

软件、算法与仿真

用于异常检测的小参数集树突状细胞算法

王杰,张毅,姜念

郑州大学电气工程学院, 河南 郑州 450001

摘要:

树突状细胞算法(dendritic cell algorithm, DCA)是受自然免疫系统中树突状细胞的功能启发的免疫算法。当应用于实时异常检测时该算法具有优越的性能,但由于参数和随机元素相当多,算法难于分析。提出了一种用于异常检测的小参数集树突状细胞算法,在保证算法实现正确功能的前提下,减少了DCA中的参数,使算法参数数量得到了控制。此外,新算法还定义了更为简洁的信号处理过程以及对应的异常度量 and 异常阈值。最后,利用端口扫描数据集对算法进行了测试,实验结果表明,新算法是DCA的一种有效形式,新的异常度量更加敏感且它体现出的正确分类时间延长了30.3%~56.7%。

关键词: 异常检测 端口扫描 树突状细胞算法

Small set of parameters dendritic cell algorithm for anomaly detection

WANG Jie,ZHANG Yi,JIANG Nian

School of Electrical Engineering, Zhengzhou Univ., Zhengzhou 450001, China

Abstract:

The dendritic cell algorithm (DCA) is an immune-inspired algorithm based on the function of dendritic cells of the natural immune system. The algorithm performs very well when applied to real-time anomaly detection, but it is difficult to analyze the detected results because of a large number of parameters and stochastic elements. This paper presents a novel dendritic cell algorithm based on the small set of parameters for anomaly detection. It reduces the number of parameters of DCA on the premise of ensuring the correct function of the algorithm, so that the number of parameters is under control. Moreover, the new algorithm yet defines a more concise signal processing procedure, as well as the corresponding anomaly measure and an anomaly threshold. Finally, a port scan data set is applied to test the algorithm. Experimental results show that the new algorithm is an effective form of DCA, the new anomaly measurement is more sensitive and it extends the time of correct classification by 30.3%~56.7%.

Keywords: anomaly detection port scan dendritic cell algorithm

收稿日期 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-506X.2010.11.47

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献:

本刊中的类似文章

扩展功能

本文信息

- Supporting info
- PDF(OKB)
- [HTML全文]
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

本文关键词相关文章

- 异常检测
- 端口扫描
- 树突状细胞算法

本文作者相关文章

PubMed