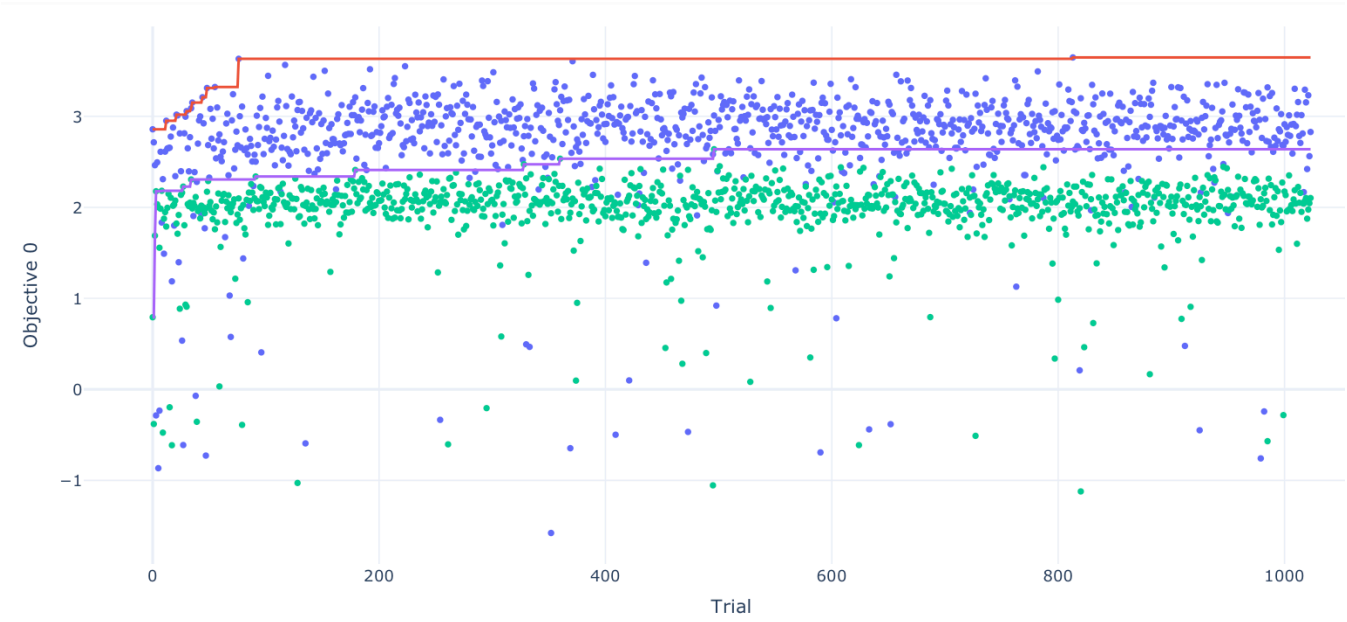
祝纪元20250425报告

使用 2012-2016 年作为 valid 数据集划分的表现

实验设置：
使用 variance preserving 初始化，其中 gain 的设置为通过我们数据集计算出的 alpha = 0.2501，数据集为 49 特征数据集，处理方式为 `clip(-0.2, 0.2)`。

下图绿色为 MLP 表现蓝色为 KAN 表现：



A Bidirectional Differential Evolution-Based Unknown Cyberattack Detection System

IEEE Transactions on Evolutionary Computation, April 2025

原文链接

本文提出的 BDE-IDS 中有关演化计算算子的细节

A. Clustering of Self Antigens

使用 Min-Max 对原始数据归一化后，对 self antigens 进行 k-means 聚类，记为 $\mathbf{S}_{clu}^{(1)}, \mathbf{S}_{clu}^{(2)}, \ldots, \mathbf{S}_{clu}^{(n_{clu})}$，其中第 k 个聚类对应的中心点记为 $\mathbf{c}_{clu}^{(k)}$，同时其对应的半径为：

$$r_{clu}^{(k)} = \max_{g_s^{i_k} \in \mathbf{S}_{clu}^{(k)}} \| c_{clu}^{(k)} - g_s^{i_k} \|_2$$

B. Bidirectional Differential Evolution for Nonself Antigens

BDE 算法旨在从已知的抗原中创造可能的未知非自身抗原。BDE 算法的初始种群为所有已知的非自身抗原集合的子集，即 $\mathbf{G}_{ini} \in \mathbf{N}_{tr}$，与此同时，我们希望新创造的抗原离已知的自身抗原尽可能远，离已知的非自身抗原尽可能进。

突变 Mutation

BDE 过程包含 FDE（forward differential evolution）与 RDE（reverse differential evolution）两个过程，其中 FDE 的目标为创造离已知抗原更近的抗原，RDE 的目标为创造离自身抗原和已知非自身抗原更远的抗原。

对于第 k 个簇，即 $\mathbf{S}_{clu}^{(k)}$，定义第 t 代的 RDE 和 FDE 的种群为 $\mathbf{P}_{fde}^{(k)}(t)$ 和 $\mathbf{P}_{rde}^{(k)}(t)$。注意到第一代即（$t = 1$）时，$\mathbf{P}_{fde}^{(k)}(t) = \mathbf{P}_{rde}^{(k)}(t) = \mathbf{G}_{ini}$。

对于前向过程 FDE 和反向过程 RDE，二者的突变策略是分开的，但形式类似，均为从父辈种群的随机组合，其中 RDE 的突变向量为：

$$\begin{aligned} \boldsymbol{v}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t) =& \lambda_1 \times \left[\boldsymbol{p}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t) - \boldsymbol{g}_{\mathrm{s}}^{(i_k)} \right] \\ &+ \lambda_2 \times \left[\boldsymbol{p}_{\mathrm{rde}}^{(k,l'_{\mathrm{r}})}(t) - \boldsymbol{p}_{\mathrm{rde}}^{(k,l''_{\mathrm{r}})}(t) \right] \end{aligned}$$

其中 $\boldsymbol{p}_{\mathrm{rde}}^{(k,l'_{\mathrm{r}})}(t)$，$\boldsymbol{p}_{\mathrm{rde}}^{(k,l''_{\mathrm{r}})}(t)$ 为对应第 k 个簇的 RDE 的父代种群中的两个随机个体。将突变向量加上父代个体得到突变抗原：

$$\boldsymbol{m}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t) = \boldsymbol{p}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t) + \boldsymbol{v}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t).$$

对于 FDE 来说，其突变向量服从类似规则：仅在第一项上符号相反：

$$\begin{aligned}\boldsymbol{v}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t) =& \lambda_3 \times \left[\boldsymbol{g}_{\mathrm{s}}^{(i_k)} - \boldsymbol{p}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t)\right] \\ &+ \lambda_4 \times \left[\boldsymbol{p}_{\mathrm{fde}}^{\left(k,l_{\mathrm{f}}'\right)}(t) - \boldsymbol{p}_{\mathrm{fde}}^{\left(k,l_{\mathrm{f}}''\right)}(t)\right]\end{aligned}$$

其对应的突变抗原为：

$$\boldsymbol{m}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t) = \boldsymbol{p}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t) + \boldsymbol{v}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t).$$

交叉 Crossover

注意在 mutation 过程中得到的突变抗原仍非我们最终用于测试的个体，最终测试个体 u 由以下过程交叉过程生成：

$$u_{\mathrm{rde}}^{(k,l_{\mathrm{r}},d)}(t) = \begin{cases} m_{\mathrm{rde}}^{(k,l_{\mathrm{r}},d)}(t), & \text{if } \rho_{\mathrm{rand}} \leq \rho_{\mathrm{cr}} \text{ or } d = d_{\mathrm{rand}} \\ p_{\mathrm{rde}}^{(k,l_{\mathrm{r}},d)}(t), & \text{otherwise} \end{cases} \tag{11}$$

$$u_{\mathrm{fde}}^{(k,l_{\mathrm{f}},d)}(t) = \begin{cases} m_{\mathrm{fde}}^{(k,l_{\mathrm{f}},d)}(t), & \text{if } \rho_{\mathrm{rand}} \leq \rho_{\mathrm{cr}} \text{ or } d = d_{\mathrm{rand}} \\ p_{\mathrm{fde}}^{(k,l_{\mathrm{f}},d)}(t), & \text{otherwise} \end{cases} \tag{12}$$

其中 d 的含义为第 d 个维度，即第 d 个位置的坐标。ρ_{cr} 为超参数交叉率，ρ_{rand} 为随机概率，随机整数 $d_{\mathrm{rand}} \in [1, n_d]$ 保证至少有一个维度是来自于突变抗原。

选择 Selection

在设定 RDE 的目标函数时，一个朴素的想法是希望新个体与簇的中心距离越大越好，即：

$$\mathcal{F}_{\mathrm{rde}}^{(k)}(\boldsymbol{x}) = \|\boldsymbol{x} - \boldsymbol{c}_{\mathrm{clu}}^{(k)}\|_2 \tag{13}$$

需注意到先前数据已经做过 Min-Max 归一化，其所有坐标都在 $[0, 1]$ 之间，因此二者最远的距离实际上为 $\sqrt{n_d}$，由此真正的满足 RDE 条件的个体应为：

$$\mathcal{F}_{\mathrm{rde}}^{(k)}\left(\boldsymbol{p}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t)\right) < \mathcal{F}_{\mathrm{rde}}^{(k)}\left(\boldsymbol{u}_{\mathrm{rde}}^{(k,l_{\mathrm{r}})}(t)\right) < \rho_{\mathrm{rde}} \times \sqrt{n_{\mathrm{d}}} \tag{14}$$

其中 ρ_{rde} 为调整系数，取值在 $[1,2]$。

对于 FDE 类似，其目标函数为 RDE 目标函数的倒数：

$$\mathcal{F}_{\mathrm{fde}}^{(k)}(\boldsymbol{x}) = 1 \div \|\boldsymbol{x} - \boldsymbol{c}_{\mathrm{clu}}^{(k)}\|_2. \tag{15}$$

考虑归一化后的坐标，满足条件的个体为：

$$\mathcal{F}_{\mathrm{fde}}^{(k)}\left(\boldsymbol{p}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t)\right) < \mathcal{F}_{\mathrm{fde}}^{(k)}\left(\boldsymbol{u}_{\mathrm{fde}}^{(k,l_{\mathrm{f}})}(t)\right) < 1 \div \left(\rho_{\mathrm{fde}} \times r_{\mathrm{clu}}^{(k)}\right) \tag{16}$$

将经过 t 期的进化后的个体集合记为：

$$\mathbf{G}_{\mathrm{bde}}^{(k)}(t) = \mathbf{G}_{\mathrm{rde}}^{(k)}(t) \bigcup \mathbf{G}_{\mathrm{fde}}^{(k)}(t). \tag{17}$$

当某个 t 期的进化个体集合为空集时，终止对第 k 个簇的进化过程，同时开启对第 $k+1$ 个簇的进化。