一种采用边界检测器的实值否定选择算法

王大伟 张风斌
(哈尔滨理工大学计算机科学与技术学院 哈尔滨 150080)

摘 要 针对实值否定选择算法中由边界困境问题引发的在自体与非自体区域边界产生漏洞的现象,提出了一种采用边界检测器的实值否定选择算法。该算法在边界上生成具有一定侵略性的边界检测器,通过边界阈值控制的边界检测器不仅能够有效地减少边界上的漏洞,还能探明自体与非自体区域边界。使用人工数据和 MIT Darpa 1998 离线数据对算法进行了测试,结果表明尽管新方法具有较高的最小误报率,但在误报率相同的情况下,有更高的检测率。

关键词 人工免疫,否定选择算法,边界困境,漏洞
中图法分类号 TP274.5 **文献标识码** A

Real-valued Negative Selection Algorithm with Boundary Detectors

WANG Da-wei ZHANG Feng-bin
(Department of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China)

Abstract A large quantity of holes is generated on the boundary of self and nonself region, because of the boundary dilemma of real-valued negative selection (RNS) algorithm. A real-valued negative selection algorithm with boundary detectors was presented. In the new approach, the detectors were interpreted using an aggressive interpretation, and during the training phase the boundary detectors whose aggressiveness was controlled by boundary threshold were generated and deployed on the boundary. The boundary detectors can reduce the holes on the boundary efficiently, and also probe the boundary between the self and nonself region implicitly. The algorithm was tested using both synthetic 2-D data set and MIT Darpa 1998 offline data set. Results demonstrate that the new approach has a much higher detection rate than RNS algorithm, in the case of the same false alarm rate, although it has a little higher minimum false alarm rate.

Keywords Artificial immune, Negative selection algorithm, Boundary dilemma, Hole

1 引言

人工免疫系统是一种新型的软件计算技术,它试图利用生物免疫系统表现出的机制来解决计算问题[1,2]。目前的人工免疫算法主要有:否定选择算法、免疫网络和克隆选择算法[3]。其中,否定选择算方法是一种自体/非自体识别技术[4],在可供选择的算法中具有明显作用并且能够以更高的质量提供独特的效果。该算法可以解决异常检测和检测时间序列中的异常等问题。

否定选择算法有很多变种,但全部变种的核心思想是定义一个自体集作为训练集来产生不与自体集模式匹配的检测器集,使用这些检测器来进行检测。目前大部分否定选择算法变种产生的检测器均采用二进制表示。选择二进制表示有两个优点:首先,二进制表示法提供了一个易于分析的有限空间;其次,二进制表示易于使用。然而,很多问题定义在实值空间,并且二进制表示的检测器很难处理。针对二进制表示检测器的局限性,Gonzalez 提出了实值否定选择算法[5]。该算法的搜索空间通常是连续的,并且适用于一些无法有效采用二进制表示法解决的应用。在实值否定选择算法中,通常以超球体或超立方体的形式表示检测器[6]。与二进制表示相比,实值表示最主要的特点是把与 R^n 子集对应的自体/非自体检测空间,归一化到超立方体空间$[0,1]^n$。

在实值否定选择算法的基础上,本文提出了一种新的采用边界检测器的实值否定选择算法。该方法引入了一种边界检测器,并以边界阈值来控制其侵略性。这种侵略性允许边界检测器靠近或者甚至"触摸"自体点。这样不仅能够有效地减少自体与非自体区域边界的漏洞,还能够隐式探明边界。

2 "边界困境"和漏洞

文献[7]提出了实值否定选择算法的"边界困境"问题。图1描述了"边界困境"情景,图中灰色部分代表自体区域,点代表自体样本,圆代表自体样本的阈值。如果自体阈值过小,自体样本间的空间便无法表示,也就是说,自体区域需要更多的自体样本点才能构成自体区域;另一方面,如果自体阈值过大,处于自体与非自体区域边界的自体样本覆盖的错误区域可能过大,造成结果无法接受。由于实值否定选择算法中自

到稿日期:2008-09-04 返修日期:2008-12-04 本文受国家自然科学基金项目(60671049),黑龙江省普通高校青年学术骨干支持计划项目(1511G012),黑龙江省研究生创新基金(YJSCX2007-0100HLJ)资助。

王大伟(1982—),男,博士研究生,主要研究方向为信息安全技术、网络安全,E-mail:stonetools@sohu.com;张风斌(1965—),男,教授,博士生导师,主要研究方向为信息安全技术。

体样本的这种可变性，使自体样本不可避免地超出自体与非自体区域边界，并在边界附近产生了一些不可能被检测器覆盖的非自体区域。另外，在靠近边界处，算法不知道生成多少检测器，亦不知道哪个检测器靠近边界，这样也容易在边界处产生未被覆盖的非自体区域。

漏洞是训练时未被检测器发现并覆盖的形态空间中的一部分非自体区域[8]。实值否定选择算法边界问题，使自体与非自体区域边界产生了很多漏洞。图 2 描述了二维空间中实值否定选择算法在自体与非自体边界产生漏洞的现象。深灰色区域代表自体区域，浅灰色圆表示检测器，而漏洞则用黑色区域来表示。

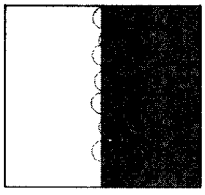

图 1　边界困境

图 2　实值检测器

3　算法与分析

本文提出的新方法采用具有侵略性的边界检测器来解决区域边界的漏洞问题。

3.1　边界检测器

算法使用一种具有侵略性的解释描述边界检测器。图 3 描述了检测器的传统解释方法与具有一定侵略性的解释方式的不同之处。图 3(a)以传统的方式描述了检测器集合覆盖情况，图 3(b)以具有一定的侵略性的方式进行描述。

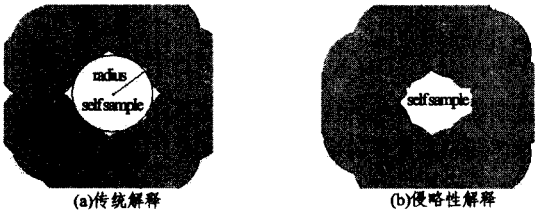

图 3　对检测器的不同解释

所谓侵略性就是允许检测器对自体数据的一部分进行覆盖，而即使检测器在自体区域具有一定的侵略性，自体样本仍然可以泛化成一个最终的自体区域。类似前面的讨论，如果在自体与非自体区域边界的边界检测器的侵略性过强，可能会使得检测器对正确样本区域的覆盖过大，造成较高的误报率，以至于结果难以接受。因此，本文设定一个边界阈值 r_b，引入这个阈值的主要目的在于衡量边界检测器在自体区域边界的侵略性。如果 $r_b=0$，则算法等同于实值否定选择算法；如果 $r_b=r_{self}$，即边界阈值等于自体数据半径，则边界检测器将可能“触摸”到自体数据的中心。换句话说，边界阈值越大，边界检测器对于自体区域越具有侵略性。

另外，图 3 还显示了由于自体阈值的限制，实值否定选择算法产生的检测器无论如何都不能靠近自体样本点，而具有侵略性的边界检测器可以靠近甚至“触摸”到自体样本点，因此，当一组自体点同时出现时，边界检测器通过在自体与非自体区域边界对自体区域的侵略性，可以隐式地探测出区域的边界。

图 4 描述了实值否定选择算法在边界上各个元素之间的关系，图中任意两个元素具有最小上界和最大下界。其中边界区域由自体、检测器和漏洞 3 部分组成，另外 self-o 和 detector-o 表示不靠近区域边界的自体和检测器，self-b 和 detector-b 表示靠近区域边界的自体和检测器。本文提出的新方法的目的在于通过边界阈值的设定，增加边界检测器的侵略性，使得 self-b 和 detector-b 更加紧密，从而减少边界上的漏洞。

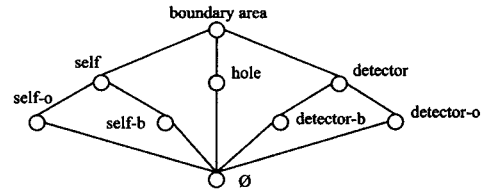

图 4　边界上各个元素之间的关系

3.2　算法

采用边界检测器的实值否定选择算法关键部分流程图，如图 5 所示。

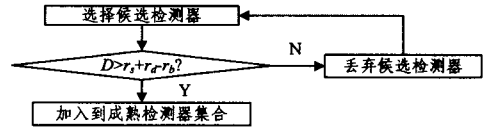

图 5　算法关键部分

从图 5 可以看出，本文提出的算法和实值否定选择算法的差别就在于边界阈值 r_b。看似微不足道的改变，却带来更加微妙的变化。由于边界阈值 r_b 的设定使得在自体与非自体区域边界的检测器具有一定的侵略性，能够有效减少漏洞。另一方面，边界阈值 r_b 又控制了边界检测器的侵略程度，使得边界上的检测器无法覆盖大量自体区域，能够有效控制误报率的增加。

具体算法如下：

算法　生成边界检测器

S：检测器集合
n：检测器数量
r_s：自体半径
r_d：检测器半径
r_b：边界阈值

```
1:D←Ø
2:Repeat
3:   x←random sample from [0,1]^n
4:     Repeat for every s_i in S
5:       d←Euclidean distance between s_i and x
6:       if d≤r_s+r_d−r_b,go to 2
7:     D←D∪{x}
8:Until |D|=n
9:return D
```

4　实验

设计试验来证明本文提出的算法的有效性。为了对比性能，本文对相同的数据集分别采用实值否定选择算法和本文提出的方法进行异常检测。计算出 TP(正确肯定次数)，TN(正确否定次数)，FP(错误肯定次数)，FN(错误否定次数)，并使用这 4 个值算出检测率和误报率。

由于使用不同的自体阈值可以均衡灵敏性和特意性，因此试验使用 ROC 曲线来对比算法性能。

4.1　人工二维数据

设计这个试验主要是为了证明本文提出的算法生成的检

测器与实值否定选择算法生成检测器的不同。整个搜索空间是一个二维正方形$[0,1]^2$。假定耐受自体点随机分布在特定的自体空间上，生成检测器后，使用随机分布于整个空间上的点评价算法性能。

图 6(a)显示了一种条带状的自体区域。这种条带状自体区域是能够显示出两种算法不同之处的最简单的形状。实验在条带状自体区域中随机生成 100 个自体样本点。检测器和自体数据的半径均为 0.05。图 6(b)描述了使用实值否定选择算法产生检测器的例子，图 6(c)描述了使用本文提出的算法产生检测器的例子，边界阈值为 0.03。图 6(d)描述了使用本文提出的算法在边界阈值为 0.05 时产生边界检测器的例子。其中深灰色的部分代表自体样本，浅灰色的部分代表检测器，在自体与非自体区域边界的空白部分代表漏洞。

图 6　条带状自体区域

从图 6 中提供的例子来看，采用边界检测器虽然侵略了部分自体区域，但却消除了区域边界的漏洞，并能隐式探测出区域边界。从图 6(c)和图 6(d)中可以看出，取不同边界阈值可以不同程度地减少边界上的漏洞。总的来说，当边界阈值比较大时可以完全消除边界上的漏洞，但是对自体区域的覆盖也随之变大。而图 6(b)所示的例子中，在区域边界存在明显的漏洞。

测试数据为随机分布于整个空间的 1000 个样本点。图 7(a)是边界阈值为 0.03 时两种算法的 ROC 曲线图。图 7(b)是边界阈值为 0.05 时的 ROC 曲线图。虽然由于边界阈值限定侵略性使得采用边界检测器的实值否定选择算法的最小误报率高一些，但相比实值否定选择算法却有更高的检测率。当边界阈值增大时，最小误报率也会增大，不过检测率也随之提高。

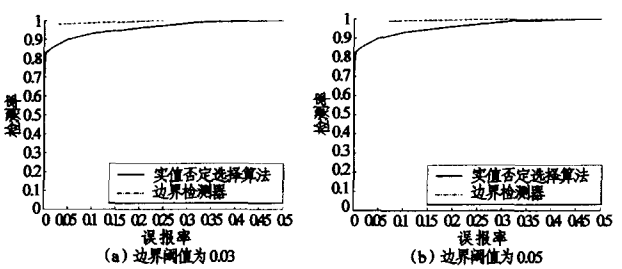

图 7　人工二维数据实验 ROC 图

4.2　MIT Darpa 1998 离线数据

设计这个实验证明本文提出的方法在真实网络环境中相比原来的实值否定选择算法具有更高的检测率。

MIT Darpa 1998 离线数据由麻省理工大学林肯实验室创建并管理，使用原始 tcpdump 数据提炼而成。这个数据集包括 2 个部分，第一个部分是训练数据，第二个部分是测试数据。本文选取训练数据中第一周星期一的 tcpdump 数据作为实验的训练数据，测试数据中的第一周星期一的 tcpdump 数据作为试验的测试数据。

构造自体样本时选择 3 个参数：每秒钟流过的字节数，每秒钟流过的包数，每秒钟流过 ICMP 包数。这些参数每分钟采样一次并正规化。由于这些参数可以被看成一个时间序列函数，因此特征可以使用大小为 3 的滑动覆盖窗口提取。这样就生成了一个 9 维的特征向量作为自体样本。训练数据记录了 634595 条数据，实验共生成 1279 个自体数据。为了对比两种算法的性能，训练时生成相同数量的检测器。使用不同的检测器阈值获得检测结果，边界阈值设定为 0.05。实验结果如图 8 所示。

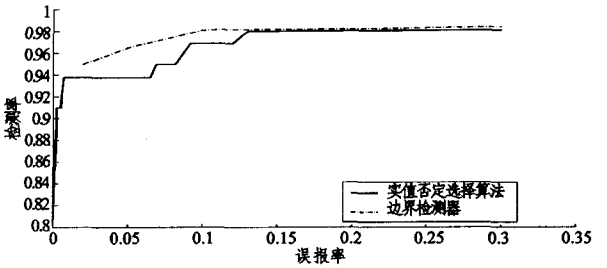

图 8　MIT Darpa 1998 离线数据 ROC 曲线图

从图中可以看出，与人工二维数据的结果类似，本文提出的算法有较高的最小误报率，不过在相同误报率的情况下，采用边界检测器的实值否定选择算法有更高的检测率。

结束语　本文提出的边界检测器的实值否定选择算法采用一种具有侵略性的解释描述检测器，使具有侵略性的边界检测器能够隐式地探测出边界，并覆盖自体与非自体区域边界的漏洞。通过设定边界阈值来控制边界检测器的侵略性，使得边界检测器在减少边界漏洞的前提下，不会覆盖过多的自体区域，这样可以控制最小误报率。

最后，实验结果表明，虽然最小误报率有所提高，但在检测率提高的前提下，这种结果还是可以接受的。

参 考 文 献

[1] Dasgupta D, Ji Z, Gonzalez F. Artificial immune system (AIS) research in the last five years[C]// Evolutionary Computation, 2003. CEC 03. The 2003 Congress. Canberra, Australia, 2003: 123-130

[2] de Castro L N, Timmis J I. Artificial immune systems as novel soft computing paradigm[J]. Soft Computing Journal, 2003, 7(7): 526-544

[3] Gonzalez F, Dasgupta D, Gomez J. The effect of binary matching rules in negative selection[C]// Genetic and Evolutionary Computation Conference. Heidelberg: Springer Berlin, 2003, 1723: 198-209

[4] Chmielewski A, Wierzchon S T. Simple method of increasing the coverage of nonself region for negative selection algorithms[C]// 6th International Conference on Computer Information Systems and Industrial Management Applications. Elk, Poland, 2007: 155-160

[5] Gonzalez F, Dasgupta D. Anomaly detection using real-valued negative selection[J]. Genetic Programming and Evolvable Machines, 2003, 4(4): 383-403

[6] Stibor T, Timmis J, Echert C. On the use of hyperspheres in artificial immune system as antibody recognition regions[J]. Lecture Notes in Computer Science, 2006, 4136: 215-228

[7] Ji Z. A boundary-aware negative selection algorithm [C]// IASTED International Conference on Artificial Intelligence and Soft Computing (ASC). Benidorm, Spain, 2005: 120-125

[8] Stibor T, Timmis J, Echert C. On permutation masks in hamming negative selection[C]// ICARIS 2006. Heidelberg: Springer Berlin, 2006: 122-135