基于免疫 MHC 的否定选择算法孔洞修复方法

朱方东¹, 李涛^{2*}, 杨进²

1. 四川大学计算机学院, 成都 610065

2. 四川大学网络空间安全学院, 成都 610065

* 通信作者. E-mail: litao@scu.edu.cn

收稿日期: 2019-02-25; 修回日期: 2019-05-31; 接受日期: 2019-08-08; 网络出版日期: 2020-10-13

国家重点研发计划 (批准号: 2016YFB0800600)、国家自然科学基金 (批准号: U1736212, 61572334) 和四川省重点研发项目 (批准号: 2018GZ0183) 资助项目

摘要 否定选择算法 (negative selection algorithm, NSA) 是人工免疫系统的核心基础算法. 孔洞是引起 NSA 检测率低的重要因素. 传统 NSA 未考虑孔洞的分布, 采取在特征空间内通过完全随机的方式盲目生成检测器以修复孔洞, 导致孔洞修复效果不佳, 并且淘汰无效的检测器也异常耗时. 孔洞问题在生物免疫系统中也同样存在. 生物免疫系统利用 MHC 分子针对孔洞产生的特殊形态, 对免疫细胞的发育过程进行限定, 从而训练出覆盖孔洞的免疫细胞, 进而解决孔洞问题. 受此启发, 本文提出一种基于免疫 MHC 的否定选择算法——孔洞修复方法 MHC-NSA. 首先以训练样本生成的维诺图 (Voronoi) 对形态空间进行划分, 利用维诺图的最邻近特性, 在维诺图中两类点处快速生成两类检测器, 以较小训练代价达到对非自体空间较好的覆盖; 其次模拟 MHC 针对孔洞所具有的特殊形态, 对所产生的孔洞位置进行定位, 并限定该位置生成孔洞修复检测器, 从而提升孔洞修复效果. 理论分析表明, MHC-NSA 所生成的孔洞修复检测器可将孔洞最高占比降低 62.8%, 且 MHC-NSA 的时间复杂度由传统 NSA 算法的指数阶降低到多项式阶. 在 UCI 数据集 Balance Scale 上的实验表明, MHC-NSA 的检测器训练时间较典型 NSA 算法代表 RNSA, V-Detector 和 BIORV-NSA 在分别降低 53.73%, 96.43% 和 92.66% 的同时, 检测率分别提升 69.57%, 44% 和 17.54%.

关键词 人工免疫系统, MHC, 否定选择算法, 孔洞

1 引言

人工免疫系统 (artificial immune system, AIS) 是借鉴生物免疫系统的机制和理论发展而来的自适应系统^[1], 现已广泛应用于网络入侵检测、故障诊断、异常检测等领域. 否定选择算法 (negative selection algorithm, NSA) 作为人工免疫系统中训练检测器的核心基础算法, 在 1994 年由美国新墨西哥

引用格式: 朱方东, 李涛, 杨进. 基于免疫 MHC 的否定选择算法孔洞修复方法. 中国科学: 信息科学, 2020, 50: 1529–1543, doi: 10.1360/N112018-00188
Zhu F D, Li T, Yang J. A negative selection algorithm hole improvement method based on MHC (in Chinese). Sci Sin Inform, 2020, 50: 1529–1543, doi: 10.1360/N112018-00188

哥大学 (The University of New Mexico) 终身教授 Forrest 等^[2] 提出后引起广泛关注. 国际权威学术期刊 *Nature*^[3], *Science*^[4] 也多次专题报道. 它通过模拟生物免疫系统中免疫细胞的发育过程, 仅以正常样本为自体, 训练出通过自体耐受的成熟检测器. 从而达到无需异常样本的前提下, 有效识别未知元素^[5].

孔洞是指 NSA 算法训练的检测器无法覆盖的非自体空间区域, 它是引起 NSA 性能下降的重要因素^[6]. 近年来, 国内外 AIS 学家针对孔洞问题提出了一系列的改进方法, 技术路线主要分为以下 3 类: (1) 优化检测器的生成数量^[2,7,8], 以 2003 年美国孟菲斯大学 (The University of Memphis) González 等^[7] 提出的 RNSA 为代表. RNSA 通过蒙特卡洛 (Monte Carlo) 方法来估计所需生成的检测器数量, 避免了因检测器生成数量不足导致的孔洞问题. 但由于随机的盲目性, 生成的检测器互相覆盖程度较高, 孔洞范围仍较大. (2) 改进检测器的表达方式^[6,9~11], 以 2009 年美国哥伦比亚大学 (Columbia University) Ji 等^[6] 提出的 V-Detector 为代表. V-Detector 通过将检测器的检测半径从固定值改进为可变值, 有效改进了检测器互相覆盖导致孔洞较大的问题. 但由于未考虑孔洞的分布, 在特征空间内完全随机方式生成检测器, 当覆盖率升高时, 随机生成的检测器与已有检测器或自体的耐受成功概率急剧下降, 导致时间复杂度随自体集数量成指数级增长^[1]. (3) 修改自体耐受原则^[12~15], 以 2015 年南京航空航天大学皮德常教授等^[12] 提出的 BIORV-NSA 为代表. BIORV-NSA 认为自体边缘区域是自体可“忍受”的区域, 允许检测器的检测范围覆盖该区域. 该方法可有效改进自体周边难以解决的孔洞区域, 但由于检测器的检测范围覆盖部分自体区域, 导致部分自体元素被误识为非自体, 从而误报率上升.

虽然以上算法从多个角度改进 NSA 的孔洞问题, 但忽略了孔洞的分布, 在特征空间内以完全随机方式生成检测器, 导致孔洞修复效率较低. 孔洞在生物免疫系统中同样存在, 且病原体总在向孔洞进化, 从而躲避查杀^[16]. 最新医学研究表明^[17,18], MHC (主要组织相容性复合体) 是生物免疫系统解决孔洞问题的关键. MHC 是细胞表面存在的一组特异的糖蛋白分子, 也是免疫系统重要的组成部分. 生物免疫系统利用 MHC 分子针对孔洞产生的特殊形态, 对免疫细胞的发育过程进行限定, 从而训练出覆盖孔洞的免疫细胞, 进而解决孔洞问题.

受此启发, 本文提出一种基于免疫 MHC 的否定选择算法孔洞修复方法 MHC-NSA. MHC-NSA 包含两个阶段: (1) 检测器快速生成阶段. 以训练样本生成的维诺图 (Voronoi) 对形态空间进行划分, 在维诺图中两类点处快速生成两类检测器. 由于维诺图具备将空间按距离划分邻近区域的特性, 从而避免了传统 NSA 中耗时的查找最邻近自体过程, 以较小训练代价达到对非自体空间较好的覆盖. (2) 孔洞修复阶段. 由于维诺图将特征空间划分为不同的区域, 且在区域内两类 MHC 检测器与自体的位置关系相对确定, 因此孔洞的分布可计算. 本阶段模拟 MHC 针对孔洞所具有的特殊形态. 针对 (1) 阶段存在的孔洞进行定位, 并限定孔洞位置生成孔洞修复检测器, 从而提高孔洞修复效果.

本文的创新在于: 将传统 NSA 算法未考虑孔洞的分布, 在整个特征空间内通过完全随机、盲目地进行修复孔洞的方式, 改进为模拟 MHC 修复生物免疫系统孔洞过程, 通过计算孔洞产生的位置, 针对性地生成孔洞修复检测器, 从而提高孔洞修复效率. 理论分析表明, MHC-NSA 所生成的孔洞修复检测器可将孔洞最高占比降低 62.8%, 且 MHC-NSA 的时间复杂度由传统 NSA 算法的指数阶降低到多项式阶. 在 UCI 数据集 Balance Scale 上的实验表明, MHC-NSA 的检测器训练时间较典型 NSA 算法代表 RNSA, V-Detector 和 BIORV-NSA 在分别降低 53.73%, 96.43% 和 92.66% 的同时, 检测率分别提升 69.57%, 44% 和 17.54%.

2 MHC-NSA 算法

MHC-NSA 算法的主要思路是在快速生成检测器的基础上, 通过定位孔洞位置, 针对性地修复孔

图 1 (网络版彩图) 特征空间划分示意. $S_1 \sim S_5$ 是特征空间 $[0, 1]^2$ 下 5 个基点. 实线是对应的维诺图 $\text{Vor}(S)$, 其将特征空间划分为 5 个区域 $\nu(S_1) \sim \nu(S_5)$. 点 p 是 MHC-I 类检测器中心. 点 q 是 MHC-II 类检测器中心

Figure 1 (Color online) A partition of feature space. $S_1 \sim S_5$ are 5 base points. The solid lines are the Voronoi diagram $\text{Vor}(S)$. The feature space $[0, 1]^2$ is partitioned into 5 cells $\nu(S_1) \sim \nu(S_5)$. p is a center of MHC-I detector. q is a center of MHC-II detector

洞, 从而提高检测率. MHC-NSA 算法包括两个阶段: 检测器快速生成阶段和孔洞修复阶段.

2.1 检测器快速生成阶段

MHC-NSA 检测器快速生成阶段通过利用维诺图的最邻近特性^[19], 快速生成 MHC-I 和 MHC-II 类检测器. 该阶段可分为 3 个步骤: 特征空间划分、MHC-I 类检测器生成和 MHC-II 类检测器生成.

2.1.1 特征空间划分

维诺图具备将空间按距离划分最邻近区域的特性^[19], 是计算几何领域最重要的数据结构之一. MHC-NSA 以给定的 n 个互异的自体元素 (训练样本) 作为基点集 S , 生成维诺图 $\text{Vor}(S)$, 对 $[0, 1]^d$ 特征空间 X 进行划分. 如图 1 所示. 维诺图 $\text{Vor}(S)$ 将特征空间 X 划分为 n 个互不重叠的区域 (cell) $\nu(S_i)$, $S_i \in S$, 其中 S_i 为基点 (site). 并满足以下特性:

- (1) 每个区域 $\nu(S_i)$ 包含并仅包含 1 个基点 S_i ;
- (2) 特征空间 X 内任一点 $p \in \nu(S_i)$, 点 p 与所有基点的位置关系满足 $\text{dist}(p, S_i) \leq \text{dist}(p, S_j)$, 其中 $S_i, S_j \in S$;
- (3) 所有区域的并集构成基点集 S 在特征空间内唯一的维诺图 $\text{Vor}(S)$.

因此, 若在任一点 S_i 所对应的区域 $\nu(S_i)$ 内产生检测器 $\langle c, r \rangle$, 则 S_i 是 S 中距离检测器中心 c 最近的自体之一. 从而避免了传统 NSA 中耗时的查找最邻近自体过程.

2.1.2 MHC-I 类检测器生成

MHC-NSA 在维诺图 $\text{Vor}(S)$ 中 3 个或 3 个以上区域的交点处生成 MHC-I 类检测器, 表示为 $\langle c_1, r_1 \rangle$. 故 MHC-I 类检测器中心 c_1 为区域顶点集 $\text{Vet}(S_i)$ 中重复 3 次以上的元素. 即

$$c_1 = \{x | x \in \text{Vet}(S_p) \cap \text{Vet}(S_q) \cap \text{Vet}(S_t), p \neq q \neq t\}, \quad (1)$$

其中 S_p, S_q 和 S_t 为基点集中任意 3 个元素, 且由维诺图的性质 (2) 可知, S_p, S_q 和 S_t 同为距离 c_1 最临近的基点. 由自体耐受原则, MHC-I 类检测器的检测半径 r_1 为

$$r_1 = \text{dist}(c_1, S_i) - r_s, \quad i \in \{p \cup q \cup t\}, \quad (2)$$

其中 r_s 为自体半径. 为避免因生成检测范围极小的检测器所引起的过拟合现象, 本文引入最小检测半径 θ . 当某一 MHC-I 类检测器的检测半径 $r_1 < \theta$, 不生成此检测器. 但若 θ 过大, 将使大量的检测器无法生成, 从而导致欠拟合现象. 因此建议 θ 取值不宜过大和过小, 在实际应用中, θ 的取值建议不超过 0.1. 4.1 小节将进一步讨论 θ 取值对算法性能的影响.

2.1.3 MHC-II 类检测器生成

MHC-NSA 选择维诺图 $\text{Vor}(S)$ 中两个相邻区域的共有边与单位超立方体 $[0, 1]^d$ 的交点处生成 MHC-II 类检测器, 表示为 $\langle c_2, r_2 \rangle$. 故 MHC-II 类检测器中心 c_2 为区域顶点集 $\text{Vet}(S_i)$ 中仅重复两次的元素. 即

$$c_2 = \{x | x \in \text{Vet}(S_p) \cap \text{Vet}(S_q), p \neq q\}, \quad (3)$$

其中 S_p 和 S_q 为基点集中任意两个元素, 且同为离 c_2 最临近的基点. MHC-II 类检测器的检测半径 r_2 可计算为

$$r_2 = \text{dist}(c_2, S_i) - r_s, \quad i \in \{p \cup q\}, \quad (4)$$

其中 r_s 为自体半径. 同样引入最小检测半径 θ 以避免过拟合.

检测器快速生成阶段的算法关键步骤伪代码见算法 1.

Algorithm 1 To calculate MHC-I detectors and MHC-II detectors

Input: Set of self samples S , Self radius r_s , Minimum detector radius θ ;

Output: Set of MHC-I detectors and MHC-II detectors D .

```

1:  $S \leftarrow \text{normalize } S \text{ into } [0, 1]^d$ ;
2:  $\text{Vor}(S) \leftarrow \text{construct voronoi diagram by } S$ ;
3:  $\text{Vet}(S_i) \leftarrow \text{get all vertex in } \text{Vor}(S)$ ;
4:  $\text{Vet}(S_j) \leftarrow \text{get duplicate samples in } \text{Vet}(S_i)$ ;
5: for  $\text{Vet}(S_k) \in \text{Vet}(S_j)$  do
6:    $r = \text{dist}(\text{Vet}(S_k), S_k)$ ;
7:   if  $r > \theta$  then
8:      $D \leftarrow \langle \text{Vet}(S_k), r \rangle$ ;
9:   end if
10: end for
11: return  $D$ .
```

2.2 孔洞修复阶段

2.2.1 孔洞定位

在检测器快速生成阶段, 由自体集 S 生成的维诺图 $\text{Vor}(S)$ 将特征空间 X 划分为互不覆盖的区域, 故在特征空间内的所有孔洞是由每个区域内的孔洞所组成. 以平面空间为例, 依据自体半径的大小及自体与区域内相邻顶点的位置关系, 孔洞的分布可分为以下几类, 见图 2.

如图 2(c) 和 (d) 所示, 基点 S_2 向区域边 cd 上的投影点不在边 cd 上, 此时孔洞仅有 1 处, 紧邻自体空间边缘, 但范围较小. 图 2(b) 中, 基点 S_1 向区域边 ab 上的投影点在边 ab 上, 但基点 S_1 和投影

图 2 (网络版彩图) 某区域内部分孔洞分布示意. S_1, S_2 为自体元素. 点 a, b, c, d 均为所在区域的顶点. 以 S_1, S_2 为中心的纯色圆代表自体区域. 以点 a, b, c, d 为中心的条纹阴影圆代表 MHC-I 类检测器或 MHC-II 类检测器

Figure 2 (Color online) The distribution of holes. S_1 and S_2 are self samples. The points a, b, c and d are vertices in the cell. The pure color circle centered on S_1 and S_2 represents the self region. The fringe shadow circle centered on point a, b, c and d represents the MHC-I detector or the MHC-II detector. The projection of S_1 on line ab is located in line segment ab , and the distance between S_1 and line ab is (a) greater than self radius r_s , and (b) less than self radius r_s . The projection of S_2 on line cd is not located in line segment cd , and the distance between S_2 and line cd is (c) greater than self radius r_s , and (d) less than self radius r_s .

点的距离小于自体半径, 此时孔洞范围有 2 处, 范围也较小. 如果在图 2(b)~(d) 3 种情况下新产生检测器可能面临两个弊端: (1) 新产生的检测器的有效检测范围较小, 效率较低; (2) 可能造成过拟合. 图 2(a) 中, 基点 S_1 向区域边 ab 上的投影点在边 ab 上, 且基点 S_1 和投影点的距离大于自体半径. 此时孔洞范围较大, 可能引起较严重的非自体漏检, 需要进行孔洞修复.

定理1 在平面空间中, 检测器快速生成阶段所产生孔洞面积占整体特征空间总面积的比率 $\varphi \leq 21.46\%$, 当且仅当基点与任意两顶点的夹角均为 90° , 且自体半径为基点与检测器中心距离的一半时取最大值.

证明 由上文, 图 2(a) 中孔洞范围远大于图 2(b)~(d) 的情形, 因此 φ 的最大值仅讨论在图 2(a) 中基点与区域顶点所成三角形中孔洞面积占整个三角形面积的比率 φ_Δ .

如图 3 所示, S 为任一基点, A 和 B 为同一区域内两相邻顶点. 以 AB 连线作为 X 轴. 以 AB 的法向量, 且通过 S 点作为 Y 轴建立坐标系. 故

$$\varphi_\Delta = \frac{S_\Delta - S_1 - S_2}{S_\Delta} = 1 - \frac{S_1 + S_2}{S_\Delta}, \quad (5)$$

其中 S_1 为自体区域在 $\triangle oSA$ 中的范围, S_2 为检测器中心向量为 A 的检测器在 $\triangle oSA$ 中的检测范围, S_Δ 为 $\triangle oSA$ 的面积.

图 3 (网络版彩图) 孔洞局部位置分解. 以点 S 为中心的扇形为自体区域. 以点 A, B 为中心的扇形为某 MHC-I 类检测器或 MHC-II 类检测器的检测范围. 空白区域为检测器无法覆盖的孔洞区域

Figure 3 (Color online) Part of the hole. The sector with a point S as the center is a self region. The sector with a point A or B as the center is an MHC-I or MHC-II detector region. The blank area is the hole

在 $\triangle oSA$ 中, 记 $\angle oSA$ 为 α , 则 $\alpha \in (0, \pi/2)$. 可得 S 点坐标为 $(0, \cos \alpha)$, A 点坐标为 $(\sin \alpha, 0)$. 令 SA 的距离为单位 1, 自体半径为 r . 由式 (2) 和 (4) 可知, 检测器中心向量为 A 的检测器检测半径为 $1-r$. 由图 2(a) 易推出, $r \in (1 - \sin \alpha, \cos \alpha)$. 故 $S_{\Delta} = \frac{1}{2} \sin \alpha \cos \alpha$, $S_1 = \frac{1}{2} \alpha r^2$, $S_2 = \frac{1}{2} (\frac{\pi}{2} - \alpha) (1-r)^2$. 代入式 (5) 中, 可得

$$\varphi_{\Delta} = 1 - \frac{\alpha r^2 + (\frac{\pi}{2} - \alpha) (1-r)^2}{\sin \alpha \cos \alpha}.$$

令 $F(r, \alpha) = \frac{\alpha r^2 + (\frac{\pi}{2} - \alpha) (1-r)^2}{\sin \alpha \cos \alpha}$. 由于 $S_{\Delta} \neq 0$, 故 $F(r, \alpha)$ 在定义域内连续. 故

$$\frac{\partial F}{\partial r} = \frac{\pi r - \pi + 2\alpha}{\frac{1}{2} \sin 2\alpha}, \quad \frac{\partial F}{\partial \alpha} = \frac{\frac{1}{2} (2r - 1) \sin 2\alpha - [\frac{\pi}{2} (1-r)^2 + \alpha (2r - 1)] \cos 2\alpha}{(\frac{1}{2} \sin 2\alpha)^2}.$$

解方程组

$$\begin{cases} \frac{\partial F}{\partial r} = 0, \\ \frac{\partial F}{\partial \alpha} = 0, \end{cases}$$

可得在 (r, α) 定义域内驻点 $(\frac{1}{2}, \frac{\pi}{4})$. 令

$$\frac{\partial}{\partial r} \left(\frac{\partial F}{\partial r} \right) \bigg|_{\substack{r=1/2 \\ \alpha=\pi/4}} = 2\pi = X, \quad \frac{\partial}{\partial \alpha} \left(\frac{\partial F}{\partial r} \right) \bigg|_{\substack{r=1/2 \\ \alpha=\pi/4}} = 2 = Y, \quad \frac{\partial}{\partial \alpha} \left(\frac{\partial F}{\partial \alpha} \right) \bigg|_{\substack{r=1/2 \\ \alpha=\pi/4}} = \pi = Z.$$

由判断极值点得充分条件可知: $X \cdot Z - Y^2 = 2\pi^2 - 4 > 0$, 且 $X = 2\pi > 0$. 故 (r, α) 取定义域内一驻点 $(\frac{1}{2}, \frac{\pi}{4})$ 时, $F(r, \alpha)$ 取极小值. 此时, $\angle BSA = 2\angle oSA = 90^\circ$, $r_s = \frac{1}{2} \text{dist}(S, A)$, $\varphi_{\Delta} \leq 1 - F(\frac{1}{2}, \frac{\pi}{4}) = 1 - \frac{\pi}{4} \approx 0.2146 = 21.46\%$.

2.2.2 孔洞修复检测器生成

基于以上分析, 本文认为需要对以下情况所产生的孔洞进行修复. 即基点 S_i 向所关联区域 $\nu(S_i)$ 任一边 ab 上的投影点在边 ab 上, 且基点 S_i 和投影点 p 的距离大于自体半径 r_s .

定义1 (孔洞修复检测器) 该类检测器可表示为 $\langle c_{\text{hole}}, r_{\text{hole}} \rangle$, 其中 c_{hole} 为孔洞修复检测器的检测器中心向量, 位于基点 S_i 在所关联区域 $\nu(S_i)$ 边上投影. r_{hole} 为孔洞修复检测器的检测半径, 需满足

$$r_{\text{hole}} = \text{dist}(S_i, p) - r_s, \quad (6)$$

其中 p 为基点 S_i 在所关联区域 $\nu(S_i)$ 边上的投影. 同样引入最小检测半径 θ 以避免过拟合.

孔洞修复检测器生成算法的关键步骤伪代码如算法 2 所示.

Algorithm 2 Calculate the hole improvement detectors

Input: Set of cells V , Self radius r_s , Minimum detector radius θ ;

Output: Set of the hole improvement detectors D .

```

1: base  $\leftarrow$  get the base point in  $V$ ;
2:  $E \leftarrow$  get all polyhedron in  $V$ ;
3: for  $e \in E$  do
4:    $p \leftarrow$  get the projection of base in  $e$ ;
5:   if  $p \in e$  then
6:      $r = \text{dist}(p, \text{base}) - r_s$ ;
7:     if  $r > \theta$  then
8:        $D \leftarrow \langle p, r \rangle$ ;
9:     end if
10:  end if
11: end for
12: return  $D$ .
```

3 算法理论分析

定理2 在平面空间中, MHC-NSA 算法所产生的孔洞修复检测器可将孔洞面积占整体特征空间总面积的最大比率从 21.46% 降低到 7.98%, 降比 62.8%.

证明 如图 3 所示, 可知孔洞修复检测器中心向量位于原点 o . 令孔洞修复检测器在 $\triangle oSA$ 中的检测范围为 S_3 , 则

$$\varphi_{\Delta} = \frac{S_{\Delta} - S_1 - S_2 - S_3}{S_{\Delta}} = 1 - \frac{S_1 + S_2}{S_{\Delta}} - \frac{S_3}{S_{\Delta}}. \quad (7)$$

根据定理 1, 当孔洞占比最大时,

$$S_{\Delta} = \frac{1}{2} \sin \alpha \cos \alpha \bigg|_{\alpha=\pi/4}^{r=1/2} = \frac{1}{4}, \quad S_1 = \frac{1}{2} \alpha r^2 \bigg|_{\alpha=\pi/4}^{r=1/2} = \frac{\pi}{32}, \quad S_2 = \frac{1}{2} \left(\frac{\pi}{2} - \alpha \right) \cdot (1-r)^2 \bigg|_{\alpha=\pi/4}^{r=1/2} = \frac{\pi}{32}. \quad (8)$$

由式 (6) 知

$$S_3 = \frac{1}{4} \cdot \pi \cdot r_{\text{hole}}^2, \quad r_{\text{hole}} = \text{dist}(S, o) - r_s = \cos \alpha - r \bigg|_{\alpha=\pi/4}^{r=1/2} = \left(\frac{\sqrt{2}}{2} - \frac{1}{2} \right). \quad (9)$$

将式 (8) 和 (9) 代入式 (7), 得

$$\varphi_{\Delta} = 1 - \frac{\pi}{4} \cdot \left[1 + \left(\sqrt{2} - 1 \right)^2 \right] \approx 0.0798 = 7.98\%.$$

故孔洞修复检测器可将孔洞面积占整体特征空间总面积的最大降比为 $(21.46\% - 7.98\%) / 21.46\% = 62.8\%$.

定理3 MHC-NSA 算法所产生的 MHC-I 类检测器, MHC-II 类检测器和孔洞修复检测器均满足自体耐受过程.

证明 为方便证明, 记此不满足自体耐受的某一 MHC-I 类检测器, MHC-II 类检测器或孔洞修复检测器为 $d = \langle c, r \rangle$, 其检测中心向量为 c , 检测半径为 r . NSA 算法的自体耐受过程可表示为

$$f_{\text{nsa}}(x) = \begin{cases} 1, & \text{iff } \forall s \in S : \text{dist}(x, s) > r_s, \\ 0, & \text{otherwise,} \end{cases} \quad (10)$$

其中 $f_{\text{nsa}}(x)$ 值为 1 表示检测器 x 通过自体耐受, x 表示未成熟检测器, S 表示自体集, $\text{dist}()$ 表示亲和度, 本文使用欧氏距离进行计算.

此处使用反证法. 假设存在某一 MHC-I 类检测器, MHC-II 类检测器或孔洞修复检测器 d 不满足自体耐受过程. 即存在某一自体 s 在检测器 d 的检测范围内. 由式 (10) 得

$$\exists s \in S \Rightarrow \text{dist}(c, s) < r. \quad (11)$$

由式 (2), (4) 和 (6) 知

$$r = \text{dist}(c, s') - r_s, \quad (12)$$

其中 s' 为距离检测器 d 最近的基点. 将式 (12) 代入 (11), 得

$$\exists s \in S \Rightarrow \text{dist}(c, s') > \text{dist}(c, s) + r_s, \quad (13)$$

其中 r_s 非负, 式 (13) 与维诺图的特性 (2) 相矛盾. 假设不成立. 故 MHC-NSA 算法所产生的 MHC-I 类检测器, MHC-II 类检测器和孔洞修复检测器均满足自体耐受过程.

定理4 MHC-NSA 算法的时间复杂度为 $O(N_S \log N_S + N_S^{\lceil d/2 \rceil})$, 空间复杂度为 $O(N_S^{\lceil d/2 \rceil})$ 其中 N_S 为自体集数量, d 为特征空间维度.

证明 MHC-NSA 算法由两个阶段组成, 以下将分别讨论每个阶段的时空复杂度.

检测器快速生成阶段: 在特征空间划分步骤, 主要算力消耗于以给定的 N_S 个自体元素构造维诺图. 文献 [19] 给出在 d 维空间中, n 个基点所对应的维诺图可以使用增量法 (incremental method) 在时间复杂度 $O(n \log n + n^{\lceil d/2 \rceil})$ 内构造出来, 且存储维诺图顶点、边及其他元素的空间复杂度为 $O(n^{\lceil d/2 \rceil})$. 因此, N_S 个自体元素在特征空间划分步骤的时间复杂度为 $O(N_S \log N_S + N_S^{\lceil d/2 \rceil})$, 空间复杂度为 $O(N_S^{\lceil d/2 \rceil})$. 在生成 MHC-I 和 MHC-II 类检测器步骤, 训练单个检测器的时空复杂度均为 $O(1)$, 且生成 MHC-I 和 MHC-II 类检测器的数量不超过维诺图顶点和边的总数, 因此可认为生成 MHC-I 和 MHC-II 类检测器的时空复杂度最坏情况下仍小于特征空间划分的时空复杂度. 因此, 检测器快速生成阶段的时间复杂度为 $O(N_S \log N_S + N_S^{\lceil d/2 \rceil})$, 空间复杂度为 $O(N_S^{\lceil d/2 \rceil})$.

孔洞修复阶段: 文献 [20] 给出 $d > 2$ 维空间中 n 个基点所对应的维诺图的总边数为 $(3n - 6) + (d - 2) \cdot \binom{n}{2}$. 故 $d > 2$ 维空间中, 以给定的 N_S 个自体元素构造维诺图的总边数 k 为 $(3N_S - 6) + (d - 2) \cdot \binom{N_S}{2}$. 由于孔洞修复检测器的中心向量位于维诺图的边上, 在最坏情况下, 孔洞修复检测器需要在每条边上生成, 且训练单个孔洞修复检测器的时空复杂度均为 $O(1)$. 则孔洞修复阶段的时空复杂度均为 $O(k)$, 即 $(3N_S - 6) + (d - 2) \cdot \binom{N_S}{2}$.

综合以上可知, 孔洞修复阶段在最坏情况下时空复杂度远小于检测器快速生成阶段. 故 MHC-NSA 算法的时间复杂度为 $O(N_S \log N_S + N_S^{\lceil d/2 \rceil})$, 空间复杂度为 $O(N_S^{\lceil d/2 \rceil})$.

表 1 给出主要 NSA 算法的时间复杂度对比. 其中 P_m 表示检测器识别抗原成功的概率, P_f 表示检测器识别失败的概率, N_S 表示自体集数量, d 表示维度. 由表 1^[2,6,7] 中可见传统 NSA 算法 (NNSA, RNSA 和 V-Detector) 的时间复杂度随自体数量增长成指数阶增长, MHC-NSA 去除了传统 NSA 中耗时的查找最邻近自体过程, 时间复杂度降低到多项式阶.

表 1 主要 NSA 算法时间复杂度对比

Table 1 Comparison of time complexity

	Time complexity	Comment
NNSA [2]	$O(-\frac{\ln P_f \cdot N_S}{P_m(1-P_m)^{N_S}})$	Exponential level
RNSA [7]	$O(\frac{ D \cdot N_S}{(1-P_m)^{N_S}})$	Exponential level
V-Detector [6]	$O(\frac{ D \cdot N_S}{(1-P_m)^{N_S}})$	Exponential level
MHC-NSA	$O(N_S \log N_S + N_S^{\lceil d/2 \rceil})$	Polynomial level

4 实验

本节通过实验对 MHC-NSA 算法进行讨论. MHC-NSA 算法部分实现代码引用开源计算几何工具包 MPT 3.0 [21]. 实验使用 2 个 NSA 研究领域通用的性能评价指标: 检测率 (detection rate, DR) 和误报率 (false alarm rate, FAR), 计算方法如下:

$$DR = \frac{TP}{TP + FN}, \quad FAR = \frac{FP}{FP + TN},$$

其中 TP, TN, FP 和 FN 分别代表检测器正确识别的非自体的数量、正确识别的自体的数量、错误识别的自体的数量和错误识别的非自体的数量.

4.1 参数选取对算法性能的影响

根据第 2 节可知, MHC-NSA 算法的参数包括自体集数量 N_S , 自体半径 r_s 和最小检测半径 θ . 为深入讨论这 3 个参数对算法性能的影响, 本小节通过著名人工免疫研究机构美国孟菲斯大学智能安全实验室提出 4 个 SDS 数据集进行实验分析: Intersection-mid, Pentagon-mid, Ring-mid, Triangle-mid¹⁾. 这 4 个数据集已被国际学术界普遍接受 [6, 7, 12, 22], 已成为 NSA 研究领域公认的数据集之一.

实验采用控制变量法分别讨论参数选取对算法性能的影响. 实验过程中自体集数量 N_S 的变化范围为 50~1000, 自体半径 r_s 的变化范围为 0.01~0.1, 最小检测半径 θ 的变化范围是 0.005~0.03. 实验分别在每个数据集的训练集中随机抽取 N_S 个元素进行训练, 使用对应测试集的全部元素进行测试, 每项实验均独立运行 20 次. 实验结果如图 4 所示.

图 4(a)~(c) 分别表示自体集数量 N_S 变化对 MHC-NSA 性能的影响. 实验结果图 4(b) 显示, 在其他参数相同的情况下, N_S 的增加将使误报率迅速收敛. 这是由于自体集数量较少时, 自体区域无法有效覆盖所有自体抗原, 部分自体抗原落入非自体区域, 被误识为非自体, 从而导致误报率偏高. 随着自体集数量增加, 自体区域将完整覆盖所有的自体抗原, 故误报率迅速收敛到 0. 此外, 实验结果图 4(c) 也证实了定理 4 的结论: 自体集数量 N_S 的增加引起训练时间上升. 因此在实际应用中, 对训练时间敏感的应用场景下可降低自体集数量, 而对误报敏感的场景可增加自体集数量.

图 4(d)~(f) 分别表示自体半径 r_s 变化对 MHC-NSA 性能的影响. 实验结果图 4(d) 和 (e) 显示, 在其他参数相同的情况下, 较小的自体半径将使 MHC-NSA 具备较高的检测率和误报率, 而较大的自体半径将使 MHC-NSA 的检测率和误报率均下降: 如 Pentagon-mid 数据集中, $0 < r_s < 0.02$; $95\% < DA$, $5\% < FAR$. $0.5 < r_s$; $DA < 90\%$, $FAR \approx 0$. 因此在实际应用中, 对异常样本敏感的场景可降低自体半径的取值, 而对误报敏感的场景可增加自体半径.

1) <http://ais.cs.memphis.edu/files/datasets/2DSyntheticData.zip>.

图 4 (网络版彩图) MHC-NSA 算法参数 N_S , r_s 和 θ 对算法性能影响的实验结果Figure 4 (Color online) The results of N_S (a)–(c), r_s (d)–(f) and θ (g)–(i) impact on the performance of MHC-NSA

图 4(g)~(i) 分别表示最小检测半径 θ 变化对 MHC-NSA 性能的影响. 实验结果图 4(i) 显示, 在其他参数相同的情况下, 较低的 θ 取值 ($\theta < 0.02$) 将使 MHC-NSA 产生更多的检测器, 但这些检测器不仅不能有效增加检测率 (如图 4(g)), 误报率反而更高 (如图 4(h)), 此时 MHC-NSA 算法出现过拟合现象. 而 θ 取值过大 ($\theta > 0.13$) 时, 生成的检测器数量迅速下降 (如图 4(i)), 且检测率也大幅降低 (如图 4(g)), 此时 MHC-NSA 算法出现欠拟合现象. 因此, 在实际应用中 θ 的取值需综合考虑上述两种问题. 如本实验中, θ 取 0.04 较为合适.

4.2 孔洞修复方式对比

为了直观展现 MHC-NSA 算法在孔洞修复方式上相比传统 NSA 的优势, 本小节采用一个由德国著名计算机免疫专家 Stibor 等^[8] 提出并广泛应用于后续研究^[6, 7, 12, 22] 的数据集. 数据集共有 9 个自体元素, 分布在 $[0, 1]^2$ 特征空间中, 如图 5 中深色圆. 实验对比算法选取典型 NSA 算法代表 RNSA,

图 5 (网络版彩图) 4 种 NSA 算法孔洞修复方式对比. 红色十字代表检测器中心, 白色区域代表检测范围, 深色区域为检测器无法覆盖的“孔洞”区域. (d) 中, 绿色虚线是以自体为基点产生的维诺图, 红色边缘的检测器为孔洞修复检测器

Figure 5 (Color online) Contrast of 4 NSAs for detector generation. The center of detectors are represented by red cross, and the range of detection is represented by the white area. The hole is represented by the dark area. In (d), the Voronoi diagram is represented by the green dotted line. The red edge detectors are the hole repair detectors. (a) RNSA, 500 detectors, DR = 92.46%; (b) V-Detector, 43 detectors, DR = 95.42%; (c) BIORV-NSA, 85 detectors, DR = 95.44%; (d) MHC-NSA, 24 detectors, DR = 99.78%

V-Detector 和 BIORV-NSA. 实验参数参照文献 [6~8, 12] 设定如下: 所有 NSA 算法的自体半径 r_s 均设为 0.05 以保证实验公平. RNSA, V-Detector 和 BIORV-NSA 的最大检测器数量分别为 500, 500, 85. V-Detector 的期望覆盖率为 95%. BIORV-NSA 的抗体耐受值和自体边缘耐受值分别为 0.8 和 1.2. MHC-NSA 的最小检测半径 θ 设为 0.005. 本小节实验中, 所有自体元素均被用作自体集, 此外在非自体空间随机产生 5000 个点为非自体.

图 5 直观展示了目前 NSA 孔洞修复的 4 种典型方法. RNSA: 图 5(a) 随机生成的检测器互相覆盖程度较高, 即使生成 500 个检测器, 检测率仅能达到 92.46%. V-Detector: 图 5(b) 将检测半径改进为可变值, 并增加了与成熟检测器耐受过程. 为达到指定期望覆盖率, V-Detector 在淘汰大量未成熟检测器的基础上 (共淘汰未成熟检测器 213 个), 生成大量检测半径极小的检测器, 但孔洞范围仍较大. BIORV-NSA: 图 5(c) 引入抗体耐受值和自体边缘耐受值的概念, 允许检测器“覆盖”部分自体区域, 但这种方式可能引起误报. MHC-NSA: 图 5(d) 模拟 MHC 修复生物免疫系统孔洞过程, 针对孔洞进行定向修复, 从而可在生成较少检测器的同时, 达到较高的检测率. MHC-NSA 的生成检测器数量相比 RNSA, V-Detector 和 BIORV-NSA 分别减少 95.2%, 44.18% 和 71.76%, 检测率分别提高 7.92%, 4.57% 和 4.35%.

表 2 Balance Scale 数据集仿真结果^{a)}
Table 2 The results on Balance Scale dataset

	DR (%)		FAR (%)		Generated detectors		Eliminated detectors		Training time (s)	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
RNSA	55.18	1.56	1.43	1.76	1500.00	0	2700.45	171.09	6.83	0.29
V-Detector	64.98	1.84	4.18	2.04	1485.95	62.83	3769.75	288.11	88.52	7.66
BIORV-NSA	79.61	1.60	4.18	2.14	1500.00	0	230.30	26.07	43.04	0.06
MHC-NSA	93.57	0.56	4.49	2.15	366.60	24.67	60.10	7.57	3.16	0.76

a) MHC-NSA 相比 RNSA, V-Detector 和 BIORV-NSA 算法, 在检测器训练时间大幅降低 53.73%, 96.43% 和 92.66% 的前提下, 检测率分别提高 69.57%, 44% 和 17.54%.

4.3 算法性能验证

为验证 MHC-NSA 算法在真实应用场景下的性能, 本小节在 UCI 中的 Balance Scale 数据集²⁾下进行仿真. Balance Scale 数据集由美国加州大学欧文分校 (University of California, Irvine) Tim Hume 提出, 数据来源于心理学实验报告. 数据集为 5 维共 625 条数据, 其中标签为平衡的数据 49 条占比 7.84%, 左倾类和右倾类的数据均为 288 条, 分别占 46.08%.

实验将标签为平衡的数据选择为自体, 其余两类选择为非自体. 实验在自体集中随机选取 45 个自体为训练集, 选择全部数据集为测试集, 在相同随机种子的前提下, 重复实验 20 次. 实验对比算法为 RNSA, V-Detector 和 BIORV-NSA. 实验相关参数参照文献 [6, 7, 12] 设置如下: 所有 NSA 算法的自体半径 r_s 均设为 0.2 以保证实验公平. RNSA, V-Detector 和 BIORV-NSA 的最大检测器数量均为 1500. V-Detector 的期望覆盖率为 95%. BIORV-NSA 的抗体耐受值和自体边缘耐受值分别为 0.8 和 1.2. MHC-NSA 的最小检测半径 θ 设为 0.001.

从表 2 的实验结果来看, 由于 RNSA 算法采用固定半径检测器, 且未考虑检测器间的相互覆盖情况, 因此难以解决孔洞问题, 检测率仅 55.18%. V-Detector 通过随机生成变半径的检测器降低孔洞范围, 但这种随机没有考虑孔洞的分布, 具有较大的盲目性. 这导致 V-Detector 耗费大量的时间 (同比最高的 88.52 s) 淘汰随机产生的未成熟检测器 (高达 3769 个). BIORV-NSA 通过引入自体边缘耐受值和抗体耐受值的概念进一步降低孔洞范围, 但检测器训练过程并未改变随机产生检测器的盲目性. MHC-NSA 通过增加孔洞修复检测器, 在指定位置修复孔洞, 从而提高检测率. 从表 2 中可见, MHC-NSA 相比 RNSA, V-Detector 和 BIORV-NSA 算法, 在检测器训练时间大幅降低 53.73%, 96.43% 和 92.66% 的前提下, 检测率分别提高 69.57%, 44% 和 17.54%.

4.4 应用: 网络入侵检测

网络入侵检测是网络安全领域重要的主动防御手段, 然而在网络入侵检测的实际工程应用中, 经常面临着网络攻击手段多变, 难以获取新攻击手段先验知识的困境^[23]. MHC-NSA 算法通过模拟免疫细胞在骨髓中的生长过程, 仅使用正常样本训练检测器, 生成的检测器可用于检测识别网络空间中的所有攻击, 包括未知攻击, 因此在网络入侵检测等领域具备广阔的应用前景. 为了进一步证实 MHC-NSA 算法在工程应用领域的有效性, 本小节将 MHC-NSA 算法与 3 种实际工程中广受认可的异常检测算法 (One-Class SVM, Isolation Forest 和 LOF) 在网络入侵检测领域进行讨论.

2) <http://archive.ics.uci.edu/ml/datasets/balance+scale>.

表 3 KDD CUP 99 数据集仿真参数

Table 3 The simulation parameters in KDD CUP 99 dataset

	MHC-NSA			One-Class SVM			Isolation Forest		LOF	
	N_S	r_s	θ	Kernel	ν	γ	Max_samples	Contamination	k	Contamination
HTTP	300	0.2	0.001	RBF	0.004	0.33	256	0.004	20	0.004
FTP	100	0.05	0.001	RBF	0.0772	0.33	256	0.0772	20	0.0772
FTP-Data	300	0.004	0.0001	RBF	0.0237	0.33	256	0.0237	20	0.0237

表 4 KDD CUP 99 数据集仿真结果^{a)}

Table 4 The results on KDD CUP 99 dataset

	MHC-NSA		One-Class SVM		Isolation Forest		LOF	
	DR (%)	FAR (%)	DR (%)	FAR (%)	DR (%)	FAR (%)	DR (%)	FAR (%)
HTTP	99.88	0.40	99.02	0.39	99.74	89.14	99.43	51.79
FTP	99.92	1.45	91.60	61.64	90.70	0.27	91.94	0.00
FTP-Data	94.56	3.23	97.49	84.52	97.55	85.00	97.99	54.93
Mean	98.12	1.69	96.03	48.85	96.00	58.14	96.45	35.57

a) MHC-NSA 算法相比 One-Class SVM, Isolation Forest 和 LOF, 误报率分别平均降低 96.54%, 97.09% 和 95.25%, 检测率分别平均提高 2.18%, 2.21% 和 1.73%.

实验数据集选择网络入侵检测领域著名的 KDD CUP 99 数据集³⁾. KDD CUP 99 源于美国国防部 DARPA 在 MIT 林肯实验室采集的真实网络入侵数据. 然而 KDD CUP 99 中攻击数据包高达 80.1%, 这与实际工程中面临的应用场景有所差别. 为此, 本小节参照目前对该数据集主流的预处理方法^[24~26], 将 KDD CUP 99 按照协议分为更符合实际应用场景的 HTTP, FTP 和 FTP-Data 3 个主要的数据子集. 其中 HTTP 数据集共有数据 567498 条, 攻击数据占比 (0.4%); FTP 数据集共有数据 4091 条, 攻击数据占比 (7.72%); FTP-Data 数据集共有数据 30464 条, 攻击数据占比 (2.37%). 实验共运行 20 次, 对比算法使用工程领域广受认可的 Python 机器学习库 scikit-learn 实现, 其参数参照 scikit-learn 中的建议值⁴⁾, 详细设定见表 3.

实际应用中, 误报率高是制约网络入侵检测进一步推广的关键^[23]. 从表 4 所示的实验结果来看, MHC-NSA 算法有效解决了网络入侵检测误报率高的问题, 相比 One-Class SVM, Isolation Forest 和 LOF, 误报率分别平均降低 96.54%, 97.09% 和 95.25%, 检测率分别提高 2.18%, 2.21% 和 1.73%. 这是由于 MHC-NSA 算法所生成的检测器均满足自体耐受过程, 可有效降低检测器误识自体的概率, 从而降低误报率, 且 MHC-NSA 算法改进了传统 NSA 算法存在的孔洞问题, 进一步提高检测率.

此外, 3 种对比算法保持较高检测率的前提条件是需要准确指定攻击样本的比例. 如: 本实验按照算法参数设置建议, 将 One-Class SVM 算法中的 ν , Isolation Forest 算法和 LOF 算法中的 contamination 均设定为数据集中攻击样本总占比. 而实际应用中, 面临复杂的网络环境且缺乏攻击手段先验知识的前提下, 这个比例通常难以确定, 这将进一步降低传统异常检测算法在实际应用中的可用性. 而 MHC-NSA 算法无此限制.

3) <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.

4) https://scikit-learn.org/stable/modules/outlier_detection.html.

5 结论

传统 NSA 算法未考虑孔洞的分布, 在特征空间内通过完全随机的方式盲目生成检测器以修复孔洞, 导致孔洞修复效果不佳, 并且淘汰无效的检测器也异常耗时. 针对这些问题, 本文受 MHC 修复生物免疫系统孔洞过程启发, 提出一种基于免疫 MHC 的否定选择算法孔洞修复方法 MHC-NSA. MHC-NSA 算法模拟 MHC 针对孔洞所具有的特殊形态, 对所产生的孔洞位置进行定位, 并限定该位置生成孔洞修复检测器, 从而提升孔洞修复效果. 理论分析和实验结果显示, MHC-NSA 算法相较现有典型 NSA 算法在孔洞修复效果和效率方面具有明显的改进.

参考文献

- 1 Castro L R D, Timmis J. Artificial Immune Systems: A New Computational Intelligence Paradigm. New York: Springer, 2002. 368
- 2 Forrest S, Perelson A S, Allen L, et al. Self-nonself discrimination in a computer. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, 1994. 202–212
- 3 Klarreich E. Inspired by immunity. *Nature*, 2002, 415: 468–470
- 4 Balhrop J, Forrest S, Newman M E J, et al. Technological networks and the spread of computer viruses. *Science*, 2004, 304: 527–529
- 5 Ji Z, Dasgupta D. Revisiting negative selection algorithms. *Evolutionary Comput*, 2007, 15: 223–251
- 6 Ji Z, Dasgupta D. V-detector: an efficient negative selection algorithm with “probably adequate” detector coverage. *Inf Sci*, 2009, 179: 1390–1406
- 7 González F A, Dasgupta D, Niño L F. A randomized real-valued negative selection algorithm. In: Proceedings of the 2nd International Conference on Artificial Immune Systems, Edinburgh, 2003. 261–272
- 8 Stibor T, Timmis J, Eckert C. A comparative study of real-valued negative selection to statistical anomaly detection techniques. In: Proceedings of International Conference on Artificial Immune Systems, Banff, 2005. 262–275
- 9 Zhang H, Wu L F, Zhang Y S, et al. An algorithm of r -adjustable negative selection algorithm and its simulation analysis. *Chin J Comput*, 2005, 28: 1614–1619 [张衡, 吴礼发, 张毓森, 等. 一种 r 可变阴性选择算法及其仿真分析. *计算机学报*, 2005, 28: 1614–1619]
- 10 He S, Luo W J, Wang X F. A negative selection algorithm with the variable length detector. *J Softw*, 2007, 18: 1361–1368 [何申, 罗文坚, 王煦法. 一种检测器长度可变的非选择算法. *软件学报*, 2007, 18: 1361–1368]
- 11 Idris I, Selamat A, Nguyen N T, et al. A combined negative selection algorithm-particle swarm optimization for an email spam detection system. *Eng Appl Artif Intell*, 2015, 39: 33–44
- 12 Cui L, Pi D C, Chen C M. BIORV-NSA: bidirectional inhibition optimization r -variable negative selection algorithm and its application. *Appl Soft Comput*, 2015, 32: 544–552
- 13 Gong M G, Zhang J, Ma J J, et al. An efficient negative selection algorithm with further training for anomaly detection. *Knowl-Based Syst*, 2012, 30: 185–191
- 14 Fouladvand S, Osareh A, Shadgar B, et al. DENSA: an effective negative selection algorithm with flexible boundaries for self-space and dynamic number of detectors. *Eng Appl Artif Intell*, 2017, 62: 359–372
- 15 Li D, Liu S L, Zhang H L. Negative selection algorithm with constant detectors for anomaly detection. *Appl Soft Comput*, 2015, 36: 618–632
- 16 Ljunggren H G, Kärre K. In search of the ‘missing self’: MHC molecules and NK cell recognition. *Immunol Today*, 1990, 11: 237–244
- 17 Yates A J. Theories and quantification of thymic selection. *Front Immunol*, 2014, 5: 1–15
- 18 Carpenter A C, Bosselut R. Decision checkpoints in the thymus. *Nat Immunol*, 2010, 11: 666–673
- 19 de Berg M. Computational Geometry: Algorithms and Applications. Berlin: Springer, 2008
- 20 Klee V. On the complexity of d -dimensional Voronoi diagrams. *Arch Math*, 1980, 34: 75–80
- 21 Herceg M, Kvasnica M, Jones C, et al. Multi-parametric toolbox 3.0. In: Proceedings of the European Control Conference, Zurich, 2013. 502–510
- 22 Silva G C, Caminhas W M, Palhares R M. Artificial immune systems applied to fault detection and isolation: a brief review of immune response-based approaches and a case study. *Appl Soft Comput*, 2017, 57: 118–131
- 23 Yu Z, Tsai J P. Intrusion Detection: A Machine Learning Approach. London: Imperial College Press, 2011

- 24 Yamanishi K, Takeuchi J-I, Williams G, et al. On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. In: Proceedings of the 6th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2000. 320–324
- 25 Liu F T, Ting K M, Zhou Z. Isolation forest. In: Proceedings of 2008 8th IEEE International Conference on Data Mining, Oakland, 2008. 413–422
- 26 Ting K M, Zhou G-T, Liu F T, et al. Mass estimation and its applications. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2010. 989–998

A negative selection algorithm hole improvement method based on MHC

Fangdong ZHU¹, Tao LI^{2*} & Jin YANG²

1. College of Computer Science, Sichuan University, Chengdu 610065, China;

2. College of Cybersecurity, Sichuan University, Chengdu 610065, China

* Corresponding author. E-mail: litao@scu.edu.cn

Abstract The negative selection algorithm (NSA) is the key algorithm of the artificial immune system. The hole is an important factor that causes low detection rates of NSAs. Traditional NSAs do not consider hole distribution. To eliminate holes, detectors are randomly generated in the feature space; however, this approach is ineffective, and eliminating invalid detectors is also time consuming. The hole problem also exists in the biological immune system, in which the MHC molecules are used to handle the hole problem. Inspired by the function of MHC, a hole improvement method, namely, the MHC-NSA method, is proposed. First, the feature space is divided by Voronoi, and two types of detectors are generated at two points in Voronoi. Second, the hole improvement detectors are directly generated at the holes by positioning the holes. Theoretical analysis shows that the hole improvement detectors can reduce the highest percentage of holes by 62.8%. Moreover, relative to traditional NSAs, the time complexity of MHC-NSA decreases from the exponential level to the polynomial level. Experiments on the UCI dataset show that compared with RNSA, V-Detector, and BIORV-NSA, the training time of MHC-NSA is reduced by 53.73%, 96.43%, and 92.66% and the detection rate of MHC-NSA increases by 69.57%, 44%, and 17.54%, respectively.

Keywords AIS, MHC, NSA, Holes

Fangdong ZHU was born in 1984. At present, he is pursuing his Ph.D. degree at the College of Computer Science, Sichuan University, Chengdu, China. His main research interests include artificial immune system, cybersecurity security, and blockchain.

Tao LI was born in 1965. He received his Ph.D. degree in computer science from University of Electronic Science and Technology of China in 1994. At present, he is a professor at the College of Cybersecurity at Sichuan University, China. His current research interests are cybersecurity security, artificial immune theory, and disaster recovery application.

Jin YANG was born in 1980. He received his Ph.D. degree in computer science from Sichuan University in 2007. Currently, he is an associate researcher at the College of Cybersecurity, Sichuan University, China. His main research interests include network security, knowledge discovery, and expert systems.