文章编号: 1006-9348( 2019) 07-0449-05

# 智能通讯网络敏感信息连接可靠性监测仿真

倪铉珣

( 成都信息工程大学银杏酒店管理学院,四川 成都 643000)

摘要: 采用当前方法监测智能通讯网络中敏感信息的连接可靠性时,监测时间较长,得到的监测结果与实际不符,存在监测效率低和监测结果准确率低的问题。为了解决上述问题,提出一种智能通讯网络敏感信息连接可靠性监测方法,综合考虑信息在智能通讯网络中的结构信息和语义信息,计算信息在智能通讯网络中的敏感度,根据计算得到的信息敏感度检测智能通讯网络中存在的敏感信息。将风险矩阵法引入智能通讯网络敏感信息连接可靠性的监测中,结合层次分析法、Borda 排序法和专家二维矩阵构建敏感信息连接可靠性评估模型,利用评估模型检测得到的敏感信息连接可靠性,根据评估结果完成对智能通讯网络敏感信息连接可靠性的监测。仿真实验结果表明,所提方法的监测效率高、监测结果准确率高。

关键词: 智能通讯网络; 敏感信息; 可靠性监测

中图分类号: TP309 文献标识码: B

# Intelligent Communication Network Sensitive Information Connection Reliability Monitoring Simulation

NI Xuan-xun

( Yinxing Hospitality Management College of CUIT, Sichuan Chengdu 643000, China)

**ABSTRACT:** Currently, the monitoring time is long and the monitoring result is inconsistent with the actual situation. Therefore, a method to monitor the connection reliability for sensitive information in intelligent communication network was proposed. After considering the structural information and semantic information in the intelligent communication network, the sensitive degree of information in intelligent communication network was calculated. Based on the sensitive degree, the sensitive information in intelligent communication network was detected. Moreover, the risk matrix method was introduced into the monitoring of connection reliability of sensitive information in intelligent communication network. Based on analytic hierarchy process, Borda ranking method and expert two-dimensional matrix, the reliability evaluation model of sensitive information connection was built. Finally, the evaluation model was used to detect the connection reliability of sensitive information. According to the evaluation result, we completed the monitoring of connection reliability of sensitive information in intelligent communication network. Simulation results show that the proposed method has high monitoring efficiency and high monitoring accuracy.

**KEYWORDS:** Intelligent communication network; Sensitive information; Reliability monitoring

## 1 引言

智能通讯网络为人们带来信息的同时也存在一些安全隐患[1]。在智能通讯网络中存在迷信、色情、反动和暴力等敏感信息、不良信息、非法信息,这些信息会对人们造成极大的负面影响,也会成为危害社会和谐的因素,所以对智能通讯网络中敏感信息的连接可靠性进行监测的意义较大[2]。敏感词具体指的是不文明、政治倾向、暴力倾向和反执政党倾向的词汇。不同的网站会根据网站的基本情况设定符合本网站的敏感信息。通常情况下敏感信息多存于文本中,需要加大网络文本中敏感信息连接可靠性的监测力度[3]。敏感信息连接可靠性监测方法被广泛的应用到垃圾邮件过滤,敏感信息识别、过滤和定位等领域中。当前网络敏感信息连接可靠性监测方法存在监测效率低和监测结果准确率低的问题,需要分析并研究网络敏感信息连接可靠性监测方法。

薛朋强、努尔布力等人提出基于文本信息的网络敏感信息连接可靠性监测方法,该方法改进了 DFA 过滤算法,构建敏感信息决策树,对智能通讯网络中存在的信息进行过滤,实时更新敏感信息语料库,实现网络敏感信息可靠性连接的实时监测,该方法监测敏感信息连接可靠性时所用的时间较

基金项目: 四川省电子商务与现代物流研究中心项目( DSWL18-8)

收稿日期: 2018-11-22

长，导致监测效率低[4]。杨洁、李松斌、邓浩江提出基于贝叶斯网络的敏感信息连接可靠性监测方法，该方法在矢量量化码字的基础上建立时空转移网络，利用码字转移指数简化智能通讯网络中存在的敏感信息，根据 SS-CSTN 建立贝叶斯网络，将 Dirichlet 分布作为网络参数，实现网络敏感信息连接可靠性的监测，该方法得到的监测结果与实际结果之间的误差较大，导致监测结果准确率低[5]。李扬、潘泉、杨涛提出基于短文本情感分析的网络敏感信息连接可靠性监测方法，该方法通过监督学习的方法度量网络中文本信息的情感极性，将网络文本分为正负两类，定义反动、色情、邪教、违禁和暴力等敏感关键词，构建敏感信息连接可靠性监测模型，完成智能通讯网络中敏感信息连接可靠性的监测，该方法过于复杂，监测所用的时间较长，导致监测效率低[6]。

综上所述，提出智能通讯网络敏感信息连接可靠性监测方法。

## 2 基于结构和语义的敏感信息检测

智能通讯网络的普及，增加了智能通讯网络中的信息量，数据维数也在发生变化，敏感信息存在一定的结构[7]。为了提高敏感信息连接可靠性监测结果的准确率，智能通讯网络敏感信息连接可靠性监测方法结合结构信息和语义信息检测智能通讯网络中存在的敏感信息，缩短监测敏感信息连接可靠性的时间。

### 2.1 敏感信息间距离

智能通讯网络敏感信息连接可靠性监测方法结合结构信息和语义信息检测智能通讯网络中存在的敏感信息，需要考虑网络文本信息和敏感信息的结构信息，智能通讯网络敏感信息连接可靠性监测方法通过敏感词间距离描述敏感信息在通讯网络中的位置。

设 $T(t_1,t_2)$ 代表的是敏感词间距离，其计算公式如下：

$$T(t_1,t_2)=\begin{cases}1, p_{t_1}=p_{t_2}\\ |lev(p_{t_1})-lev(p_{t_2})|, p_{t_1}//p_{t_2}\\ or\quad p_{t_2}//p_{t_1}\\ |lev[p_{t_1}-lev(p_{t_2})]|+|lev[lev(p_{t_2})\\ \qquad -lev(p_t)]|, p^i_{t_1}=p^j_{t_1}\end{cases} \tag{1}$$

式中，$T(t_1,t_2)$ 代表的是敏感词 $t_1$ 和 $t_2$ 在智能通讯网络中的距离；函数 $p_{t_1}$、$p_{t_2}$ 代表的是返回敏感词在网络中对应的双亲元素节点；$p^i_{t_1}=p^j_{t_1}$ 代表的是具有相同祖先的两个节点，但以上两个节点不存在后代关系；$p_{t_1}//p_{t_2}$ 代表的是两个函数在智能通讯网络中为祖先后代关系；函数 $lev(\ )$ 代表的是返回元素节点在智能通讯网络中的层数；$t_c$ 代表的是 $t_1$ 和 $t_2$ 之间为相同祖先的元素节点。

当 $p_{t_1}=p_{t_2}$ 时，表明两个敏感词在智能通讯网络中的双节点相同，即两个敏感词在智能通讯网络中为兄弟节点，在智能通讯网络中的距离为 1；当 $p_{t_1}$ 和 $p_{t_2}$ 在智能通讯网络中为祖先后代关系时，两个敏感词在网络中层次差的绝对值即为两个敏感词在智能通讯网络中的位置差；当两个敏感词的祖先相同时，需要寻找敏感词在网络中的祖先节点，求取祖先节点与节点之间层次差值对应的绝对值，将计算得到两个绝对值相加，得到敏感词在网络中的距离。

多个敏感词之间在网络中的距离 $T(t_1,t_2,\cdots,t_n)$ 计算公式如下：

$$T(t_1,t_2,\cdots,t_n)=\sum_{i=1}^{n-1}T(t_i,t_{i+1}) \tag{2}$$

可以通过敏感词距离的计算，反映智能通讯网络中敏感信息的分布情况，当敏感信息距离越小时，表明智能通讯网络中敏感信息越集中，即文档的敏感程度越高；当敏感信息的距离越大时，表明智能通讯网络中敏感信息越分散，即文档的敏感程度越低[8]。

### 2.2 结合语义和结构的敏感度计算方法

设 $J(t_i)$ 代表的是敏感词在智能通讯网络中的结构相关度，在敏感词间距离的基础上得到敏感词结构相关度的计算公式：

$$J(t_i)=\frac{\sum_{i=1}^{n}TF(t_i)}{1+|td(t_1,t_2,\cdots,t_n)-T(t_1,t_2,\cdots,t_n)|} \tag{3}$$

式中，$TF(t_i)$ 代表的是在智能通讯网络中检测出敏感词 $t_i$ 的总数；$td(t_1,t_2,\cdots,t_n)$ 代表的是敏感词之间在检测数据中的距离。$td(t_1,t_2,\cdots,t_n)$ 和 $T(t_1,t_2,\cdots,t_n)$ 的值之间的差距越小，对应的差值绝对值越小，表明敏感词在检测数据中符合原始的结构关系，对应的敏感度值越大；相反，差值对应的绝对值越大，说明敏感词在检测数据中不符合原始的结构关系，对应的敏感度值越小。

结合敏感词的结构信息和语义信息得到敏感信息在智能通讯网络中的敏感度 $S(t_i)$：

$$S(t_i)=\alpha T(t_1,t_2,\cdots,t_n)+\beta J(t_i) \tag{4}$$

式中，$\alpha$、$\beta$ 为系数，满足下式：

$$\alpha+\beta=1 \tag{5}$$

根据式(4)计算得到的敏感度检测智能通讯网络中存在的敏感信息。

## 3 智能通讯网络敏感信息连接可靠性监测

根据网络信息安全的相关准则，智能通讯网络敏感信息连接可靠性的监测工作包括资产、脆弱性和威胁识别。在风险矩阵法的基础上结合信息安全管理的相关规范，构建敏感信息连接可靠性评估模型，完成智能通讯网络敏感信息连接可靠性的监测。

确定风险矩阵是构建敏感信息连接可靠性评估模型的基础[9]。构建敏感信息连接可靠性评估模型的具体过程如下：

1) 建立风险矩阵栏

风险矩阵栏用于敏感信息连接可靠性的评估，敏感信息风险矩阵栏如表 1 所示。

表 1　敏感信息风险矩阵栏

| R | P | | I | RR | RW |
|---|---|---|---|---|---|
| | L | D | L | D | |

表 1 中，R 代表的是风险项；P 代表的是风险概率；L 代表的是量化值；D 代表的是等级；I 代表的是风险影响；RR 代表的是风险等级；RW 代表的是风险权重。

2) 确定风险要素

在信息系统安全评估准则和信息安全管理规范的基础上，确定影响智能通讯网络敏感信息连接可靠性的风险要素：

①网络应用，包括数据库系统、网络设备、操作系统、应用服务和网络结构。

②人事，包括信息访问维护、人事资源、信息访问控制、安全培训和安全意识。

③物理，包括介质、环境、电缆和设备。

④资产，权责规定和资产管理框架。

⑤风险控制与策略，包括政策、策略方针、组织机构、制度规范等。

⑥管理，包括投资预算、运行、法律法规、变更控制、行政管理等

⑦组织体系，包括行政层、管理层和决策层。

3) 影响和风险概率栏的说明

确定敏感信息风险等级的基础是风险影响和风险发生的概率，将连接敏感信息的风险划分成 5 个等级，在风险发生概率中从 1 级到 5 级表示的是发生风险的概率越来越高，在风险影响中表示的风险程度逐渐加大。

识别资产、脆弱性和威胁是确定信息连接风险影响和发生概率的基础，将资产、脆弱性划分 5 个等级，并赋值：1-很低，2-低，3-中，4-高，5-很高。

设 P 代表的是信息连接风险发生的概率，其计算公式如下：

$$P = f_1(V, Q) \tag{6}$$

式中，$V$ 代表的是脆弱性严重程度；$Q$ 代表的是威胁出现的频率。

设 $I$ 代表的是风险影响值，其计算公式如下：

$$I = f_2(V, A) \tag{7}$$

式中，$A$ 代表的是资产价值。$Q = (q_1, q_2, \cdots, q_i, \cdots, q_m)$，$1 \leqslant i \leqslant m$，$q_i$ 为正整数；$V = (v_1, v_2, \cdots, v_j, \cdots, v_n)$，$1 \leqslant j \leqslant n$，$v_j$ 为正整数。其中，$f_1$、$f_2$ 代表的是专家二维矩阵，两个矩阵中存在的行均表示脆弱性的严重程度，矩阵 $f_1$ 中存在的列代表的是威胁在智能通讯网络中出现的频率；矩阵 $f_2$ 中存在的列代表的是资产重要性对应的等级。

4) 风险等级确定

在风险影响等级和风险概率等级的基础上构建风险等级表，如表 2 所示。

表 2　风险等级表

| | | P | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| | 1 | 0.5 | 1 | 1.5 | 2.5 | 3 |
| | | hd | hd | d | z | z |
| | 2 | 1 | 1.5 | 1.5 | 3 | 3.5 |
| | | hd | d | d | z | g |
| 1 | 3 | 1.5 | 2 | 3 | 3 | 4 |
| | | d | d | z | z | g |
| | 4 | 2.5 | 2.5 | 3 | 3.5 | 4.5 |
| | | z | z | z | g | hg |
| | 5 | 3 | 3.5 | 4 | 4.5 | 5 |
| | | z | g | g | hg | hg |

表 2 中，I 代表的是风险影响；P 代表的是风险概率；数字代表的是等级量化；d 为低；hd 为很低；z 为中；g 为高；hg 为很高。将检测得到的敏感信息的风险影响等级和风险概率等级带入表 2 中，确定敏感信息的风险等级。

5) 确定风险权重

智能通讯网络敏感信息连接可靠性监测的关键步骤是计算敏感信息的风险权重。通常情况下，在风险矩阵中会产生风险结，即风险要素在智能通讯网络中的风险等级相同[10]。所以智能通讯网络敏感信息连接可靠性监测方法采用 Borda 序值法将风险项对应的重要性进行排序，消除风险矩阵中存在的风险结，结合层次分析法和 Borda 序值法计算风险要素对应的权重。

Borda 序值指的是根据重要性对评估要素进行排序，具体方法如下：

设 N 代表的是智能通讯网络中存在的风险要素的总数；i 代表的是智能通讯网络中存在的某个风险；k 代表的是某个准则；$r_{ik}$ 代表的是 $k$ 准则下风险 $i$ 在智能通讯网络中对应的风险等级；$b_i$ 代表的是 *Borda* 序值，其表达式如下：

$$b_i = \sum_{k=1}^{n} (N - r_{ik}) \tag{8}$$

利用层次分析法构建判断矩阵，得到风险项对应的权重值 $RW_i$。

6) 敏感信息连接可靠性监测

在敏感信息风险等级的基础上，根据风险项的权重和 *Borda* 序值构建敏感信息连接可靠性评估模型 *RRT*，完成智能通讯网络敏感信息连接可靠性的监测：

$$RRT = b_i \sum_{i=1}^{k} RR \times RW_i \tag{9}$$

## 4　实验结果与分析

为了验证智能通讯网络敏感信息连接可靠性监测方法的整体有效性，需要测试智能通讯网络敏感信息连接可靠性

监测方法，本次测试的实验平台为 Matlab，操作系统为 Microsoft Windows 8 Pro。分别采用智能通讯网络敏感信息连接可靠性监测方法（方法 1）、基于文本信息的网络敏感信息连接可靠性监测方法（方法 2）和基于贝叶斯网络的敏感信息连接可靠性监测方法（方法 3）进行测试，对比三种不同方法的监测效率和监测结果准确率。

1）监测效率。

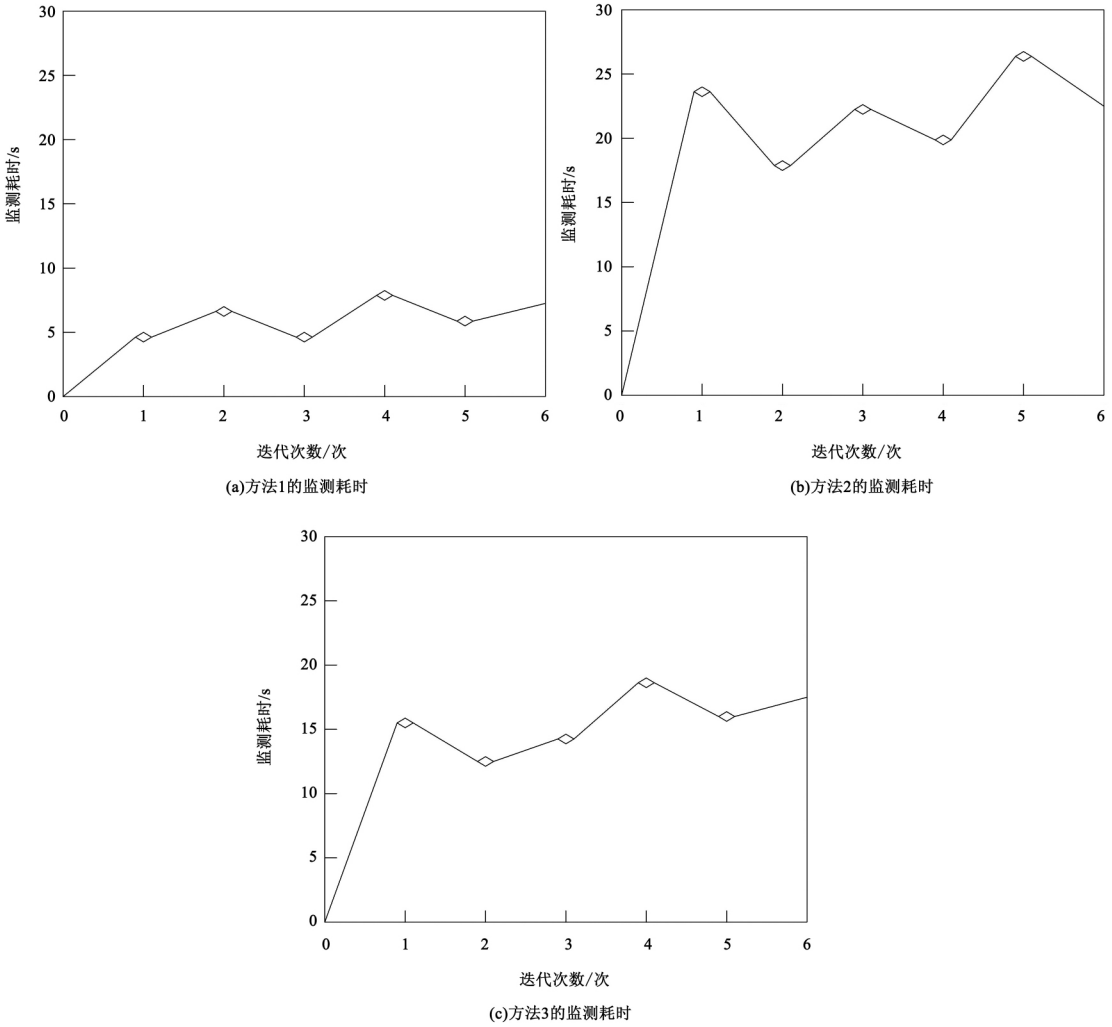



图 1　三种不同方法的监测耗时

分析图 1 可知，采用智能通讯网络敏感信息连接可靠性监测方法监测敏感信息的连接可靠性时，监测所用的时间均少于基于文本信息的网络敏感信息连接可靠性监测方法和基于贝叶斯网络的敏感信息连接可靠性监测方法监测所用时间。因为智能通讯网络敏感信息连接可靠性监测方法结合结构信息和语义信息检测智能通讯网络中存在的敏感信息，缩短了检测敏感信息所用的时间，提高了监测敏感信息连接可靠性的效率。

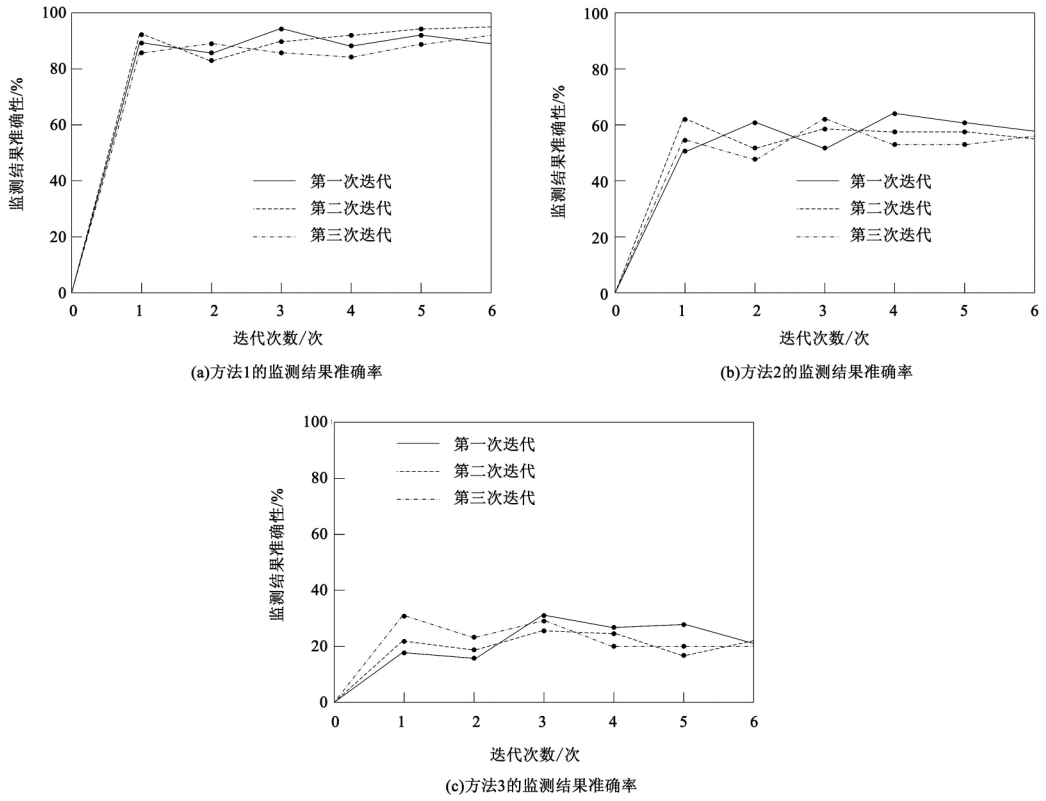
2）监测结果准确率

分析图 2 可知，智能通讯网络敏感信息连接可靠性监测方法的监测结果准确率高于基于文本信息的网络敏感信息连接可靠性监测方法和基于贝叶斯网络的敏感信息连接可靠性监测方法的监测结果准确率。因为智能通讯网络敏感信息连接可靠性监测方法先是确定敏感信息的风险等级，并利用层次分析法计算风险项对应的权重，根据计算结果结合 Borda 序值和风险等级构建敏感信息连接可靠性评估模型，根据评估结果完成敏感信息连接可靠性的监测，提高了监测结果的准确率。

## 5　结束语

智能通讯网络的飞速发展，丰富了网络中的信息资源，也增加了敏感信息、不良信息和非法信息在智能通讯网络中的数量，使智能通讯网络成为谣言讹传、封建迷信、反动言论和色情暴力等信息主要的传播媒介。当前敏感信息连接可

靠性监测方法存在监测效率低和监测结果准确率低的问题，提出智能通讯网络敏感信息连接可靠性监测方法，可在较短的时间内完成敏感信息连接可靠性的监测，解决了当前方法中存在的问题，为智能通讯网络的发展提供了保障。




(a)方法1的监测结果准确率

(b)方法2的监测结果准确率

(c)方法3的监测结果准确率

**图 2　三种不同方法的监测结果准确率**

**参考文献:**


[1] 韩立权. 无线网络攻击中保护用户敏感隐私信息仿真 [J]. 计算机仿真，2017，34(3)：277-280.

[2] 李伟明，贺玄，王永剑. 基于动态污点跟踪的敏感文件泄露检测方法 [J]. 华中科技大学学报: 自然科学版，2016，44(11)：39-42.

[3] 于合龙，丁民权，黄浦，等. 基于 ZigBee 网络的人参生长监测及病害预警 [J]. 吉林农业大学学报，2017，39(1)：120-126.

[4] 王战红.计算机网络安全中数据加密技术的应用对策 [J].现代电子技术，2017，40(11)：88-90.

[5] 杨洁，李松斌，邓浩江. 基于贝叶斯网络的压缩语音信息隐藏检测 [J]. 计算机应用，2018，38(7)：1967-1973.

[6] 李扬，潘泉，杨涛. 基于短文本情感分析的敏感信息识别 [J]. 西安交通大学学报，2016，50(9)：80-84.

[7] 郭浩，潘仲明，周靖. 无线传感器网络信息质量评估的柔性框架 [J]. 国防科技大学学报，2016，38(1)：150-155.

[8] 沙乐天，何利文，傅建明，等. 物联网环境下的敏感信息保护方法 [J]. 四川大学学报: 工程科学版，2016，48(1)：132-138.

[9] 苏赢彬，杜学绘，曹利峰，等. 文档敏感信息控制模型 DSI-CON 研究与分析 [J]. 计算机应用研究，2016，33(3)：876-881.

[10] 胡玉玺，李轶鲲，杨萍. 基于上下文敏感的贝叶斯网络及方向关系的遥感图像检索 [J]. 国土资源遥感，2017，29(3)：70-76.



**[作者简介]**

**倪铉珣**(1983-)，女(汉族)，四川自贡人，硕士，讲师，主要研究方向: 网络信息安全，企业信息化。