作人员要结合其他数据进行控制，不能单纯依赖一个手段，仔细核实重点区域，及时删除无用信息，同时发布真实信息，指责发布虚假信息的人，利用网络谴责居心不良的人。

很多舆论的制造是为了造成某种效果，这些虚假信息通常是带有攻击性的，受害者可能会被这些虚假信息严重打击，而一些不明真相的人，也会完全不考虑信息的真实性，盲目跟风。这时候，智能设备网络管理者采取强制手段，发布澄清信息，证明网络上大肆传播的信息是不真实的、虚假的、被人恶意利用的，然后严禁他人继续评论和转发，防止事态进一步恶化。

一旦调查出散发不实消息的人要利用法律手段进行惩罚，并将惩罚结果公布在网上，让人引以为戒。智能网络还要实行实名制，使人们在发布信息时有压力，不敢随便发送不实消息。

3 验证实验

3.1 实验目的

为了检测本文研究的智能设备网络虚假信息行为识别与控制技术实际效果，与传统技术进行对比，分析识别效果和控制效果。

3.2 实验参数设置

设置实验参数如下：设定工作系统的电源电压为 150～400 V，工作电流为 50～100 A，工作频率 200 Hz，系统的时钟精度为 1.50 s/d，工作温度为－50～80 ℃，消耗功率为 15 kW，工频耐压为 500 V，冲击电压为 200 V，硬件接口方式为红外通信接口，维护方式为 MID 维护，运营环境为 ADE 环境。

3.3 实验结果与分析

根据上述参数进行实验，选用本文研究的网络虚假信息行为识别与控制技术和传统技术对同一区域网络信息进行识别，分析识别效果和控制效果，根据结果对两种技术的性能进行具体的分析。得到的实验结果如图 6 所示。

3.3.1 虚假信息识别技术对比结果

在智能设备中构建三维网络，分别建立 x 轴、y 轴和 z

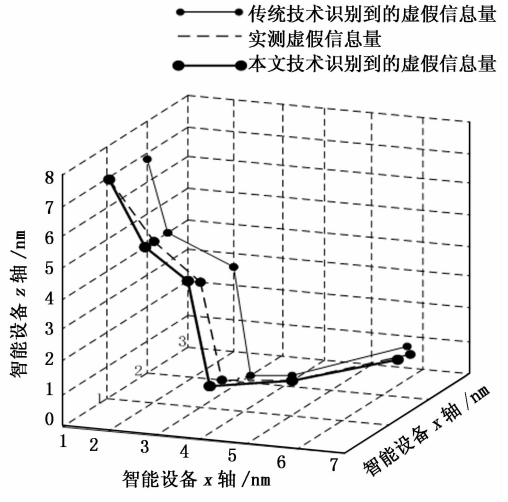

图 6　识别效果实验图

轴，以纳米为单位，对虚假信息进行识别，分析传统识别技术、本文识别技术识别到的虚假信息和实际值的出入。观察上图可知，无论是传统识别技术，还是本文技术都很难完全识别到网络信息的虚假信息，但是本文识别技术对于信息的识别精度要优于传统识别技术，对于虚假信息的识别，本文技术出现了多个吻合点，但传统识别技术始终与实际值有着很大不同。观察图 6 可以发现，传统技术的识别精度仅为 78.25%，而本文技术的识别精度可以达到 83.56%，虽然对虚假信息的遗漏依然很大，但是已经是目前学术界的一大进步标志。

3.3.2　虚假信息控制技术对比结果

选取传统控制技术和本文控制技术对虚假信息进行控制，控制时间相同，以 1：1000 字节为单位记录控制效果。观察图 7，在相同时间内，传统控制技术仅能控制 6000 字节的虚假信息，而本文的控制技术能控制 16000 字节的虚假信息，控制能力超过传统技术的二倍。传统控制技术仅能针对小范围信息进行控制，而本文技术能够针对大范围信息进行控制。

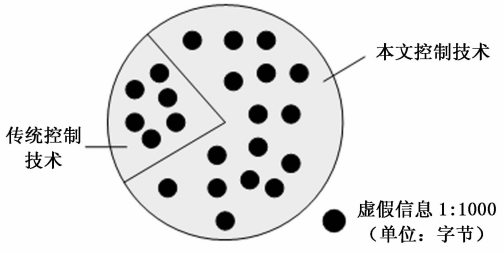

图 7　控制效果实验图

3.3.3　两种技术之间的紧密度分析

观察表 1 可以发现，当传统识别技术识别到虚假信息后，传统的控制技术很难快速采取有效的控制手段对虚假信息进行控制，防止事件进一步扩大。当虚假信息量达到 1.825 字节，传统识别技术与传统控制技术的时间间隔高达 2.56 小时，造成非常不好的影响。本文研究的技术虽然不能在识别到虚假信息后，就立刻采取有效的解决措施，但是两项技术中的工作间隔最大不会超过 1 个小时，可以较为快速地对虚假信息进行处理，防止事件想进一步恶化的方向发展，将造成的个人损失、经济损失、社会损失和名誉损失降低到最小化，让人们能够在一个相对绿色、安全的环境下沟通，防止不法分子利用网络平台攻击他人，为自己谋求利益。

表 1　紧密度实验结果分析

识别到的虚假信息总量/字节	传统识别技术与传统控制技术的时间间隔/h	本文识别技术与本文控制技术的时间间隔/h
0.452	0.52	0.13
0.685	0.83	0.41
0.982	1.17	0.63
1.237	1.68	0.72
1.439	1.92	0.85
1.671	2.31	0.89
1.825	2.56	0.93

3.4　实验结论

根据上述实验结果与分析，得到如下实验结论：传统的网络虚假信息识别和控制技术效果不强。传统的识别技术只能针对一些在网上引起关注量很大的信息进行识别，而对于一些在网上缺少关注量，或者没有关注量的信息很少识别，传统技术只针对固定地区进行识别，识别范围很小，对于关键词的提取能力很差。由于传统技术的智能性不强，所以对于网络信息的识别性也不强，只能识别到包含关键词的虚假信息。但是不能识别到不包含关键词的虚假信息。本文研究的虚假信息识别技术拥有多个网络终端，能够针对智能设备的各个网络进行识别，哪怕是没有关注量的虚假信息，本文技术也能很好地识别，识别范围广。除此之外，本文的识别技术引用更先进的智能技术，对于虚假信息的识别不仅仅局限于只能识别到含有关键词的虚假信息，对一些不含有关键词，但和关键词类似的虚假信息也能够进行识别，识别精确度高。

传统控制技术执行力度不足，所以产生的震慑力不强，很多人在网上散布信息后账号被封，就立刻新建另一个账号，这种控制手段治标不治本。本文采用的控制技术对于虚假信息的传播有着强力的控制，从根源杜绝虚假信息散布，一旦发现，给予严惩，同时对于事态严重的虚假信息，严禁评论和转载，杜绝事态恶化。

传统识别技术和控制技术联系不够紧密，往往发现传统识别技术很久以后才采取措施进行控制，而这时候造成的损失更大。本文的识别技术和控制技术在同一个中心网络运行，一旦识别到虚假信息后，系统就会立刻下达控制指令，根据所识别到的虚假信息性质选择合适的控制手段。综上所述，本文研究的虚假信息识别和控制手段，实时性更高、工

（下转第 133 页）