文章编号:1006-9348(2020)08-0239-04

基于机器学习算法的网络信息可信性感知仿真

王 燕[1],刘琳芳[2],黄大志[3]

(1. 贵州警察学院侦查系,贵州 贵阳 550005;
2. 贵州大学数学与统计学院,贵州 贵阳 550005;
3. 贵州省公安厅禁毒总队,贵州 贵阳 550001)

摘要: 针对传统感知网络信息可信性的方法存在感知结果与事实不一致、影响网络运行速度等问题,提出一种基于机器学习算法的网络信息可信性感知。对网络信息可信性影响要素进行分析,将其主要分为三种影响因素,建立机器学习算法的基础相关向量机模型。通过贝叶斯理论等,将机器学习算法向量机模型进行推导,采用狄拉克函数进行相对应的近似计算,降低信息数据传输,提升核函数选择范围。将网络信息可信性感知评价标准分为主观和客观两部分,主观为信息内容质量感知,客观为网络稳定性感知,以此实现网络信息可信性感知的评价。仿真结果表明:所提感知方法能够快速评判目标信息可信程度,在网络不稳定时能够精准感知,且网络运行速度较快。

关键词: 机器学习算法; 相关向量机; 网络信息; 信息可信性

中图分类号: TP393 **文献标识码:** B

Simulation of Network Information Trustworthiness Based on Machine Learning Algorithm

WANG Yan[1], LIU Lin-fang[2], HUANG Da-zhi[3]

(1. Investigation Department, Guizhou Police College, Guiyang Guizhou 550005, China;
2. School of Mathematics and Statistics, Guizhou University, Guizhou Guiyang 550005, China;
3. Guizhou Public Security Bureau Anti-Drug General Team, Guizhou Guiyang 550001, China)

ABSTRACT: Traditionally, the perceived result is inconsistent with the fact, affecting the running speed of network. Therefore, a method of network information credibility perception based on machine learning algorithm was proposed. The influencing factors of network information credibility were analyzed, and then they were divided into three main influencing factors, and the basic relevant vector machine model of machine learning algorithm was built. Based on Bayesian theory, the vector machine model of machine learning algorithm was inferred. The approximate calculation was carried out by Dirac delta function, so that the information data transmission was reduced and the kernel function selection range was expanded. The evaluation standard of network information credibility was divided into two parts: subjective and objective. The subjective perception was to sense the information content quality, and the objective perception was to sense the network stability. Thus, the evaluation for credibility perception of network information was achieved. Simulation results show that the proposed method can quickly judge the reliability of target information and sense the target information accurately when the network is not stable. In addition, the network operation speed is fast.

KEYWORDS: Machine learning algorithms; Relevant vector machine; Network information; Information reliability

基金项目: 贵州省科技厅科技支撑项目(黔科合支撑[2019]2885)

收稿日期: 2019-12-26 **修回日期:** 2020-01-04

1 引言

网络信息可信性的观念和涉及内容不断发展，促使网络可信性需要不断被完善和标准化，研究其感知方法与结构，以及对网络可信性的影响条件进行分析尤为重要[1]。维持网络整体运行安全的基础是确保信息的可信性。在网络运行过程中，其表现为是否为用户提供需求信息以及信息的准确率[2]。网络可信性与网络硬件、软件的可靠性存在直接关系。在规定的单位时间、整体环境下，根据条件能够完成相对应规定的指令要求，其概率度量[3]成为衡量网络信息可信度的标准。关于网络整体可信性研究受到了该领域人士的普遍关注。

文献[4]针对现有网络信息可信性感知建模困难问题，提出一种感知可信性的 Petri 网络。该方法根据已知概念和可信性感知建模规律，提出一种智能学习算法，以此构建感知系统模型，且在此基础上分析出信息定量值，进一步验证算法的有效性。Petri 网络可信性感知法可在根本上加快感知运算速度，以达到提升网络运行的效果，但随着计算次数的增加，易在感知过程中出现待测数据失误问题。文献[5]根据对网络可信性和信息流综合感知，提出保护输出网络的可信性感知方法，同时能够确定网络整体环境的安全性及可信性。该方法基于网络数据保护系统框架构建网络故障模型，假设在网络故障环境下对向量进行测量和感知其可信性。该方法可以快速完成目标信息可信性判定以及收集网络运行数据，但对向量数据的信息流稳定性考虑甚少，导致感知的结果精准度不高。

基于上述问题的存在，本文提出一种基于机器学习算法的网络信息可信性感知。机器学习算法是计算机、概率统计等多个学科的完美融合结果，能够精准模拟现实环境，智能获取数据和学习知识。通过机器学习算法相关向量机对网络信息可信性进行感知，可有效提升感知准确率，使用户拥有极佳的使用体验。

2 基于机器学习算法的相关向量机模型构建

2.1 网络信息可信性影响要素分析

在进行相关向量机模型构建之前，需要分析影响网络信息可信性的影响要素。主要包括以下三点要素:

1) 规定单位时间

由于信息网络可信性只能体现在其网络运行的时间段内，所以本文将运行时间作为规定内单位时间度量。考虑到网络的基本运行环境以及遭受恶意攻击的随机性，所以将网络失效描述为随机事件，因此网络正常运行下信息的可信性时间也属于随机变量。

2) 规定条件

规定条件是指网络的基本运行环境，其中涵盖各种不同支持条件，例如: 运行执行系统、受到攻击时的防护措施以及数据格式等。在不同环境情况下，信息网络的可信性也是不同的。

3) 规定功能

网络信息可信性与规定的运行任务存在不可脱离的关系，由于网络需要根据不同的接收指令完成相对应的任务，有时便会造成运行不一致的后果，进而导致网络运行的子模块不同，信息的可信性就会因此原因而不同。

2.2 基础向量机

为了实现基于机器学习算法的网络信息可信性感知，需要建立机器学习算法的基础相关向量机模型[6]。

假设样本训练集为 $\{x_n,t_n\}_{n-1}^{N}$，其中所定目标值 t_n 独立分布，输入值 x_n 是一个独立的分布样本。则有

$$t_n = y(x_n,w) + \xi_n \tag{1}$$

式中，t_n 表示输入值 x 与目标 t 之间的关系，ξ_n 表示附加噪声，且噪声符合于下列 *Gamma* 的分布

$$\xi_n \sim N(0,\sigma^2) \tag{2}$$

其中，预期望值为 0，方差为 σ^2。假设 σ^2 在模型中表示未知量，由(1)和(2)式可得

$$P(t_n \mid w,\sigma^2) = N(\Phi\omega,\sigma^2) \tag{3}$$

式中，Φ 为 $N\times(N+1)$ 根据核函数构建成的结构型矩阵，即: $\Phi=[\Phi(x_1),\Phi(x_2),\cdots,\Phi(x_n)]^T$。

在评价 ω 和 σ^2 最大似然估计值时，对 *ARD* 概括了概率分布为

$$P(W\mid\alpha) = \prod_{i=0}^{N}(\omega_i\mid 0,\alpha_i^{-1}) \tag{4}$$

式中，$\alpha=(\alpha_0,\alpha_1,\cdots,\alpha_N)$ 是根据超参数所产生的向量集，假设超参数 α 和方差 σ^2 服从于 *Gamma* 概率分布，那么则有

$$P(\alpha_i) = Gamma(a,b) \tag{5}$$

$$P(\sigma^2) = Gamma(c,d) \tag{6}$$

式中，参数 a、c 是 *Gamma* 分布的基本形状参数，b、d 是 *Gamma* 分布尺度参数。为了达到无信息先验假设，取值为 10^{-4}。

2.3 机器学习算法向量机模型推导

根据基础向量机知识以及贝叶斯理论[7]可以得出下列关系式

$$P(\omega,a,\sigma^2\mid t) = \frac{P(t\mid\omega,a,\sigma^2)P(\omega,a,\sigma^2)}{P(t)} \tag{7}$$

$$P(t) = \int P(t\mid\omega,a,\sigma^2)P(\omega,a,\sigma^2)\,d\omega da d\sigma^2 \tag{8}$$

其中，式(9)后验概率分布可以分解成

$$P(\omega,a,\sigma^2\mid t) = P(\omega\mid t,a,\sigma^2)P(a,\sigma^2\mid t) \tag{9}$$

其中，ω 的后验概率又可以分解成

$$P(\omega\mid t,a,\sigma^2) = \frac{P(t\mid\omega,a,\sigma^2)P(\omega\mid a)}{P(t\mid a,\sigma^2)} = N(\mu,\sum) \tag{10}$$

$$\sum = (\sigma^2\Phi\Phi+A)^{-1} \tag{11}$$

$$\mu = \sigma^2\sum\Phi_t^T \tag{12}$$

式中，矩阵 $A=diag(a_0,a_1,\cdots,a_N)$。

由于后验证概率 $p(a,\sigma^2\mid t)$ 并不能经过分解计算的方式得到，所以可以采用狄拉克函数[8]来做相对应的近似计算。它的表达式为

$$p(a,\sigma^2 \mid t) \approx \varsigma(a_{MP},\sigma^2_{MP}) \tag{13}$$

其中 a_{MP} 和 σ^2_{MP} 将是后验证概率 $p(a,\sigma^2 \mid t)$ 的最优解，即

$$a_{MP} = \arg \max p(a \mid t) \tag{14}$$

$$\sigma^2_{MP} = \arg \max p(\sigma^2 \mid t) \tag{15}$$

其中，式(14)(15)的求解，将经过式(10)和(11)转换得到下列公式

$$p(a,\sigma^2 \mid t) \propto p(t \mid a,\sigma^2)\, P(a)\, P(\sigma^2) \tag{16}$$

后验证概率 $p(a,\sigma^2 \mid t)$ 的最大最小估计能够转换为式(17)右侧的最大最小估计，根据式(11)可得

$$p(t \mid a,\sigma^2) = N(0,C) \tag{17}$$

其中，$C = \sigma^2 I + \Phi A^{-1} \Phi^T$。

针对式(16)中 $p(t \mid a,\sigma^2)\, P(a)\, P(\sigma^2)$ 进行最大似然估计，即可得到估计结果，即边缘似然估计为

$$L = \log(P(t \mid \log^{a} \log^{\sigma^2} \mid)) + \sum_{i=0}^{N} \log P(\log^{a_i}) + \log P(\log^{\sigma^2}) \tag{18}$$

通过 $C = \sigma^2 I + \Phi A^{-1} \Phi^T$ 和 $t^T C_t^{-1} = \sigma^2 t^T (t - \Phi\mu)$ 可求出

$$\log \mid C \mid = -\log \left| \sum \right| - N\log^{\sigma^2} - \log \mid A \mid \tag{19}$$

将式(19)带入(18)将得到下列结果

$$L = \frac{1}{2}\left[\log \left| \sum \right| + \log \mid A \mid - \sigma^2 t^T (t - \Phi\mu)\right] + \sum_{i=0}^{N} (a\log^{a_i} - b^{a_i}) + N\log^{\sigma^2} + c\log^{\sigma^2} - d_{\sigma^2} \tag{20}$$

求式(20)偏导可得

$$\frac{\partial L}{\partial \log a_i} = -\frac{1}{2}(-a_i \sum\nolimits_{ii} + 1 + a_i \mu_i^2 + 2a - 2b^{a_i}) \tag{21}$$

表示式(10)中矩阵所对应的第 i 行平均权重数据值，表达了后验证权重数据中对应的协方差矩阵中的第 i 个对角元素。假设式(21)结果为零，则有

$$a_i^{new} = \frac{1 + 2a}{\mu_i^2 + \sum\nolimits_{ii} + 2b} \tag{22}$$

假设 $r_i = 1 - a_i \sum_{ii}$，那么(22)可变换为

$$a_i^{new} = \frac{r_i + 2a}{u_i^2 + 2b} \tag{23}$$

$$(\sigma^2)^{new} = \frac{\| t - \Phi\mu \|^2 + 2d}{N - \sum_{i=0}^{N} r_i + 2c} \tag{24}$$

在实际应用中，可以通过式(23)和(24)更新超出参数值 a_i 和 σ^2，以便实现关于向量的学习。a_i 的取值在无穷大的边缘徘徊，通过式(10)可获取到 ω 趋于零的结果。这时较少的样本点具有基本作用，这些样本点统称为机器学习相关向量机。

3 网络信息可信性感知

网络信息可信性是评价信息质量的主要因素之一，其中部分研究学者认为消息来源的可信性，是指接收者对信息质量以及可信性的客观认知。把信息质量概括为其中某一个用户的认知标准，在一定程度上信息具有真实性特[9]。在网络信息可信性感知上，信息质量通常会被标识为“认为信息是准确的、及时的、有用的”，是感知信息可信度的主要因素。

当网络信息可信性与信息质量分开判定时，其中可信性的概念与可靠性相似。可信性是一个多元化的理论，被定义为诚信、可信的、准确等。综上所述，网络信息可信性感知可分为两部分，主观标准为信息内容质量，客观为网络稳定性评级。信息可信性主观评价标准内容如表 1 所示。

表 1 信息可信性主观评价标准

标准(积极/消极)	定义
是否可以识别	信息对作者的识别度
信息作者声誉	对作者的评价
专业/不专业	在该领域能力
公正/不公正	是否公正考虑问题
守信/不守信	提供消息可信度
合理性/不合理性	表达个人观点方式
表达能力(积极/消极)	是否可以清楚表达问题
相似性/不相似性	个人观点与他人相似性

网络信息可信性的客观评价标准是指在安全可靠硬件、软件支持下，信息数据正常接收和传输。但多数情况下会遇到数据中断、篡改、伪造等问题的影响，导致信息可信性降低。

1) 网络失效：网络失效是指在网络正常运行中，并不能按照规定来实现网络指定功能，进而导致网络运行被迫中断的情况出现。

2) 网络信息丢失率[10]：每个网络单元在规定的单位时间内，一直到 r 时仍可以正常运行，在 r 之后每个单位规定时间内可能发生失效的可能性。

3) 网络可靠度：网络在规定的工作条件框架下，与单位规定时间内所完成的规定功能概率，将这个概率描述为 $Q(r)$。针对其概率，系统可靠性分析来看，即可导出下列关于 $\lambda(r)\, Q(r)$ 的关系式为

$$Q(r) = e_0^{\int^t \lambda(r)\, dt} \tag{25}$$

失效率 $\lambda(r)$ 可以经过对某一网络在 $(r,\Delta r)$ 的规定时间内失效的概率为 $P(r < R \leqslant r + \Delta r > r)$，在 Δr 规定的时间内，网络平均失效率为

$$\lambda(r) = \frac{P(r < R \leqslant r + \Delta r \mid R > r)}{\Delta r} \tag{26}$$

根据式(26)可以得到整体网络正常运行工作时间间 $MTBF$(指网络系统在接近的两次故障之间的平均工作时间)为

$$MTBF = \int_0^{\infty} e_0^{\int^t \lambda(r)\, dt} dt \tag{27}$$

为了能够更好的表述网络受到软攻击时的状态，运用网络信息丢失率表示网络的整体受损程度。根据 $MTBF$ 的变化来衡量被攻击产生的破话等级。

假设在未找到攻击来源的情况下，受攻击损坏的网络失效率为 $\lambda_h(r)$，网络正常运行的平均时间为 $MTBF_k$，则攻击源对网络所产网络信息丢失率为

$$\lambda_w = \frac{MTBF - MTBF_h}{MTBF} \tag{28}$$

当 $\lambda(r) = \lambda$、$\lambda_h(r) = \lambda_h$ 时，则有

$$\lambda_w = 1 - \lambda/\lambda_h \tag{29}$$

根据上述定义可知，网络信息丢失率 λ_w 是在[0,1]区间上的一个常规数值。

在网络正常运行的过程中，$\lambda_h(r) = \lambda(r)$；网络信息非正常运行时，根据 $\lambda_h(r) > \lambda(r)$ 可知：$0 < \lambda_w < 1$。根据网络受到攻击的程度来看，受到攻击程度越严重 λ_w 阈值就越接近于1，信息的可信度越低。

4 仿真分析

4.1 仿真环境

为了验证本文所提方法的有效性进行了仿真分析。实验采用的系统为 Intel(R) i5 - 2400，CPU 为 3.10 GHz，系统内存为 64GB，采用 VisualStudio2010 进行数据的编程。

4.2 实验参数

仿真算法参数值设置如下：学习速率为 $\gamma = 0.7$，模型集最大值为 $L = 30$，实际上融合预测的模型数量 $\Delta = 10$，正常运行时间间隔为 5 s，其中模型的预计使用时间衰减参数值 $\theta = 0.9$，初始权值决定参数值 $\tau = 0.7$。

实验通过对比本文方法、文献[4]方法和文献[5]方法在 τ 取值不同情况下可信性曲线的变化，感知时间开销以及感知信息的准确率为实验指标。

4.3 实验结果分析

4.3.1 可信性曲线变化分析

为了验证本文方法的有效性，实验对比了在 τ 取值不同情况，不同方法可信性曲线变化。实验结果如图2所示。

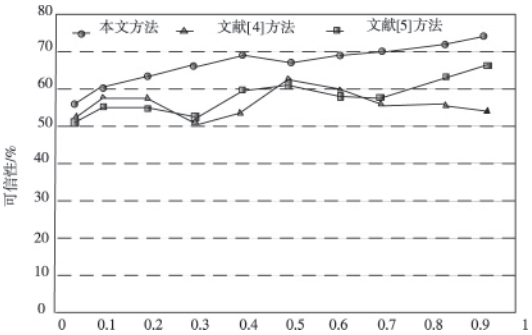

图1 τ 取值不同时可信性曲线

分析图1可知，随着初始权值决定参数值 τ 的变化，不同方法的可信性也随之改变。当 τ 取值为 0.5 时，本文方法的可信性约为 69 %，文献[4]方法的可信性约为 62 %，文献[5]方法的可信性约为 60 %，当 τ 取值为 0.7 时，本文方法的可信性约为 70 %，文献[4]方法的可信性约为 57 %，文献[5]方法的可信性约为 58 %。可以看出采用本文方法进行可信性感知的效果更好。

4.3.2 感知时间开销分析

为了验证本文方法在网络信息可信性感知中的优势，实验对比了三种方法感知时间开销。实验结果如表2所示。

表2 不同方法感知时间开销(s)

可信性信息量/条	本文方法	文献[4]方法	文献[5]方法
100	4.5	6.1	6.4
200	4.8	6.9	7.2
300	5.0	7.3	7.8
400	5.2	7.9	8.1
500	5.4	8.1	8.3

分析表2中的数据可以看出，随着感知的可信性信息量的不断增加，感知时间也随之变化。当可信性信息量为 200 条时，本文方法感知时间为 4.8 s，文献[4]方法用时为 6.9 s，文献[5]方法的用时为 7.2 s；当可信性信息量为 400 条时，本文方法感知时间为 5.2 s，文献[4]方法用时为 7.9 s，文献[5]方法的用时为 8.1 s。可以看出本文方法的时间开销均在 6 s 以下，而其它两种方法的时间开销高于本文方法的时间开销。验证了本文方法的实用性。

4.3.3 感知信息的准确率

为了进一步验证本文方法的有效性，实验对比了三种方法感知信息的准确率。实验结果如图3所示。

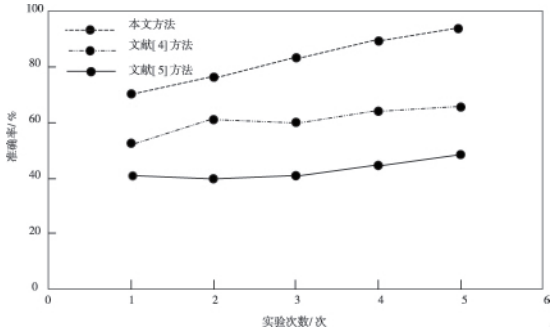

图2 不同方法下感知信息准确率对比

通过分析图2可知，实验次数的改变，感知信息的准确率也在不断改变。当实验次数为 2 时，本文方法的准确率约为 79 %，文献[4]方法的准确率约为 61 %，文献[5]方法的准确率约为 40 %；当实验次数为 5 时，本文方法的准确率约为 93 %，文献[4]方法的准确率约为 63 %，文献[5]方法的准确率约为 48 %；本文方法感知信息的准确率高于其它两种方法的准确率，证明本文方法具有一定可行性。

5 结论

本文通过基于机器学习的相关向量机，(下转第 445 页)

运用本文的预测模型，基于现有的许可证申请历史数据，可以预知未来一段时间内可能出现的许可证申请高发状况，一方面可以辅助监管部门提前准备应急方案，在业务高发期前进行业务培训，以提高行政监管效率；另一方面可以辅助监管部门监控风险，许可证申请业务短时间内激增往往带来相关风险，监管部门可以有针对性地加强检查或控制许可证批准数量，从而可以有效控制业务风险。

综上，本文提出的预测模型可信度高、实用性强，推动了我国辐射安全许可证监管现代化进程，促进我国核能及核技术利用事业的健康发展。

参考文献：

[1] 李干杰. 科学谋划协调推进全面实现核与辐射安全监管现代化[J]. 环境保护，2015，43(7).

[2] Executive Office of the President. Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights[DB]. (2016-05-04)[2016-10-09]. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[3] 尹诗画，董春. 辽宁省教育与产业结构的时空灰色关联分析[J]. 测绘与空间地理信息，2018，(5).

[4] 杨金宝，梁勇，曹现宪. 一种基于灰色理论-隐马尔科夫模型的装备故障预测方法[J]. 舰船电子工程，2018，38(8) 128-145.

[5] P Rothenbuehler, J Runge, F Garcin, et al. Hidden Markov models for churn prediction[C]. Sai Intelligent Systems Conference. IEEE, 2015.

[6] J Shin, M Sunwoo. Vehicle Speed Prediction Using a Markov Chain With Speed Constraints[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 99: 1-11.

[7] 环境保护部. 环境保护部关于修改《放射性同位素与射线装置安全许可管理办法》的决定[J]. 司法业务文选，2009，(6)：3-15.

[8] 牛佳伟. 复杂机械产品装配设备运行状态预测及评估方法研究[D]. 合肥工业大学，2016.

[9] 崔琼，舒杰，吴志锋，等. 基于GLRM模型和MC误差修正的中长期负荷预测[J]. 新能源进展，2017，5(6)：472-477.

[作者简介]

于浩洋(1993-)，男(汉族)，山东省烟台市人，硕士研究生，主要研究领域为智慧物流和人工智能。

曾　瑞(1985-)，男(汉族)，北京市海淀区人，学士，核与辐射安全中心职员，主要研究领域为信息化(通讯作者)。

左　敏(1973-)，男(汉族)，北京市海淀区人，教授，硕士研究生导师，主要研究领域为智能管理和人工智能。

张青川(1982-)，男(汉族)，北京市海淀区人，博士研究生，副教授，主要研究领域为智能软件、分布式计算和人工智能。

(上接第242页)

在一定程度上表明向量的随机不确定性和相关性。将感知评价指标分为主观和客观两部分，对主观感知信息能否识别、合理性、表达能力、相似性，以及客观评判网络失效、网络可靠度、信息丢失率对网络可信性进行感知。仿真结果表明：所提方法感知性能优越，并且不会影响网络正常运行。虽然本文在现阶段取得了一定成果，但还存在很多不足，未来对网络信息可信性的研究将从以下两点出发：

1) 机器学习相关向量机可有效保护待感知信息的隐私安全，可随各类学习算法发展，网络数据安全威胁大幅度增加，如何加大感知模型隐私保护成为一个重要课题。

2) 机器学习相关向量机算法，在本质上虽可以有效减少威胁和漏洞的出现，但运算过程比较复杂，未达到理想感知速度，下一步将对融合神经网络算法智能程度进行研究。

参考文献：

[1] 李冬灵. 构建顶级网络安全的可行性讨论[J]. 商丘职业技术学院学报，2017，16(4)：97-99.

[2] 龚俭，臧小东，苏琪，等. 网络安全态势感知综述[J]. 软件学报，2017，28(4)：1010-1026.

[3] 张俐，袁玉宇，王枞. 基于最大相关信息系数的FCBF特征选择算法[J]. 北京邮电大学学报，2018，41(4)：86-90.

[4] 顾鸿儒. 基于高级PETRI网的网络控制系统综合分析[D]. 天津工业大学，2017.

[5] 赵海文，齐恒佳，王旭之，等. 基于机器学习的人机协调操作意图感知与控制方法研究[J]. 机床与液压，2019，47(10)：147-150.

[6] 唐锟，施荣华. 基于信号蝴蝶效应提取的无线传感网络失效区域检测[J]. 吉林大学学报(工)，2017，47(6)：1939-1948.

[7] 冯鹏飞，朱永生，王培功，等. 基于相关向量机模型的设备运行可靠性预测[J]. 振动与冲击，2017，36(12)：146-149.

[8] 周正，叶爱中，马凤，等. 基于贝叶斯理论的水文多模型预报[J]. 南水北调与水利科技，2017，15(1)：43-48.

[9] 李华惠，邵志强. 用分离的Delta函数法研究非对称Keyfitz-Kranzer系统中Delta激波的交互性[J]. 数学物理学报，2017，37(4)：714-729.

[10] 曹明，遇炳杰，刘咸通，等. 网络数据传输高密度信息安全存储仿真[J]. 计算机仿真，2017，34(12)：153-156.

[作者简介]

王　燕(1979-)，女(汉族)，贵州贵阳人，硕士，副教授，研究方向：公安大数据应用、人工智能。

刘琳芳(1980-)，女(汉族)，河南焦作人，硕士，实验师，研究方向：计算机科学与数据库理论。

黄大志(1975-)，男(汉族)，贵州黔西南州人，工程师，研究方向：公安大数据应用、人工智能。