HAL
open science

VorAIS: A Multi-Objective Voronoi Diagram-based Artificial Immune System

Luis Marti, Arsene Fansi-Tchango, Laurent Navarro, Marc Schoenauer

To cite this version:

Luis Marti, Arsene Fansi-Tchango, Laurent Navarro, Marc Schoenauer. VorAIS: A Multi-Objective Voronoi Diagram-based Artificial Immune System . T. Friedrich and F. Neumann. Genetic and Evolutionary Computation Conference, GECCO 2016, Jul 2016, Denver, United States. pp.11 - 12, 2016, Poster at GECCO 2016 (Companion). 10.1145/2908961.2909027 . hal-01400263

HAL Id: hal-01400263

https://inria.hal.science/hal-01400263v1

Submitted on 20 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

VorAIS: A Multi-Objective Voronoi Diagram-based Artificial Immune System

Luis Martí[1,2] **Arsene Fansi-Tchango**[3] **Laurent Navarro**[3] **Marc Schoenauer**[1]

[1] TAO team, INRIA/LRI(CNRS & UPSud), Université Paris-Saclay, Paris, France.
[2] Universidade Federal Flumnense, Niterói (RJ) Brazil.
[3] ThereSIS, Thales Group, Paris, France.

Context

- Artificial Immune Systems have been derived from existing theories of the functioning of biological immune systems.
- They create a model that is able to discriminate between normal (self) and abnormal (non-self) objects.
- This feature makes AISs specially suited for dealing with problems related to anomaly and intrusion detection.

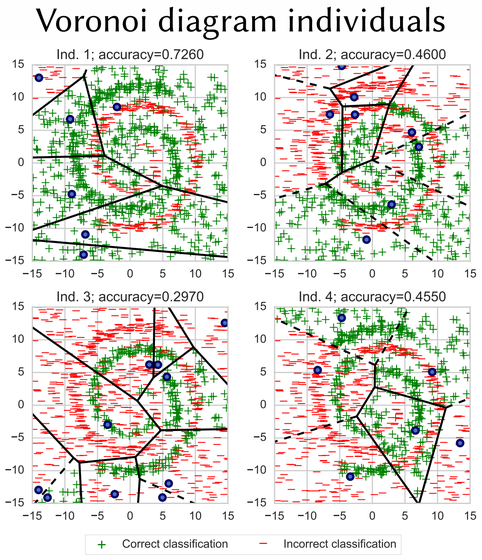
Voronoi diagram-based Artificial Immune System

VorAIS models the self/non-self using a Voronoi diagram that determines which areas of the problem domain correspond to self or to non-self.

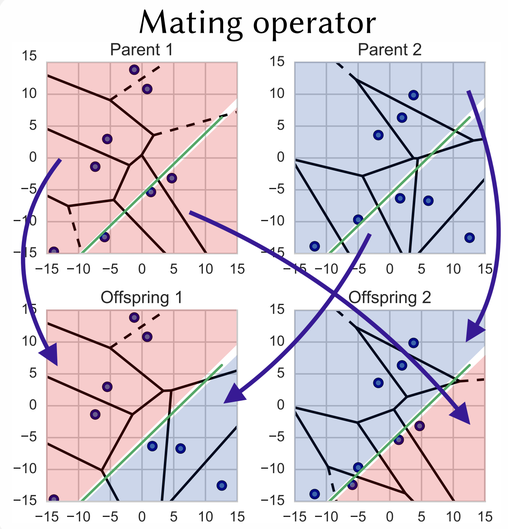
- Various classification metrics, like accuracy, recall, and specificity, must be taken into account.
- Multi-objective approach based on non-dominated sorting of NSGA-II.
- We introduce a mating operator as part of the AIS.

VorAIS components

Voronoi diagram individuals



Mating operator



Mutation operator

function mutate_voronoi($\mathcal{I}, p_s, p_f, p_t, p_+, p_-, \eta$)
- ▷ $\mathcal{I}$, individual to be mutated.
- ▷ $p_s \in [0,1]$, prob. of mutating a site.
- ▷ $p_f \in [0,1]$, prob. of mutating a site's feature.
- ▷ $p_t \in [0,1]$, prob. of changing the label of a site.
- ▷ $p_+ \in [0,1]$, prob. of adding a new site.
- ▷ $p_- \in [0,1]$, prob. of removing a site.
- ▷ $\eta \in (0,\infty]$, learning rate.

for all $S \in \mathcal{I}$ **do**
  if $U[0,1) < p_s$ **then**
    for all $x \in S$ **do**
      if $U[0,1) < p_f$ **then**
        $x \leftarrow$ mutate_log_normal(x, η)
    if $U[0,1) < p_t$ **then**
      $S.\ell \leftarrow$ switch_label$(S.\ell)$.
if $U[0,1) < p_+$ **then**
  $\mathcal{I} \leftarrow \mathcal{I} \cup \{$random_site$\}$.
if $U[0,1) < p_-$ **then**
  $i \leftarrow U[1, |\mathcal{I}|)$.
  $\mathcal{I} \leftarrow \mathcal{I} \setminus \{\mathcal{I}(i)\}$.
return $\mathcal{I}$, mutated individual.

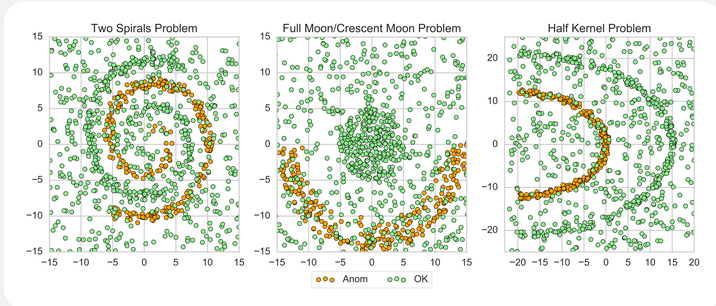
VorAIS outline

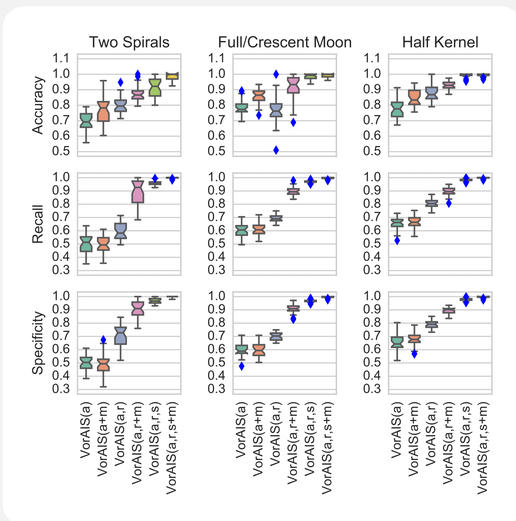
1. Create an initial random population $\mathcal{P}_0$ of n_{pop} individuals.
2. At iteration t, individuals in $\mathcal{P}_t$ are mated and mutated.
3. An offspring population, $\mathcal{P}_{\text{off}}$, with n_{off} individuals is created.
4. From $\mathcal{P}_t \cup \mathcal{P}_{\text{off}}$ the best n_{pop} individuals are selected using non-dominated sorting (with crowding distance).

Hyperparameters tuned by grid search (see PPSN paper).

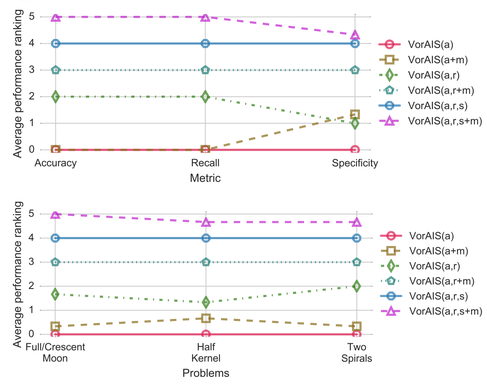
Preliminary study on test problems

- Influence of the mating operator (+m) and the use of the classification metrics (a, r and s, respectively), on two-dimensioal problems.



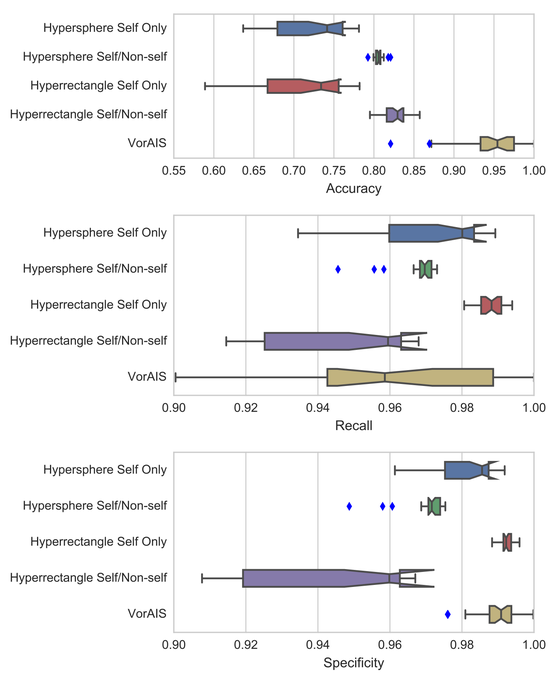


Bergmann-Hommel tests grouped by problem and metric.



NSL KDD'99 anomaly detection problem

- Compare VorAIS with other AISs in a computer network anomaly detection benchmark problem.
- NSL-KDD'99 has 41 —38 numeric and 3 categorical— features and one class attribute describing the nature of the events.



Bergmann-Hommel tests.

	NSA_{sp}	NSA^+_{sp}	NSA_{re}	NSA^+_{re}	VorAIS
Accuracy					
NSA_{sp}	×	−	∼	−	−
NSA^+_{sp}	+	×	+	−	−
NSA_{re}	∼	−	×	−	−
NSA^+_{re}	+	+	+	×	−
VorAIS	+	+	+	+	×
Recall					
NSA_{sp}	×	+	−	+	∼
NSA^+_{sp}	−	×	−	+	∼
NSA_{re}	+	+	×	+	+
NSA^+_{re}	−	−	−	×	−
VorAIS	∼	∼	−	+	×
Specificity					
NSA_{sp}	×	+	−	+	−
NSA^+_{sp}	−	×	−	+	−
NSA_{re}	+	+	×	+	+
NSA^+_{re}	−	−	−	×	−
VorAIS	+	+	−	+	×

Final remarks

- We have obtained a performance comparable with the state of the art but adequate classification performance is not enough.
- It is necessary to create a compact representation of the 'normal' data.
- We developed custom objective functions that rely on volume-based approaches.

L. Martí, A. Fansi-Tchango, L. Navarro, and M. Schoenauer, *Anomaly detection with the Voronoi diagram evolutionary algorithm*,in Proceedings of the 14th International Conference on Parallel Problem Solving from Nature (PPSN XIV), Edinburgh, UK: Springer, 2016.