粒子群特征优选的 SVDD 入侵检测研究

魏振伟 1,2，刘　飞 3
(1 郑州航空工业管理学院 航空工程系，河南 郑州 450015；2 航空经济发展河南省协同创新中心,
河南 郑州 450046;3 空军工程大学 防空反导学院，陕西 西安 710051)

摘　要： 针对入侵检测中样本集维数较高问题，提出一种基于粒子群算法（PSO）优化的支持向量数据描述（SVDD）方法，将其应用于网络异常入侵检测.该方法采用粒子群算法消除支持向量数据描述中的冗余参数并对数据降维，并建立 SVDD 超球体模型，对网络入侵数据进行检测并输出入侵检测结果.在 KDD CUP’99 的标准检测数据集上进行仿真实验，结果表明该方法和传统的 SVDD 相比不仅能够有效提高检测率，而且计算量较小.

关键词： 入侵检测；支持向量数据描述；粒子群算法

Research of Network Intrusion Detection Based on Particle Swarm Optimization and Support Vector Data Description

WEI Zhen-wei1,2, LIU Fei3
(1 Department of Computer Science and Application, Zhengzhou University of Aeronautics, Zhengzhou 450015, China；
2 Collaborative Innovation Center for Aviation Economy Development,Zhengzhou 450046, China;
3 Air-Defense and Anti-Missile Institute, Air Force Engineering University, Xi'an 710051, China)

Abstract： Concerning the data set of high dimensions in intrusion detection, the new algorithm based on support vector data description (SVDD) which optimized by particle swarm optimization (PSO) was proposed. In the improved algorithm, at firstly the particle swarm optimization was used to remove redundant features and reduce the data dimension in support vector data description. And then, the support vector data description built a super sphere model to detect the attacks from internet by analyzing the network connection data. Results from the experiments with the KDD CUP’99 network data indicate that the method of PSO-SVDD is better than traditional one class classifiers algorithm, which can improve the efficiency of intrusion detection and reduce the false detection rate.

Key words： intrusion detection；support vector data description；Particle swarm optimization

作者简介：
魏振伟　男，（1981-），硕士，工程师.研究方向为检测与诊断，模式识别.E-mail：ygszzia@126.com
刘　飞　男，（1981-），博士研究生.研究方向为计算机系统安全.