

# 基于 Monte Carlo 估计的免疫检测器分布优化算法

刘海龙<sup>1,2</sup>, 张凤斌<sup>1\*</sup>, 席亮<sup>1</sup>

(1. 哈尔滨理工大学 计算机科学与技术学院, 哈尔滨 150080; 2. 哈尔滨师范大学 计算机科学与技术学院, 哈尔滨 150025)

(\* 通信作者电子邮箱 zhangfb@hrbust.edu.cn)

**摘要:**针对免疫实值检测器的黑洞和边界入侵问题,分析规模对检测性能的影响,提出一种基于 Monte Carlo 估计的检测器分布优化算法,以 Monte Carlo 方法估计检测器对非自体空间的覆盖效果作为算法结束的条件,通过优秀子代替代不合时宜的父代来完成检测器的分布优化处理。经实验测试表明,该算法不仅可以有效地降低黑洞,而且能够以更少的检测器更精确地覆盖非自体空间,从而提升检测器的检测性能。

**关键词:**入侵检测;免疫检测器;分布优化;否定选择算法;Monte Carlo 估计

**中图分类号:** TP393.08 **文献标志码:** A

## Immune detector distribution optimization algorithm with Monte Carlo estimation

LIU Hailong<sup>1,2</sup>, ZHANG Fengbin<sup>1\*</sup>, XI Liang<sup>1</sup>

(1. College of Computer Science and Technology, Harbin University of Science and Technology, Harbin Heilongjiang 150080, China;

2. College of Computer Science and Technology, Harbin Normal University, Harbin Heilongjiang 150025, China)

**Abstract:** In order to avoid lots of holes among mature immune detectors and deal with the problem of boundary invasion in intrusion detection, analyzing the relationship between number of detectors and detection performance, a detector distribution optimization algorithm with Monte Carlo estimation was proposed: evaluating the coverage of detectors by the Monte Carlo method, and updating the detector set by the offspring to improve detectors' distribution. The experimental tests demonstrate that the algorithm can not only decrease the holes but also achieve a more precise coverage of the nonself space with fewer detectors, and increase the detector's detection performance.

**Key words:** intrusion detection; immune detector; distribution optimization; negative selection algorithm; Monte Carlo estimation

## 0 引言

生物免疫系统是一个自适应、自组织和自学习系统,具有很强的自我保护功能,人工免疫系统模拟生物免疫系统并成功应用于网络入侵检测领域<sup>[1]</sup>。在基于免疫的入侵检测系统中,最核心部件是免疫检测器,它决定了系统的检测性能的好坏<sup>[2]</sup>,主要是通过否定选择算法(Negative Selection Algorithm, NSA)将候选个体与自体集合进行耐受训练而得到<sup>[3]</sup>。按照自体与检测器的表示方法主要分为两种:二进制和实值。相应地,NSA 也分为二进制否定选择算法(Binary NSA, BNS)和实值否定选择算法(Real-valued NSA, RNS)。由于二进制表示方法过于简单且效果不理想,所以目前研究目光主要集中在实值表示法上<sup>[4]</sup>。

在免疫实值检测器集中,由于候选个体的随机性和不完备性,会存在大量的黑洞问题,而且由于检测器半径设定的不恰当也会造成部分检测器覆盖自体区域而造成边界入侵问题。为了解决这些问题,国内外学者将目光投入到检测器的优化算法上,主要通过改变检测器的表示形态<sup>[5]</sup>,增加不同的优化算子(如变异算子<sup>[6]</sup>、阳性选择算子、疫苗算子等<sup>[7]</sup>)和调整检测器半径等手段进行<sup>[8]</sup>,但都存在着复杂度过高、可控性较差等问题,效果都不甚理想。

本文就此提出一种基于 Monte Carlo 的检测器优化算法,该算法利用 Monte Carlo 方法估计当前检测器对非自体空间的覆盖效果,利用亲和力和调整检测器半径,并判定当前检测器

是否合适并生成更优的子代替代不合宜的父代,从而有效解决黑洞问题,提高检测器的检测性能。

## 1 相关工作

### 1.1 自体、检测器和否定选择算法

#### 1) 自体与检测器。

在基于免疫的入侵检测中通常将问题域  $U$  分为两部分:自体空间  $U_S$  和非自体子空间  $U_N$ :

$$U = U_S \cup U_N \quad (1)$$

其中:自体集合  $S \subseteq U_S$ ,检测器集合  $D \subseteq U_N$ 。自体 and 检测器分别分布于  $S$  和  $D$ :

$$S = \{s_1, s_2, \dots, s_{N_s}\} \quad (2)$$

$$D = \{d_1, d_2, \dots, d_{N_d}\} \quad (3)$$

其中  $N_s$  和  $N_d$  分别为自体 and 检测器个数。实值自体样本可以表示为:

$$s_i = (a_{i1}, a_{i2}, \dots, a_{iN}, r) \quad (4)$$

其中:  $i = 1, 2, \dots, N_s$ ,  $a_{ij}$  为该自体样本第  $j$  ( $j = 1, 2, \dots, N$ ) 维属性值,  $r$  为该自体样本训练半径。同理,每个检测器可以表示成:

$$d_i = (b_{i1}, b_{i2}, \dots, b_{iN}, r) \quad (5)$$

其中:  $i = 1, 2, \dots, N_d$ ,  $b_{ij}$  为该检测器第  $j$  ( $j = 1, 2, \dots, N$ ) 维属性值,为该检测器的判定半径。

#### 2) 否定选择算法。

否定选择算法是对免疫细胞的成熟过程的模拟,主要通

收稿日期:2012-09-18;修回日期:2012-10-28。 基金项目:国家自然科学基金资助项目(60671049, 61172168)。

作者简介:刘海龙(1976-),男,黑龙江佳木斯人,博士研究生,主要研究方向:网络与信息安全; 张凤斌(1965-),男,黑龙江哈尔滨人,教授,博士生导师,博士,主要研究方向:网络与信息安全; 席亮(1983-),男,河北邢台人,讲师,博士,主要研究方向:网络与信息安全。

过计算样本间的亲和力(Affinity)判断样本是否匹配<sup>[9]</sup>。算法应用两个阶段:训练检测器阶段和检测器检测阶段,如图1所示。训练阶段主要负责检测器的生成,过程为:先随机产生候选检测器并进行亲和力耐受训练,删除与自体亲和力较高(即匹配)的个体,并保留能检测非自体的个体作为成熟检测器,模拟成熟的免疫细胞;在检测阶段,事件依次与每个检测器进行亲和力计算,亲和力高的事件(即匹配检测器的事件)被认为是异常。

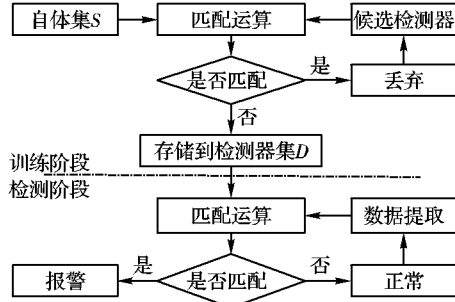


图1 否定选择算法

## 1.2 问题分析

### 1) 黑洞与边界入侵问题<sup>[10]</sup>。

黑洞就是检测器应该覆盖但没有覆盖的非自体区域,如图2所示。这些区域有可能存在异常事件所具有的特征,检测器没有覆盖它们,则在检测阶段不会检测到含有这些特征的异常事件,从而降低系统的检测率。

边界入侵是指由于检测器的半径设定的不合适,会使得位于自体/非自体边界区域的检测器覆盖自体区域,如图2所示。检测器覆盖了自体区域则在检测阶段会将位于自体区域的正常事件误判为异常从而造成误报问题。

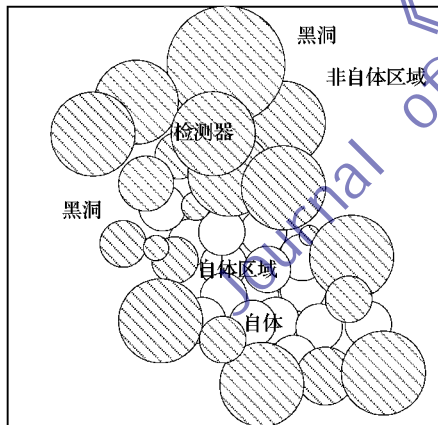


图2 黑洞问题

### 2) 检测器规模问题。

经推导,检测器漏报任一异常的概率 $p_f^{[11]}$ 为:

$$p_f \approx \exp(-N_d P_m) \quad (6)$$

其中 $p_m$ 为每个检测器匹配异常的概率(各不相同但近似相等)。可以看出,当 $p_m$ 一定时,一次误报率与检测器数量呈指数关系。而解决黑洞问题,往往通过生成大量的检测器来解决,这就造成了检测器规模(影响误报率)和黑洞(影响检测率)之间的矛盾。

## 2 基于 Monte Carlo 估计的检测器优化算法

本文在分析了检测器存在的主要问题后,提出一种基于 Monte Carlo 的检测器分布优化算法(immune Detector Distribution Optimization algorithm with Monte Carlo, DDMC),

算法通过与自体进行亲和力计算来调整检测器的半径从而阶段边界入侵问题,以及判定当前检测器是否适宜并通过生成更优秀的子代、去除不合时宜的父代来降低黑洞,从而达到调整检测器分布的效果,以 Monte Carlo 方法估计当前检测器对非自体空间的覆盖效果来判定当前优化是否结束。

### 2.1 Monte Carlo 估计

Monte Carlo 方法是一种经典的数据分析方法<sup>[12-13]</sup>。Monte Carlo 方法是通过在形态空间中随机生成一组具有独立同分布的均匀序列点: $x_1, x_2, \dots, x_m$ ,通过计算位于不同区域内的点数来近似得到相应的值,从而得到一些有关子区域占总区域比例的参考量。通过这个思想,本文采取 Monte Carlo 方法来估计单个检测器占整个形态空间的体积(百分比),单个检测器与其他检测器重叠区域占其本身区域的百分比,检测器集合对非自体空间的覆盖率以及检测器集合的总重叠率。并利用这些数值判定当前检测器集对非自体空间的覆盖效果,对优化算法过程进行约束。近似计算这几个参数的大体方法如下:

1) 估计单个检测器占整个形态空间的比值:

$$C(d) \approx \frac{\sum_{i=1}^m X_d(x_i)}{m} \quad (7)$$

其中:

$$X_d(x_i) = \begin{cases} 1, & x_i \in d \\ 0, & x_i \notin d \end{cases} \quad (8)$$

2) 估计单个检测器与其他检测器重叠区域占其本身区域的百分比:

$$O(d) \approx \frac{\sum_{i=1}^m X_{dd}(x_i)}{\sum_{i=1}^m X_d(x_i)} \quad (9)$$

其中:

$$X_{dd}(x_i) = \begin{cases} 1, & x_i \in d \text{ 且} \\ & x_i \in d_j (d_j \neq d; j = 1, 2, \dots, N_d) \\ 0, & \text{其他} \end{cases} \quad (10)$$

3) 估计检测器集对非自体空间的覆盖率:

$$C(D) \approx \frac{\sum_{i=1}^m X_D(x_i)}{m - \sum_{i=1}^m X_S(x_i)} \quad (11)$$

其中:

$$X_D(x_i) = \begin{cases} 1, & x_i \in D \\ 0, & x_i \notin D \end{cases} \quad (12)$$

$$X_S(x_i) = \begin{cases} 1, & x_i \in S \\ 0, & x_i \notin S \end{cases} \quad (13)$$

4) 由式(7)和式(9)可估计检测器集的总重叠率:

$$O(D) \approx \sum_{i=1}^{N_d} (O(d_i) \cdot C(d_i)) \quad (14)$$

### 2.2 算法实现

输入 自体集 $S$ 、检测器集 $D$ 、覆盖率阈值 $\Phi$ 。

输出 优化后检测器集合 $D'$ 。

BEGIN

$\varphi = C(D)$ ;

While ( $\varphi < \Phi$ ) {

For ( $i = 0; i < N_d; i++$ ) {

// 调整检测器半径避免边界入侵

```

    查询与  $d_i$  最近的自体  $s$ ;  $d_i.r = d_i - s.r$ ;
}
For ( $i = 0$ ;  $i < N_d$  &&  $d_i \neq \text{NULL}$ ;  $i++$ ) {
    找到与  $d_i$  亲和力最大的  $d_j$ ;
    If ( $A(d_i, d_j) \leq |d_i.r - d_j.r|$ )
        // 处理被其他个体覆盖的个体
        删除半径较小者并将另一个放入  $D'$ ;
    Else {
        // 通过子代替代不合宜父代和覆盖黑洞
        取二者的中点生成子代  $d_0$ ;
        If ( $A(d_i, d_j) < (d_i.r + d_j.r)$ ) {
            查询与该子代最近的自体  $s$ ;
             $d_0.r = d_0 - s.r$ ;
            If ( $d_0.r < (d_i.r + d_j.r)/2$ ) 丢弃  $d_0$  并将  $d_i, d_j$  放入  $D'$ ;
            If ( $d_0.r > (d_i.r + d_j.r)$ ) 丢弃  $d_i, d_j$  并将  $d_0$  放入  $D'$ ;
            Else 将  $d_i, d_j, d_0$  放入  $D'$ ;
        }
    }
}
If ( $A(d_i, d_j) > (d_i.r + d_j.r)$ ) {
     $d_0.r = A(d_i, d_j) - (d_i.r + d_j.r)$ ;
    If ( $d_0$  覆盖自体) 丢弃  $d_0$  并将  $d_i, d_j$  放入  $D'$ ;
    Else 将  $d_i, d_j, d_0$  放入  $D'$ ;
}
}
 $\varphi = C(D'); D = D'$ ;
END

```

### 3 实验分析

本文通过两个实验来验证算法的可行性:利用二维数据集直观反映算法对检测器分布优化的效果;利用 Fisher's Iris 数据集验证优化后的检测器集的检测效果。

实验以数据集中正常记录为自体训练检测器并使用这些检测器检测数据集中的异常记录。计算正确肯定次数  $TP$ 、正确否定次数  $TN$ 、错误肯定次数  $FP$ 、错误否定次数  $FN$ , 并使用这 4 个值计算检测率 (异常事件被检测为异常的概率,  $P = TP/(TP + FN) \times 100\%$ ) 和误报率 (正确的事件被误检测为异常的概率,  $P_f = FP/(TN + FP) \times 100\%$ ) 来判定检测器对非自体空间的覆盖效果。

#### 3.1 二维数据集实验

本实验以经常被使用的五角星数据集来进行实验<sup>[14]</sup>, 该数据集的样本占据以空间中心为中心的五角星区域, 共 198 个样本如图 3(a) 所示。实验将所有样本作为自体集, 利用 RNS 生成检测器 100 个, 如图 3(b) 所示, 可以看出其中存在许多黑洞, 而且部分检测器入侵了自体区域, 此时  $C(D)$  为 62.8%,  $O(D)$  为 19.9%。利用 RNS 生成检测器 500 个, 如图 3(c) 所示, 可以看出虽然黑洞减少了, 但是需要大量的检测器, 此时  $C(D)$  为 96.1%, 但重叠率很高 ( $O(D)$  为 93.8%), 同时检测器入侵自体区域的问题更加严重, 这会增加系统的误报率 (式(6) 得)。利用本文算法对图 3(b) 的 100 个检测器进行优化, 设定  $\Phi$  为 95%, 结果如图 3(d) 所示, 可以看出, 检测器个数减少 (35 个),  $O(D)$  为 11.7%, 黑洞减少而且边界入侵问题也得到了解决。设定  $\Phi$  为 97.5%, 结果如图 3(e) 所示, 可以看出, 检测器个数略有增加 (42 个),  $O(D)$  为 16.4%。设定  $\Phi$  为 99%, 结果如图 3(f) 所示, 可以看出, 检测器个数又略有增加 (55 个),  $O(D)$  为 17.1%, 但检测器对非自体空间的覆盖率更高, 重叠率则一直处于一个相对较低的水平。

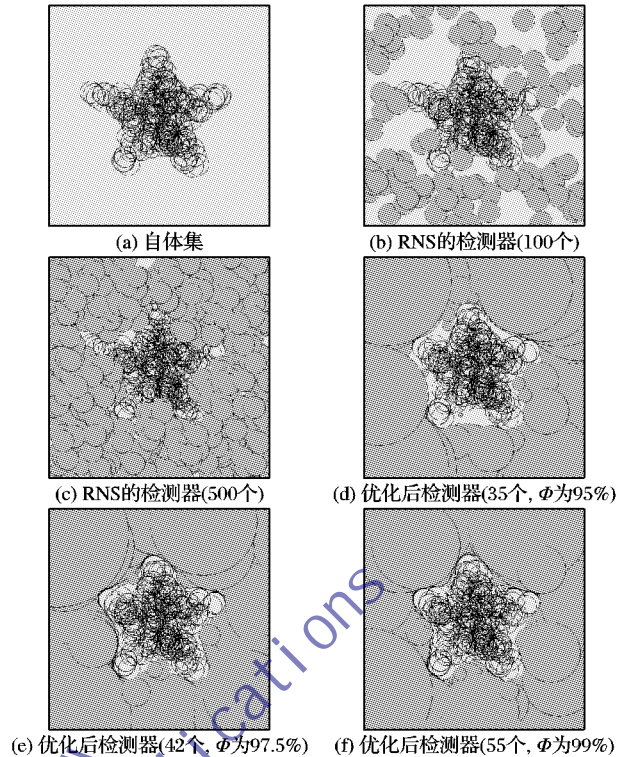


图3 自体集、RNS 及其优化后的检测器

#### 3.2 Fisher's Iris 数据集实验

该数据集是对 Iris 花型的统计数据<sup>[15]</sup>, 包含 3 组数据, 每组为 1 类 Iris 花型, 分别是 Setosa、Versicolor 和 Virginica, 每组含 50 个样本, 每个样本有 4 个属性, 分别是花萼长、花萼宽、花瓣长、花瓣宽 (单位均为 cm)。该数据集已经被用来测试异常检测、数据挖掘等领域的技术和算法的有效性和可行性。

经分析得出, 该数据集其中的 2 组 (Versicolor 组和 Virginia 组) 样本在空间中分布比较接近, 另外 1 组 (Setosa 组) 样本在空间中分布相距这 2 组样本较远<sup>[9]</sup>。在此, 选取 Setosa 组作为自体集, 另外两组作为异常事件, 使用全部数据集作为测试集来测试检测器的性能。

为了对比实验, 本文选取数据集使用优化前后的检测器分别进行测试。首先, 利用 RNS 生成检测器 100 个和 300 个, 然后利用本文的优化算法对 RNS 生成的 100 个检测器组进行优化, 分别设定  $\Phi$  为 95%、97.5%、99%, 最后用测试集分别对这 5 组检测器检测, 进行 10 次取均值结果如表 1 所示。

表1 五组检测器的检测效果

生成算法	检测器数	覆盖率/%	重叠率/%	检测率/%	误报率/%
RNS	100.0	52.9	21.1	57.7	8.43
	300.0	87.3	77.7	78.4	36.90
DDOMC	37.1	95.0	22.5	96.8	0.00
	48.8	97.5	26.3	98.4	0.00
	61.0	99.0	26.7	99.1	0.00

从表 1 可看出, RNS 生成检测器数少时检测率很低, 黑洞很多; 检测器数多时虽然检测率提升了, 黑洞减少了, 但重叠率太高, 误报率也大大增加。这就说明 RNS 生成的检测器的检测效果很差。利用 DDOMC 优化后的检测器覆盖率得到了保障, 解决了黑洞问题, 而且检测器数量也大大降低, 重叠率也不高, 检测率很高而且误报率一直为 0。这就说明了优化后的检测器的检测效果得到了明显改善。



## 4 结语

本文提出一种基于 Monte Carlo 的检测器优化算法,主要的优点如下:

1) 利用亲和力计算调整检测器半径,可以很好地避免检测器边界入侵自体区域,从而降低误报率。

2) 用子代替代不合适的个体,可以有效地剔除不合时宜的个体,同时子代的补充也可保证当前检测器的时效性。

3) 利用 Monte Carlo 估计当前检测器对非自体区域的覆盖率来判定是否达到优化的预期效果来作为优化的结束条件可以较好地掌握和控制当前检测器对非自体空间的覆盖效果,提高系统的检测率。

实验结果表明算法能够以较少的、性能更好的检测器更精确地覆盖非自体空间,解决检测器的黑洞和边界入侵问题,降低检测器的规模,从而提高了检测器的检测性能。

### 参考文献:

- [1] KIM J, BENTLEY P J. The human immune system and network intrusion detection [C]// Proceedings of the 7th European Congress on Intelligent Techniques and Soft Computing. Aachen, Germany: EUFIT, 1999: 1120 - 1125.
- [2] ZHOU J, DASGUPTA D. V-Detector: an efficient negative selection algorithm with "probably adequate" detector coverage [J]. Information Science, 2009, 179(10): 1390 - 1406.
- [3] ZHOU J, DASGUPTA D. Revisiting negative selection algorithms [J]. Evolutionary Computation, 2007, 15(2): 223 - 251.
- [4] GONZALEZ F, DASGUPTA D, KOZEMA D. Combining negative and classification techniques for anomaly detection [C]// Proceedings of 2002 Congress on Evolutionary Computation. Piscataway, NJ: IEEE Press, 2002: 705 - 710.
- [5] BALACHANDRAN S, DASGUPTA D, NINO F and *et al.* A frame-

work for evolving multi-shaped detectors in negative selection [C]// Proceedings of the 2007 IEEE Symposium on Foundations of Computational Intelligence. Piscataway, NJ: IEEE Press, 2007: 401 - 408.

- [6] 王辉, 毕晓君, 于立君, 等. 基于疫苗理论的变阈值免疫阴性选择算法[J]. 哈尔滨工程大学学报, 2011, 32(1): 69 - 72.
- [7] 方贤进, 李龙澍, 钱海. 基于人工免疫的网络入侵检测中疫苗算子的作用研究[J]. 计算机科学, 2010, 37(1): 239 - 242.
- [8] VIOLATO, R P, AZZOLINI A G, *et al.* Antibodies with adaptive radius as prototypes of high-dimensional datasets[C]// Proceedings of the 9th International Conference on Artificial Immune Systems. Berlin: Springer, 2010: 158 - 170.
- [9] FORREST S, PERELSON A S, ALLEN L. Self-nonself discrimination in a computer [C]// Proceedings of the 1994 IEEE Society Symposium on Research in Security and Privacy. Piscataway, NJ: IEEE Press, 1994: 202 - 212.
- [10] ZHOU J. A boundary-aware negative selection algorithm [C]// Proceedings of 2005 International Conference on Artificial Intelligence and Soft Computation. Anaheim, CA, USA: ACTA Press, 2005: 12 - 14.
- [11] ZHANG F B, XI L, WANG S W. V-detector optimization algorithm [J]. High Technology Letters, 2012, 22(5): 449 - 454.
- [12] MACKAY J C. Introduction to Monte carlo methods [M]. Oak Ridge, USA: Oak Ridge National Laboratory, 1995: 23 - 39.
- [13] LIU J S. Monte carlo strategies in scientific computing [M]. Berlin: Springer, 2001: 53 - 77.
- [14] ZHOU J, DASGUPTA D. Estimating the detector coverage in a negative selection algorithm [C]// Proceedings of 2005 Conference on Genetic and Evolutionary Computation. New York: ACM Press, 2005: 281 - 288.
- [15] UCI M L R. Fisher's iris data [DB/OL]. [2009-12-23]. <http://archive.ics.uci.edu/ml/datasets/Iris>.

(上接第 722 页)

## 3 结语

本文解决了一类属性权重不完全确定下的多维时序信任度排序问题,采用线性规划理论确定一维时序下信任度的上下限排序,再采用最优协调排序模型对多维时序下的信任度上下限排序进行综合,最终确定受评对象的信任度大小排序。本文提出的多属性决策的多维时序信任度排序方法具有以下特点:1) 它不必确定目标的权系数,只要确定目标权重的一定排序(弱排序),或补充一定目标的权重信息(严排序)就可以做出比较客观的评价;2) 在信任评价过程时,通过适当调高最优协调排序模型参数  $q$ ,可以识别受评对象中信任度摇摆不定的潜在不诚实对象;3) 在小样本或评价过程可能存在异常时,通过适当调低最优协调排序模型参数  $q$  可以解决传统信任评价方法在孤立点上由于数据突变所造成的错评现象。

### 参考文献:

- [1] 李峰, 申利民, 司亚利, 等. 基于交互感知的动态自适应的信任评估模型[J]. 通信学报, 2012, 33(10): 60 - 70.
- [2] 王勇, 毛国君, 代桂平, 等. 组合网络服务的信任度估算算法[J]. 北京工业大学学报, 2009, 35(10): 1407 - 1411.
- [3] 鄢旭, 陈晶, 杜瑞颖, 等. 无线传感器网络中基于组合框架的贝叶斯信任模型[J]. 计算机应用研究, 2012, 29(3): 1078 - 1083.
- [4] 陈鑫, 王晓晗, 黄河. 基于威胁分析的多属性信息安全风险评估

方法研究[J]. 计算机工程与设计, 2009, 30(1): 38 - 40.

- [5] 李兰英, 李晓芸. 一种基于层次模型的网络信息安全风险灰色评估方法[J]. 科学技术与工程, 2010, 10(2): 540 - 545.
- [6] 李艺, 李新明, 崔云飞. 软件脆弱性危险程度量化评估模型研究[J]. 计算机科学, 2011, 38(6): 169 - 172.
- [7] 付钰, 吴晓平, 王甲生. 基于模糊-组合神经网络的信息系统安全风险评估[J]. 海军工程大学学报, 2010, 22(1): 18 - 23.
- [8] NAYAGAM V L G, MURALIKRISHNAN S, SIVARAMAN G. Multicriteria decision-making method based on interval-valued intuitionistic fuzzy sets[J]. Expert Systems with Applications, 2011, 38(3): 1464 - 1467.
- [9] 江红莉, 何建敏, 庄亚明, 等. 基于直觉模糊集和证据理论的群决策方法[J]. 控制与决策, 2012, 27(5): 752 - 756.
- [10] 蔡红云, 杜瑞忠, 田俊峰. 基于多维信任云的信任模型研究[J]. 计算机应用, 2012, 32(1): 5 - 7, 34.
- [11] YE J. Multicriteria fuzzy decision-making method based on a novel accuracy function under interval-valued intuitionistic fuzzy environment[J]. Expert Systems with Applications, 2009, 36(3): 6899 - 6902.
- [12] 李登峰. 模糊多人决策与对策[M]. 北京: 国防工业出版社, 2003: 61 - 70.
- [13] 张惠珍, 马良. 几种基于匈牙利算法求解二次分配问题的方法及其分析比较[J]. 运筹与管理, 2010, 19(1): 92 - 99.