Neurocomputing 149 (2015) 515–525

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

A negative selection algorithm with online adaptive learning under small samples for anomaly detection

Dong Li [a,b], Shulin Liu [a,*], Hongli Zhang [a]

[a] School of Mechatronics Engineering and Automation, Shanghai University, Shanghai 200072, China
[b] School of Petroleum Engineering, Changzhou University, Changzhou 213164, China

ARTICLE INFO

Article history:
Received 2 December 2013
Received in revised form
2 June 2014
Accepted 10 August 2014
Communicated by Haowei Liu
Available online 21 August 2014

Keywords:
Artificial immune system
Negative selection algorithm
Anomaly detection
Interface detector
Online adaptive learning

ABSTRACT

The training stage and testing stage of traditional negative selection algorithm (NSA) are mutually independent, and NSA lacks continuous learning ability. Its detector cannot completely cover the non-self space. A new NSA with online adaptive learning under small training samples, OALI-detector, was proposed in this paper. I-detector can fully separate the self space from the non-self space with an appropriate self radius. It can adapt itself to real-time change of self space during the testing stage. The experimental comparison among I-detector, V-detector, and other anomaly detection algorithms in two artificial and Iris datasets shows that the I-detector can obtain the highest detection rate in most cases. The experimental comparison between OALI-detector and V-detector on Iris datasets shows that when overfitting does not occur, the OALI-detector can obtain the highest and lowest false alarm rates, even if only one self sample is used for training.

1. Introduction

More and more researchers in recent years have focused on Artificial Immune System (AIS), which is inspired by biological immune systems [1,2]. Currently, several AIS mechanisms, such as negative selection, clone selection and immune network, have been developed to provide more efficient solutions, including anomaly detection, fault diagnosis, computer security, clustering, and optimization [3,4]. Negative Selection Algorithm (NSA) is one of the earliest AIS models and attracts widespread interest in anomaly detection for it only requires normal samples for training [5–7]. As a one-class classification algorithm, compared with other classification methods, NSA has less control parameters and is insensitive to the parameters [8–10].

In 1994, inspired by the mechanism of T-cell maturation in the thymus, Forrest et al. proposed the negative selection algorithm [11]. Later, a variety of modified versions of this algorithm were proposed [6,12,13].

In the initial NSA, self and non-self samples were represented with binary encoding [11,14]. It is easy to understand the mechanism of NSA, but it can hardly process a lot of applications described in real-valued space [15]. Later, a real-valued negative selection algorithm was presented [16–18], and the detectors were hyperspheres with constant radius. In order to achieve enough coverage, some detector generation algorithms were proposed, such as variable-sized detector [19,20], hypercube detector [17,21], hyper-ellipsoid detector [22,23], and multi-shaped detector [24].

The number of holes decreases with the increase of the coverage, but the complete detector coverage can be hardly realized. In order to reduce holes, some improved algorithms were proposed.

ANSA [6] can build an appropriate profile of the system with a subset of self samples, and adaptively adjust the self radius, the detection radius and the number of detectors to amend the profile of the system. It can be adapted to various self/non-self spaces. Boundary detectors [25] are allowed to cover partial self space. This enables them to eliminate the holes on the boundary and to detect the deceiving anomalies hidden in the self space. However, when the boundary threshold increases, the false alarm rate also increases. V-detectors of FtNSA [26] were respectively generated in self space and non-self space to classify the testing samples within the holes. It can obtain the higher detection rate and lower false alarm rate in most cases. The 2-NSA [27] consisting of two negative selection processes can effectively improve the efficiency of detector generation, reduce the time cost of the algorithm, and reduce the false-positive rate of the detection system. NSAPF [28] can balance and adjust the true positive rate and false positive rate by adjusting the penalty factor C to achieve the better performance. The 2-NSA achieves a higher true positive rate on completely unknown malware and a better generalization ability while keeping a low false positive rate. CB-RNSA [29] is based on hierarchical clustering of self space and has the higher time efficiency and detector quality than classic NSAs.

* Corresponding author. Tel.: +86 21 56331523.
E-mail address: lsl346@shu.edu.cn (S. Liu).

http://dx.doi.org/10.1016/j.neucom.2014.08.022
0925-2312/

Although the methods mentioned above can improve the detector coverage and detection rate and eliminate the holes, little attention has been paid to the detector with online adaptive learning under small training samples. For training data are just from partial self samples, and the self/non-self space often varies with time, the generated detectors are only appropriate to special training data. If the self space is changed, the previously generated detectors are not applicable and new training process is required.

The paper presents a negative selection algorithm named interface detector (I-detector). It can completely divide state space $\boldsymbol{T}$ into self space $\boldsymbol{S}$ and non-self space $\boldsymbol{N}$. During the testing stage, it can be adapted to real-time change of self space, even if only one self sample is used for training.

The remaining sections of the paper are structured as follows: the model of I-detector and OALI-detector are presented in Sections 2 and 3, respectively. The experimental results are presented in Section 4. In Section 5, conclusions are provided.

2. Interface detector

Anomaly detection aims to identify the normal and abnormal states of a system. The states of a system can be represented by a set of features. This paper is based on real-valued NSA, and some basic concepts are defined as follows [6]:

(1) System state space $\boldsymbol{T}$: a state of the system can be represented by a vector of features $\boldsymbol{t}^i=[t_1^i,t_2^i,\ldots,t_n^i]$, $\boldsymbol{T}=\{\boldsymbol{t}^i,i=1,2,\ldots,u\}\subset \boldsymbol{R}^n$. For simplicity, it is assumed that each feature is normalized to [0,1], and $\boldsymbol{T}=[0,1]^n$.
(2) Self space $\boldsymbol{S}$: a set of feature vectors represents the normal state of a system, $\boldsymbol{S}=\{\boldsymbol{s}_i,i=1,2,\ldots,k\}\subset \boldsymbol{T}$.
(3) Non-self space $\boldsymbol{N}$: the complement space of self space is called non-self space, where $\boldsymbol{T}=\boldsymbol{S}\cup\boldsymbol{N}$, and $\boldsymbol{S}\cap\boldsymbol{N}=\emptyset$.
(4) Self sample $\boldsymbol{s}$: $\boldsymbol{s}=\{<\boldsymbol{s}_i, r_s>|\boldsymbol{s}_i\in\boldsymbol{S}, r_s\in\boldsymbol{R}\}$, where r_s is the self radius.

2.1. The implementation strategies of interface detector

In NSA, the detector coverage is a crucial content of the classification performance. The optimization of detector distribution and the elimination of the holes have been extensively studied [1,12]. However, it is still difficult to satisfy the detector coverage. The hypersurface, which is tightly around the self space, as a detector, can completely eliminate holes. Non-self samples are outside of the hypersurface and self samples are inside the hypersurface.

Definition 1. *Interface detector*, I-detector, is one or more closed hypersurface, which is tightly around the self space. It can completely divide state space $\boldsymbol{T}$ into self space $\boldsymbol{S}$ and non-self space $\boldsymbol{N}$. Non-self samples are outside of the hypersurface, and self samples are inside the hypersurface.

In 2-dimensional space, I-detector is one or more closed curves, as shown in Fig. 1.

It is difficult to directly describe I-detector, but we can use the outermost samples in self space to describe it indirectly. Because the shape of hypersurface is only related to the outermost samples of self space and has nothing to do with internal samples.

Definition 2. *Boundary samples* are the outermost samples in self space, which can affect the shape of I-detector. The boundary sample set $\boldsymbol{B}$ is a subset of self space, $\boldsymbol{B}=\{\boldsymbol{b}_i, i=1,2,\ldots,l\}\subseteq\boldsymbol{S}$. Non-self samples are outside of boundary samples and self samples are in the other side of boundary samples or within boundary samples.

The obtained the boundary samples and their position information can be used for anomaly detection. Therefore, I-detector can be described as

$$\mathrm{D}=\{\langle \boldsymbol{b}_i, r_s, p_i\rangle|\boldsymbol{b}_i\in\boldsymbol{B},\quad r_s\in\boldsymbol{R}\},$$

where $\boldsymbol{b}_i$ is the boundary sample; r_s is the self radius; p_i is the position information of $\boldsymbol{b}_i$.

It is easy to calculate the distance between two samples, but it is difficult to confirm their position relationship because samples are hypersphere with the constant radius in state space. Therefore, it is difficult to obtain the boundary samples. On the contrary, we can get the boundary of self space.

If the self space is filled with same hypercubes, the self space can be approximated through Eq. (1). Moreover, it is easy to obtain the position relationship between any two hypercubes within state space.

$$V_{\text{self space}}=\lim_{V_{\text{hypercube}}\to 0}\sum_{i=1}^{\infty}V_{\text{hypercube}}. \tag{1}$$

Fig. 2 shows the approximation progress in 2-dimensional space. Fig. 2a shows the self space. There are 20^2, 40^2, 80^2 squares in Fig. 2b, c and d, respectively. It is clear that the boundary of squares in the self space can be approximated to the boundary of self space.

After we get the boundary of these hypercubes in the self space, we can obtain the boundary of self space indirectly.

State space $\boldsymbol{T}$ is evenly divided into m^n hypercubes:

$$\boldsymbol{T}=\cup_{i=1}^{m^n}h_i \tag{2}$$

where, m is the number of segments of each dimension; n is the number of space dimension.

According to the following rules, the self samples are dispersed into the hypercubes.

$$\begin{cases} h_i=\emptyset & \text{if} \quad d>r_s \\ h_i\neq\emptyset & \text{if} \quad d\le r_s \end{cases} \tag{3}$$

where $d=\min\{d_{ij},\ i=1,2,\ldots,m^n;\ j=1,2,\ldots,k\}$; d_{ij} is the distance between $\boldsymbol{c}_i$ and self sample $\boldsymbol{s}_j$; $\boldsymbol{c}_i$ is the center of hypercube h_i.

Definition 3. *Empty hypercube* is no self sample in it, and *non-empty hypercube* is one or more self samples in it.

Definition 4. When a hypercube is non-empty and at least one of its adjacent hypercube is empty, or at least one of its surfaces is boundary, it is a *Boundary hypercube*. The samples in boundary hypercubes are boundary samples, which are the outermost samples of self space.

Definition 5. The *position information* of a boundary hypercube is used to record each of its adjacent hypercubes' property. Moreover, the *position information* of boundary hypercube is also one position information record of boundary samples in this hypercube.

The coordinate values in each dimension can be used to describe the position relationship among hypercubes. Each boundary hypercube has $2n$ position information records.

According to Eq. (3), a boundary sample may be dispersed into several boundary hypercubes, and its position information must merge all the position information of these hypercubes. When a testing sample $\boldsymbol{t}$ satisfies the position information, it is on the outer side of the I-detector and recorded as $\boldsymbol{t}=\otimes$. Otherwise, it is on the inner side of the I-detector and recorded as $\boldsymbol{t}=\mathrm{O}$.

In order to better understand these definitions, further explanation is shown in 2-dimensional dataset. There are 27 self samples in Fig. 3, and $r_s=0.0825$. The state space $[0,1]^2$ is evenly divided into 17^2 squares: the white squares are empty; others are non-empty; the dark gray squares are boundary squares.