Contents lists available at ScienceDirect

Expert Systems with Applications

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

Design of an artificial immune system based on Danger Model for fault detection

C.A. Laurentys *, R.M. Palhares, W.M. Caminhas

Federal University of Minas Gerais, Antônio Carlos Av. 6627, Mail Box 31270-010, Belo Horizonte City, Minas Gerais State, Brazil

ARTICLE INFO

Keywords:
Artificial immune system
Computational intelligence
Fault detection
Decision support
Fuzzy set
Model development
Neural network

ABSTRACT

This paper presents a methodology that enables fault detection in dynamic systems based on recent immune theory. The fault detection is a challenging problem due to increasing complexity of processes and agility necessary to avoid malfunction or accidents. The fault detection central challenge is determining the difference between normal and potential harmful activities at dynamic systems. A promising solution is emerging in the form of Artificial Immune Systems (AIS). The Danger Model (DM) proposes that the immune system reacts not against self or non-self but by threats generated into the organism: the danger signals. DM-based fault detection system proposes a new formulation for a fault detection system. A DM-inspired methodology is applied to a fault detection benchmark provided by DAMADICS to compare its relative performance to others algorithms. The results show that the strategy developed is promising for incipient and abrupt fault detection in dynamic systems.

1. Introduction

The fault detection is a major problem in the area of engineering processes. It is one of the vital components for the Abnormal Event Management (AEM) which has attracted attention. The AEM deals with detection, diagnosis, and correction of abnormal conditions in real time at processes operation. Nowadays plant operators perform operations with complex decision-making as: detecting abnormalities, identifying the fundamental cause, predicting consequences of failures beyond the planning, and implementation of corrective actions (Fangping, 2003; Laurentys et al., 2009).

The AEM is becoming increasingly challenging due the size and complexity of procedures and the broad scope of its activities, encompassing a variety of factors such as degradation of the process, measurements inadequate, incomplete and not reliable, and its interrelation with the human action (Bomfim, Caminhas, Rodrigues, & Laurentys, 2004).

Regarding the complexity, the industries of manufacturing process suffer pressure to increase the quality of products and environmental standards each time more restrictive. To meet the growing standard of quality, industrial processes added a set of observed variables. For example, there are references in the literature of cases up to 1500 variables to be observed by the second (Bailey, 1984).

A large number of variables that interact dynamically during a process give high complexity of industrial systems that despite highly automated, they still are dependent on human performance in various aspects. Analyzing the context is not surprising that people responsible for AEM take often incorrect decisions.

Immune-based techniques are gaining popularity in a wide area of applications, including the automation of the fault detection step of AEM (Araujo, Aguilar, & Aponte, 2003; Dasgupta & González, 2003; Niño, Gómez, & Vejar, 2003). It has emerged as a new branch of Artificial Intelligence. The powerful information processing capability, pattern recognition, learning, memory, and immune distributive nature provide rich metaphors for its artificial (computational) counterpart. In this context, Artificial Immune Systems (AIS) (de Castro & Timmis, 2002; de Castro Silva & Von Zuben, 2004; de Castro, 2006) are defined as a new computational paradigm based on metaphors of the biological immune systems.

This paper proposes, implements, and validates an AIS to automate the monitoring and fault detection phases of AEM in order to create a decision-making tool to support operator actions in a dynamic system avoiding malfunction or accidents.

The key contribution is an AIS inspired on the immune Danger Model (DM) (Matzinger, 2002) and a validated human immune model (de Pillis, Radunskaya, & Wiseman, 2005) to allow dynamic systems fault detection.

This article is organized as following:

- Danger Model Brief Overview section describe the Danger Model features that inspired its use for the proposed AIS,
- Methodology section presents the analogies between the proposed fault detection system and the DM mechanisms that inspire the proposed methodology,
- Process Validation Brief Description section describes the fault detection process that the AIS was applied,

* Corresponding author. Tel./fax: +55 88217802.
E-mail address: ka.laurentys@gmail.com (C.A. Laurentys).

0957-4174/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2009.12.079

- Results section presents the algorithm validation database and compares its performance to others algorithms,
- Conclusion section point out the major benefits of using this approach.

It is important to stress that the proposed methodology was applied to a fault detection benchmark provided by DAMADICS (Barty, 2002) to compare its relative performance to others algorithms. The results show that the strategy developed is promising for incipient and abrupt fault detection in dynamic systems.

2. Danger Model brief overview

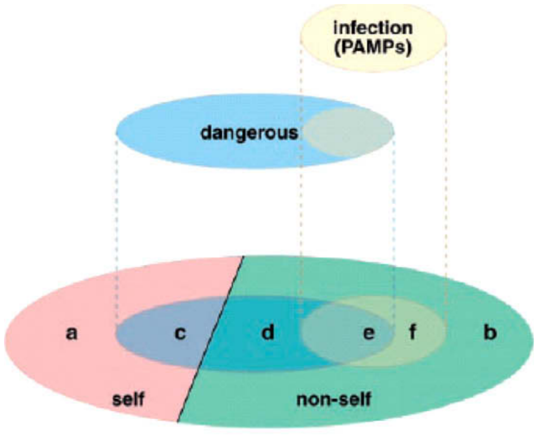
2.1. Danger Model description

For over 50 years, immunologists have based their thoughts, experiments, and clinical treatments on the idea that the immune system functions by making a distinction between self (related to belonging molecules in the organism) and non-self (related to foreign molecules in the organism) (Deaton et al., 1997; Forrest, Perelson, Allen, & Cherukuri, 1994).

Although this paradigm has often served immunologists well, years of detailed examination have revealed a number of inherent problems. The Danger Model outlines a model of immunity based on the idea that the immune system is more concerned with entities that do *damage* than with those that are *foreign*. The Danger Model came out to explain points that other theories could not.

One of the important affirmations of the Danger Model is that the immune system is activated by danger/alarm signals from injured cells, such as those exposed to pathogens and mechanical damage (Ephraim Fuchs, xxxx) instead of foreign or infections molecules. Fig. 1 depicts the key difference among the immune theories in what concerns the activation responses predicted by each immune theory.

According to the Danger Model, alarm signals can be constitutive or inducible, intracellular or secreted. Because cells dying by normal programmed processes (referred as *Apoptotic death*) are usually scavenged before they disintegrate, whereas cells that die necrotically (*Necrotic death*) release their contents, any intracellular product could potentially be a danger signal when released. Inducible alarm signals could include any substance made, or modified, by distressed or injured cells. The important feature is that danger/alarm signals should not be sent by healthy cells or by cells undergoing normal physiological deaths. Fig. 2 shows the release of alarm signal by a distressed cell and the immune cells responsible for its processing.



Responses to each set predicted by:	a	b	c	d	e	f
SNS	−	+	−	+	+	+
INS	−	−	−	−	+	+
Danger	−	−	+	+	+	−

Fig. 1. Diagram evidencing the context of the Danger Model. The immune system does not response to self–non-self theory (SNS) or Infections-non-self (INS) but instead it is activated by alarms/dangerous signals (Danger) (Dasgupta and González, 2003).

In the immune context describe by the Danger Model, APCs (antigen-presenting cells) are cells that will process the danger signal and stimulate the T Cells. The APCs are *activated by danger signals* from distressed or injured cells such as those exposed to pathogens, toxins, and mechanical damage. The activated APCs will provide an extra signal to *prime the T cells*.

2.2. Danger model

Based on the features described in Section 2.1, the Danger Model could summarize in the following steps:

- *Danger Signals Definition*: according to the Danger Model, these signals are generated by distressed or necrotical (non-programmed) cell death, and the normal cells do not generate it;
- *Transduction of Danger Signals*: the APC will collect the signal and process it in order to costimulate the T Cells;
- *Final immune outcome*: The T cell will or not prime depending on the intensity of the APC signal strength;

These steps are illustrated at the Fig. 3.

3. Methodology

The AIS proposed was inspired on the Danger Model described in Section 2.2. The source of inspiration was the proposition that the immune response is not guided by a sense of *foreignness* but in a sense of *dangerous* as described by the Danger Model.

In the fault detection context, this is interpreted as the fault is not a dynamic system foreign component but it is instead a *dangerous* conditioning behavior.

Like in the Danger Model, the dangerous signals must be defined and processed in order to provide alarms of the dynamic system behavior.

This section presents AIS the analogies between the proposed fault detection system and the Danger Model mechanisms that inspire the proposed AIS. In order to fully understand how the AIS

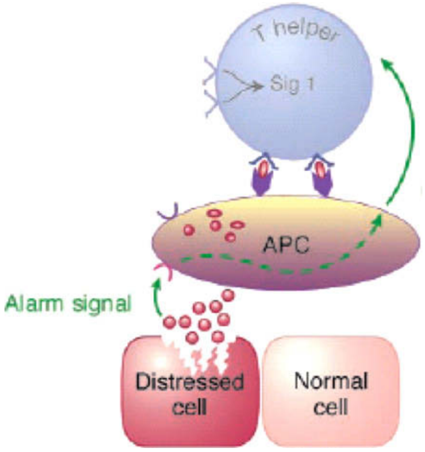


Fig. 2. According to the Danger Model, the distressed or injured cells only are able to release alarm / dangerous signals.