基于自适应卷积滤波的网络近邻入侵检测算法

卢 强[1] 游荣义[1] 叶晓红[2]
(集美大学理学院 福建 厦门 361021)[1] (集美大学诚毅学院 福建 厦门 361021)[2]

摘 要 深度无线传感组合网络中的近邻路由节点入侵具有载荷快速变化性,难以对新出现的攻击类型和网络异常行为进行有效识别,因此提出一种基于自适应卷积滤波的网络近邻入侵检测算法。在深度无线传感组合网络的传输信道中进行网络流量采集,构建网络入侵信号模型,在时间和频率上分析网络入侵信号的能量密度和攻击强度等特征信息,构建自适应卷积滤波器进行网络传输信息的盲源滤波和异常特征提取;采用联合时频分析方法进行网络近邻入侵特征信息的频谱参量估计,根据频谱特征的异常分布状态进行无线传感组合网络近邻入侵检测。仿真实验结果表明,采用该方法进行网络入侵检测的准确率较高,对未知的网络流量样本序列具有较高的识别能力和泛化能力,且所提算法优于传统的HHT检测算法、能量管理检测方法。

关键词 网络,入侵,检测,自适应,卷积滤波
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.07.026

Network Nearest Neighbor Intrusion Detection Algorithm Based on Adaptive Convolution Filtering

LU Qiang[1] YOU Rong-yi[1] YE Xiao-hong[2]
(School of Science, Jimei University, Xiamen, Fujian 361021, China)[1]
(Chengyi University College, Jimei University, Xiamen, Fujian 361021, China)[2]

Abstract The intrusion of the nearest neighbor routing nodes in the deep wireless sensor combination network has the characteristic of fast load variation, and it is difficult to effectively identify the types of attacks and abnormal network behavior. Therefore, this paper proposed a network nearest neighbor instrusion detection algorithm based on convolution filtering. Network traffic is collected in deep wireless sensor combination network, and network intrusion signal model is constructed. Energy density and attack strength of network intrusion signal are analyzed in terms of time and frequency, and blind source filtering and abnormal characteristic extraction of network information are achieved by constructing an adaptive convolution filter. Joint time-frequency analysis method is used to estimate the spectrum parameters of network intrusion feature neighbor information, and intrusion detection of wireless sensor network is done according to the abnormal distribution of spectrum features. Simulation results show that this method has high accuracy for network intrusion detection, has high recognition ability and generalization ability for the unknown network traffic sample sequence, and is superior to HHT detection method and energy management method.

Keywords Network, Intrusion, Detection, Adaptive, Convolution filtering

随着网络应用平台的不断推广,网络接入端口源不断增多,从而导致网络病毒入侵的介质增多。网络入侵会产生中断链接、拒绝服务、信息泄露和系统崩溃等问题。网络病毒入侵的种类复杂,采用传统的防火墙拦截等方式不能有效抵御未知网络病毒入侵的攻击,且该方式对网络入侵的拦截能力不佳,因此需要研究一种有效的主动网络病毒入侵检测方法,构建网络入侵检测系统,采用积极主动的网络安全检测技术对可疑的网络传输信息和数据进行识别和拦截,发现网络入侵行为,确保网络安全[1]。由于网络近邻路由节点入侵具有载荷快速变化性,对入侵的可识别性较差,因此研究网络近邻入侵检测方法在网络建设中具有重要的现实意义。

网络入侵检测技术主要分为异常流量挖掘检测和入侵数据的信号分析检测两大类,通过采集网络传输链路和通信信道中的流量数据,结合信息处理和大数据分析方法,进行网络传输流量的异常行为识别和检测[2]。传统的检测方法主要有时频检测方法、小波检测方法、主成分特征检测方法以及神经网络检测方法等[3-4],上述方法把深度无线传感组合网络中的流量传输时间序列解析模型分解为含有多个非线性成分的统计量来进行入侵异常特征提取,从而实现入侵检测。根据上述检测原理,研究人员进行了研究并取得了一定的成果。其中,文献[5]提出了一种基于偏移量递阶控制的网络入侵HHT检测算法,对网络潜质入侵信息进行Hilbert变换信号

到稿日期:2017-07-21 返修日期:2017-11-06 本文受福建省中青年教师教育科研项目:太阳能电池板光源自动跟随系统设计(JA15277)资助。
卢 强(1981-),男,硕士,工程师,主要研究方向为计算机信息;游荣义(1957-),男,博士,教授,主要研究方向为信号处理、神经网络应用;叶晓红(1982-),女,硕士,工程师,主要研究方向为计算机通信,E-mail:cvss300/@sina.com.cn(通信作者)。

处理，实现入侵信号的离散时频分析和时延估计，减小包络线失真引起的边界控制误差，从而提高检测概率；但该检测方法的虚警概率较高，容易对正常的网络信息造成误拦截。文献[6]提出了一种基于优化数据处理的深度信念网络模型的入侵检测方法，其采用随机共振模型进行网络入侵数据的冗余滤除，结合模糊 C 均值聚类方法进行网络入侵异常数据聚类，从而提高入侵检测的抗干扰能力；但该方法计算开销较大，入侵检测的实时性不好。文献[7]基于能量管理的网络入侵防波动控制方法，采用经验模态分解方法进行网络入侵波动的能量预测，该方法对网络近邻入侵检测的泛化能力和自适应能力不强。

针对上述问题，本文提出一种自适应卷积滤波的网络近邻入侵检测算法。首先，在深度无线传感组合网络的传输信道中进行网络流量采集，构建网络入侵信号模型，在时间和频率上分析网络入侵信号的能量密度和攻击强度等特征信息；然后，构建自适应卷积滤波器进行网络传输信息的盲源滤波和异常特征提取，采用联合时频分析方法进行网络近邻入侵特征信息的频谱参量估计，并根据频谱特征的异常分布实现网络近邻入侵检测；最后，进行仿真实验，以证明本文方法在提高网络入侵检测的准确性方面具有优越性能。

1　网络入侵信号的分析模型及预处理

1.1　网络入侵信号模型

为了实现对深度无线传感组合网络的近邻入侵的有效检测，采用信号处理方法构建网络入侵信息模型，并建立深度无线传感组合网络的流量采样和数据传输结构模型；结合宽平稳随机信号处理方法进行网络入侵特征分析和统计处理。在深度无线传感组合网络中，数据传输是一个高斯宽平稳的随机线性处理模型，采用时间-频率联合特征分析方法[8]构建深度无线组合网络的信道传递模型，描述为：

$$x(t)=\mathrm{Re}\{a_n(t)\mathrm{e}^{-j2\pi f_c\tau_n(t)}s_l(t-\tau_n(t))\mathrm{e}^{-j2\pi f_c t}\} \tag{1}$$

采用翻转正交频分复用(Flip-OFDM)方法对深度无线传感组合网络采样输出的通信信号 $X(t)$进行归一化处理：

$$X'(t)=X(t)/\parallel X(t)\parallel \tag{2}$$

其中，$\parallel X(t)\parallel$ 表示对 $X(t)$取模。进一步对网络的传输流量信息使用宽时域窗进行自适应加窗处理，得到网络传输信道中的流量采集输出为：

$$X(u)=\sqrt{\frac{1-j\cot\alpha}{2\pi}}\int_{-\infty}^{+\infty}x(t)\exp[j\frac{t^2+u^2}{2}\cot\alpha-j\csc\alpha]\mathrm{d}t \tag{3}$$

其中，$x(t)$表示输入到传输信道中的深度无线传感组合网络的通信数据，α 为时间窗函数。通过分数阶傅里叶变换，得到深度无线传感组合网络中病毒近邻入侵信息的相关匹配度为：

$$\lambda_{SRm}=\sum_{i=1}^{M}\lambda_i p_{im} \tag{4}$$

在第 n 条数据传输链路中心的时间轴上进行连续经验模态分解，通过信道调制得到对病毒入侵数据具有同态特征的样本相关数据的幅频包络，为：

$$\rho_{SRm}=\frac{\lambda_{SRm}}{\mu_{SRm}}=\sum_{i=1}^{M}\frac{\lambda_i p_{im}}{\mu_{im}} \tag{5}$$

采用连续小波尺度分解对网络近邻入侵信号进行经验模态，当入侵信息局部平稳时，得到的网络近邻入侵信号模型的描述为：

$$s(t)=\underbrace{\sum_{k=1}^{N}p_k\sin(\omega_k n+\Phi_k)}_{u(n)}+\zeta(n) \tag{6}$$

其中，Φ_k 为近邻入侵信号的幅度，$\zeta(n)$为两个采样时间点的相位平均，p_k 为尺度参数。通过自适应解卷积融合处理，得到入侵信号的自相关匹配函数为：

$$\begin{aligned}T_{SRm}&=T_{\mathrm{service}}+T_{\mathrm{wait}}\\&=\frac{1}{\sum_{i=1}^{M}\lambda_i p_{im}}\cdot\sum_{i=1}^{M}\frac{\lambda_i p_{im}}{\mu_{im}}+\frac{\sum_{i=1}^{M}(\frac{\lambda_i p_{im}}{\mu_{im}})T_{\mathrm{service}}[1+(\frac{\sigma_{\mathrm{service}}}{T_{\mathrm{service}}})^2]}{2(1-\sum_{i=1}^{M}\frac{\lambda_i p_{im}}{\mu_{im}})}\end{aligned} \tag{7}$$

计算出网络近邻入侵信号的矩形包络，采用多源波束形成方法，得到网络入侵的信号能量总和，记为：

$$T_{\mathrm{total}}=\sum_{i=1}^{M}\lambda_i\cdot\frac{\sum_{m=1}^{SR}P_{im}T_{SR}}{\sum_{m=1}^{SR}\lambda_{SR}} \tag{8}$$

经过上述处理可知，重构的网络入侵信号模型能反映非平稳信号统计量的时间变化[9]，采用短时傅立叶变换进行时频分解可得到网络近邻入侵的非平稳信号模型，为：

$$STFT(t,f)=\int_{-\infty}^{\infty}x(\tau)h^*(\tau-t)\mathrm{e}^{-j2\pi f\tau}\mathrm{d}\tau \tag{9}$$

求得入侵信号的能量密度谱(Spectrogram，SPEC)为：

$$SPEC(t,f)=|STFT(t,f)|^2 \tag{10}$$

通过上述处理，实现了对深度无线传感组合网络的近邻入侵信号模型的构建，结合入侵信号模型在某一频率成分的时间分布，进行深度无线传感组合网络的入侵特征分析与检测。

1.2　无线传感组合网络的入侵特征提取

根据上述构建的网络入侵信号模型，在时间和频率上分析网络入侵信号的能量频谱特征分布密度和攻击信息强度等特征信息，计算网络近邻分布源信息输入点的入侵能量谱的畸变部分，估计结果为：

$$\frac{1}{2\pi m}\sum_{k=-q/2}^{q/2}b_k\phi(n+c_k m)=\hat{f}_{i_q}(n) \tag{11}$$

其中，b_k 为经时间轴平移和伸缩得到的信号幅值，ϕ 为病毒入侵信号的分段截取长度，m 为期望的响应，c_k 为时间分辨率。在较长的信号观测时间下，提取网络近邻攻击的强度为：

$$u(t)=\frac{1}{\sqrt{T}}rect(\frac{t}{T})\exp\{-j[2\pi K\ln(1-\frac{t}{t_0})]\} \tag{12}$$

其中，$rect(t)=1$，$|t|\leqslant 1/2$。利用网络近邻入侵信号的多维相空间的指向不变性，得到网络近邻入侵信号幅频响应特征的非均匀采样输出，为：

$$\hat{f}_{i_q}(t,\tau)=\frac{1}{2\pi\tau}\sum_{k=-q/2}^{q/2}b_k\phi(t+c_k\tau) \tag{13}$$

其中，τ 为采样时延，c_k 为平移不变窗口，ϕ 为采样间隔的相位差，b_k 为核函数。根据入侵信息的 Winger-Ville 分布[10]，将网络近邻入侵数据序列分解成有限个固有模态函数，在时频平面求得入侵能量密度的近似统计平均，根据特征提取结果

得到深度无线传感组合网络近邻入侵的视频分布，描述为：

$$z(t)=x(t)+iy(t)=a(t)e^{i\theta(t)} \tag{14}$$

其中：

$$a(t)=\sqrt{x^2(t)+y^2(t)},\theta(t)=\arctan\frac{y(t)}{x(t)} \tag{15}$$

其中，$a(t)$和$\theta(t)$分别是入侵解析信号的包络和相位，它们都是时间的函数。采用窄带频谱约束方法求得原始入侵信号$x(t)$的局部频率成分，根据特征提取结果进行入侵信号滤波检测。

2 网络近邻入侵检测算法的改进

2.1 自适应卷积滤波

本节进一步对深度无线传感组合网络的近邻入侵检测算法进行改进，提出一种自适应卷积滤波的网络近邻入侵检测算法。构建自适应卷积滤波器进行网络传输信息的盲源滤波和异常特征提取[11]，滤波器的结构如图1所示。

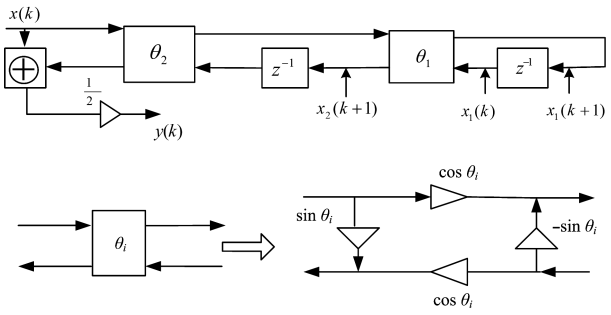


图1 自适应卷积滤波的结构框图

Fig. 1 Block diagram of adaptive convolution filtering

假设输入的网络近邻入侵信号$x(k)$为一组宽平稳的高斯随机序列，它是由网络近邻入侵信号和合法的网络数据组成，将入侵信号输入到如图1所示的自适应卷积滤波器中，用输入$x(k)$减去输出$y(k)$可以得到M组宽带时间序列。假设具有M个近邻入侵源输入的网络的入侵信号为$x(k-1)$，…，$x(k-M)$，通过选择幅度和频率调制，设置合适的$\theta_1(k)$，使得$y(k)y^*(k)$最小，其中，$*$代表复共轭。设定滤波频率为：

$$\omega_0=\arccos(-a/2) \tag{16}$$

其中，$|a|<2$，a为自适应卷积滤波的频率参数。根据入侵检测的幅频响应，得到本文滤波器的相位分布的迭代公式：

$$\theta_1(k+1)=\theta_1(k)-\mu\mathrm{Re}[y(k)\varphi^*(k)] \tag{17}$$

其中，μ是网络近邻入侵检测的带宽参数，称为步长；$\varphi(k)$是幅频响应$|H(j\omega)|^2$的衰减带宽。自适应卷积滤波的系统传递函数为：

$$H_B(z)=\frac{(1+\sin\theta_2)}{\cos\theta_2}\frac{\cos\ _1(k)\cos\theta_2 z^{-1}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2 z^{-2}}G(z) \tag{18}$$

其中：

$$G(z)=\frac{1-\sin\theta_2}{2}\frac{1-z^{-2}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2 z^{-2}} \tag{19}$$

由此计算滤波器的频率参数θ_1和带宽参数θ_2，当输入频率固定时，检测滤波函数输出幅频响应的误差最小。令$d(k)$表示滤波输出的传递误差，得到输出入侵检测信号的预测误差为：

$$\varepsilon(k)=d(k)-y(k)=d(k)-\sum_{i=1}^{M}W_i x(k-i) \tag{20}$$

对式(20)两边取数学期望，实现对深度无线传感组合网络近邻入侵信号的滤波处理[12]，以进行网络传输信息的盲源滤波和异常特征提取。

2.2 参量估计及入侵检测

采用联合时频分析方法进行网络近邻入侵信号的频谱估计，得到自适应滤波的输出信号的尺度平移为：

$$P_d=1-\prod_{i=1}^{N}[(1-P_{di})(1-P_{ei})+P_{di}P_{ei}] \tag{21}$$

根据一定的准则修改滤波参量，并设计检测准则，同时根据输入、输出及原参量值，得到网络近邻入侵信号检测的输出与期望之间的误差为：

$$\gamma_i=\frac{1}{N-1}*\frac{\sum_{i=1}^{N}(SNR_i)-SNR_i}{\sum_{i=1}^{N}SNR_i} \tag{22}$$

其中，SNR_i表示单组入侵成分的信噪比。通过自适应线性组合估计加权后的入侵信息的频谱检测结果为：

$$P_f=\sum_{\sum c_i=1}^{N}\sum_{\gamma_{c_i}\geqslant 1/2}\prod_{i=1}^{N}(P_{f,i})^{c_i}(1-P_{f,i})^{c_i} \tag{23}$$

k次分解后，以均方差值最小为优化目标函数，对自适应卷积滤波检测后的信号进行线性组合[13]，得到输出的网络入侵自相关函数为：

$$y(k)=\sum_{i=1}^{M}W_i x(k-i) \tag{24}$$

令$d(k)$代表所期望的响应，求得网络近邻入侵特征信息的频谱参量估计结果：

$$\tilde{\Sigma}_{e|v,k}=h_{e|v,k}(\tilde{\Sigma}_{ee,k}-\tilde{\Sigma}_{ve,k}^{\mathrm{T}}\tilde{\Sigma}_{vv,k}^{-1}\tilde{\Sigma}_{ve,k}) \tag{25}$$

$$h_{e|v,k}=\frac{1}{(\tilde{v}_k+d_v)}\times[\tilde{v}_k+(v_k-\tilde{u}_{v,k})^{\mathrm{T}}\tilde{\Sigma}_{vv,k}^{-1}(v_k-\tilde{u}_{v,k})] \tag{26}$$

其中，$\tilde{v}_k=v_k-d+1$表示最小均方误差，核函数$h_{e|v,k}(\cdot)$取作多项式核。根据最速下降法，若估计的入侵信号的频率点落在真实信号频率周围，则表示检测到网络入侵信号存在。

3 仿真实验分析

采用Matlab 2010b编程软件设计网络入侵检测的仿真实验，在网络流量交换中心进行深度无线传感组合网络的传输数据的采集和检测，并根据采集的传输数据进行信号拟合和检测分析。采集网络传输数据的时间为2017年6月10日至6月20日。在网络链路层中进行流量采样的时间间隔为12 s；网络传输数据采集的干扰信噪比为$SNR=-10\sim10$ dB；深度无线传感组合网络入侵特征的分布带宽为0～18 kHz；基频频率为50 kHz；调频信号的上变频为100 Hz；下变频为10 Hz，滤波器的带宽参数$\rho=0.96$；干扰信息的谱峰位置位于0.5π处；实验中取陷波频率为$\varepsilon=\pm0.064$。首先，进行网络流量采集，采集到的深度无线传感组合网络传输链路中的数据拟合时域波形如图2所示。

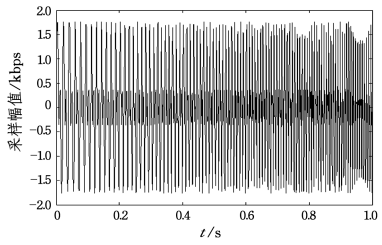
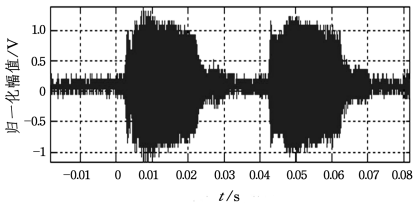


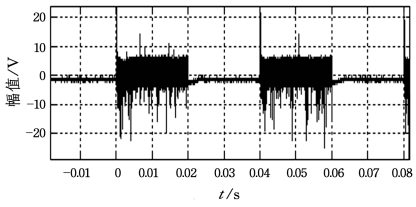
图 2　网络流量采集的时域波形

Fig. 2　Time domain waveform of network traffic acquisition

以图 2 采集的网络链路传输流量数据为研究对象进行网络入侵检测和特征提取，同时对传输数据进行归一化处理。采用本文提出的自适应卷积滤波器进行信号滤波，得到滤波前后的网络传输数据的信号波形，如图 3 所示。



(a)滤波前的原始数据



(b)滤波后的输出数据

图 3　网络传输信息流的自适应卷积滤波处理

Fig. 3　Adaptive convolution filtering for network transmission information flow

由图 3 得知，采用本文方法进行网络传输数据的自适应卷积滤波可有效滤除干扰分量。在此基础上进行入侵检测，提取网络近邻入侵特征信息的频谱参量，结果如图 4 所示。分析得知，利用本文方法进行网络近邻入侵的频谱特征提取，能准确估计出入侵点的频域位置和时域信息，实现准确检测和拦截。

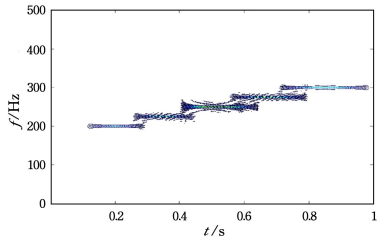


图 4　网络近邻入侵的频谱参量的提取结果

Fig. 4　Spectrum parameters extraction results of network nearest neighbor intrusion

为了对比本文方法的检测性能，将其与传统的 HHT 检测算法、能量管理检测方法进行对比，得到的检测性能曲线如图 5 所示。分析得知，本文方法进行入侵检测的准确率较高，抗干扰能力较强，对未知的网络流量样本序列的入侵特征具有较高的识别能力和泛化能力。

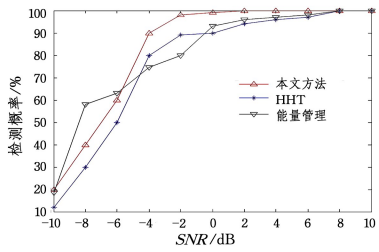


图 5　检测性能对比

Fig. 5　Comparison of detection performance

结束语　为了提高对新出现的攻击类型和网络异常行为的检测识别能力，提出一种自适应卷积滤波的网络近邻入侵检测算法。以深度无线传感组合网络为例进行检测算法的设计，并在传输信道中进行网络流量采集，构建网络入侵信号模型；在时间和频率上分析网络入侵信号的能量密度和攻击强度等特征信息，构建自适应卷积滤波器进行网络传输信息的盲源滤波和异常特征提取；采用联合时频分析方法进行网络近邻入侵特征信息的频谱参量估计，并根据频谱特征的异常分布实现网络近邻入侵检测。实验结果证明，进行网络入侵检测时，本文方法的准确率较高，对未知的网络流量样本序列具有较高的识别能力和泛化能力，抗干扰能力较强，性能较优。

参 考 文 献

[1] LI H，QIAN C J，SUN L Z，et al. Simulation of a flexible polymer tethered to a flat adsorbing surface [J]. Journal of Applied Polymer Science，2012，124(1)：282-287.

[2] ZHAO X J，SUN Z X，YUAN Y. An Efficient Association Rule Mining Algorithm Based on Prejudging and Screening[J]. Journal of Electronics & Information Technology，2016，38(7)：1654-1659.(in Chinese)
赵学健，孙知信，袁源. 基于预判筛选的高效关联规则挖掘算法[J]. 电子与信息学报，2016，38(7)：1654-1659.

[3] WANG S，ZHAO B F. Network Intrusion Detection Based on Fuzzy Data Mining and Genetic Algorithm [J]. Computer Measurement & Control，2012；20(3)：660-663.(in Chinese)
王晟，赵壁芳. 基于模糊数据挖掘和遗传算法的网络入侵检测技术[J]. 计算机测量与控制，2012，20(3)：660-663.

[4] CECI M，MALERBA D. Classifying Web documents in a hierarchy of categories：a comprehensive study[J]. Journal of Intelligent Information System，2007，28(1)：37-78.

[5] ZHANG W M，CHEN Q Z. Network Intrusion Detection Algorithm Based on HHT with Shift Hierarchical Control[J]. Computer Science，2014，41(12)：107-111.(in Chinese)
章武媚，陈庆章. 引入偏移量递阶控制的网络入侵 HHT 检测算法[J]. 计算机科学，2014，41(12)：107-111.

[6] CHEN H，WAN G X，XIAO Z J. Intrusion detection method of deep belief network model based on optimization of data processing[J]. Journal of Computer Applications，2017，37(6)：1636-1643.(in Chinese)
陈虹，万广雪，肖振久. 基于优化数据处理的深度信念网络模型的入侵检测方法[J]. 计算机应用，2017，37(6)：1636-1643.

(下转第 189 页)

两个句子中的词向量进行最大匹配，相似度高于共现阈值 α 的作为这两个短句语义层面的交集，最终计算出句子的相似度。本文在中英文数据集上分别进行了实验，并将该算法与传统的 Jaccard 算法进行了对比，从而证明了该算法的有效性。但是，该算法在中文文本的相似度计算方面的效果仍不尽如人意。如何得到一份高质量的中文词向量，以及如何将词向量与句法、词序等语言学特征结合起来提升中文文本相似度计算的效果，将是我们下一步工作的重点。

参 考 文 献

[1] ACHANANUPARP P, HU X, SHEN X. The Evaluation of Sentence Similarity Measures[C]// International Conference on Data Warehousing and Knowledge Discovery. 2008: 305-316.

[2] METZLER D, DUMAIS S, MEEK C. Similarity Measures for Short Segments of Text[C]// Advances in Information Retrieval, European Conference on Ir Research (ECIR 2007). Rome, Italy, 2007: 16-27.

[3] LI Y, MCLEAN D, BANDAR Z A, et al. Sentence Similarity Based on Semantic Nets and Corpus Statistics[J]. IEEE Transactions on Knowledge & Data Engineering, 2006, 18(8): 1138-1150.

[4] AGIRRE E, ALFONSECA E, LACALLE O L D. Approximating hierarchy-based similarity for WordNet nominal synsets using topic signatures[C]// Proceedings of Gwc. 2004.

[5] ZHANG H J, WANG G S, ZHONG Y X. Text Similarity Computing Based on Hamming Distance[J]. Computer Engineering and Applications, 2001, 37(19): 21-22. (in Chinese)
张焕炯，王国胜，钟义信. 基于汉明距离的文本相似度计算[J]. 计算机工程与应用，2001，37(19)：21-22.

[6] GUO Q L, LI Y M, TANG Q. Similarity computing of documents based on VSM[J]. Application Research of Computers, 2008, 25(11): 3256-3258. (in Chinese)
郭庆琳，李艳梅，唐琦. 基于 VSM 的文本相似度计算的研究[J]. 计算机应用研究，2008，25(11)：3256-3258.

[7] LIAO K J, YANG B B. Similarity Computing of Documents Based on Weighted Semantic Network[J]. Journal of Intelligence, 2012, 31(7): 182-186. (in Chinese)
廖开际，杨彬彬. 基于加权语义网的文本相似度计算的研究[J]. 情报杂志，2012，31(7)：182-186.

[8] LIAO Z F, QIU L X, XIE Y S, et al. A Frequency Enhanced Algorithm of Sentence Semantic Similarity[J]. Journal of Hunan University (Natural Sciences), 2013, 40(2): 82-88. (in Chinese)
廖志芳，邱丽霞，谢岳山，等. 一种频率增强的语句语义相似度计算[J]. 湖南大学学报(自然科学版)，2013，40(2)：82-88.

[9] LIAO Z F, ZHOU G E, LI J F, et al. A Chinese Short Text Similarity Algorithm Based on Semantic and Syntax[J]. Journal of Hunan University (Natural Sciences), 2016, 43(2): 135-140. (in Chinese)
廖志芳，周国恩，李俊锋，等. 中文短文本语法语义相似度算法[J]. 湖南大学学报(自然科学版)，2016，43(2)：135-140.

[10] BENGIO Y, SCHWENK H, SENÈCAL J S, et al. A neural probabilistic language model[J]. Journal of Machine Learning Research, 2003, 3(6): 1137-1155.

[11] COLLOBERT R, WESTON J, BOTTOU L, et al. Natural Language Processing (almost) from Scratch[J]. Journal of Machine Learning Research, 2011, 12(1): 2493-2537.

[12] MIKOLOV T, SUTSKEVER I, CHEN K, et al. Distributed Representations of Words and Phrases and their Compositionality[J]. Advances in Neural Information Processing Systems, 2013, 26: 3111-3119.

[13] HUANG E H, SOCHER R, MANNING C D, et al. Improving word representations via global context and multiple word prototypes[C]// Meeting of the Association for Computational Linguistics: Long Papers. 2012: 873-882.

[14] NG J P, ABRECHT V. Better Summarization Evaluation with Word Embeddings for ROUGE[C]// Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing. 2015.

[15] KUSNER M J, SUN Y, KOLKIN N I, et al. From Word Embeddings to Document Distances[C]// International Conference on Mechine Learning. 2015: 957-966.

(上接第 157 页)

[7] LI F, WU C M. Research on Prevention Fluctuation Control method of Network Intrusion Based on Energy Management [J]. Computer Simulation, 2013, 30(12): 45-48. (in Chinese)
黎峰，吴春明. 基于能量管理的网络入侵防波动控制方法研究[J]. 计算机仿真，2013，30(12)：45-48.

[8] DENG Z H, CAO L B, JIANG Y Z, et al. Minimax probability TSK fuzzy system classifier: A more transparent and highly interpretable classification model[J]. IEEE Transactions on Fuzzy Systems, 2015, 23(4): 813-826.

[9] HESS R A. Aircraft and rotorcraft system identification-engineering methods with flight test examples[J]. Journal of Guidance, Control, and Dynamics, 2013, 36(4): 1249-1250.

[10] ZHANG H B, HE Q B, KONG F R. Stochastic resonance in an underdamped system with pinning potential for weak signal detection[J]. Sensors, 2015, 15(9): 21169-21195.

[11] WANG H X, WANG S Y, WANG X, et al. Analysis of LFM signals and improvement of IFM system[J]. Acta Armamentarii, 2014, 35(8): 1193-1199. (in Chinese)
王洪迅，王士岩，王星，等. 瞬时测频系统的线性调频信号分析及改进[J]. 兵工学报，2014，35(8)：1193-1199.

[12] MAHBOUBI H, MOEZZI K, AGHDAM A G, et al. Distributed deployment algorithms for improved coverage in a network of wireless mobile sensors[J]. IEEE Transactions on Industrial Informatics, 2014, 10(1): 163-174.

[13] MAHBOUBI H. Distributed deployment algorithms for efficient coverage in a network of mobile sensors with nonidentical sensing Capabilities[J]. IEEE Transactions on Vehicular Technology, 2014, 63(8): 3998-4016.

[14] DAI W. Application of Intrusion Detection Technology in Network Security[J]. Journal of Chongqing University of Technology (Natural Science), 2018, 32(4): 156-160, 185. (in Chinese)
代威. 入侵检测技术在网络安全中的应用[J]. 重庆理工大学学报(自然科学)，2018，32(4)：156-160，185.