基于二次决策的深度学习入侵检测模型

江泽涛，翟振宇

（桂林电子科技大学 广西图像图形与智能处理重点实验室，广西 桂林 541000）

摘 要： 针对深度神经网络用于入侵检测方法时存在训练过程中由于数据不平衡和特征冗余两大问题而导致的低检测率和高误报率，提出一种基于二次决策的深度学习模型（TDDL）.该模型由深度堆栈自动编码器（DSAE）和神经网络结合，包括二个阶段特征学习，其中第一阶段使用 DSAE 对特征压缩并加入区分异常数据的概率值特征，第二阶段使用神经网络(NN)接收第一阶段的特征并训练，从而降低特征冗余和平衡对正常数据的偏向，以提高检测效果.经 KDDCUP99 数据集进行实验测试，仿真实验结果表明，该模型能有效提升深度神经网络在入侵检测数据上特征学习的效果，使其具有更高的准确率的同时，还具有较低的误报率.

关键词： 深度学习；入侵检测；自动编码器；特征学习

Based ontwice decision for deep learning intrusion detection model

JIANG Ze-tao, ZHAI Zhen-yu

（Guilin University of Electronic Technology Guangxi Key Laboratory of Imageand Graphic Intelligent Processing,Guilin University of Electronic Technology, Guilin 541000， China）

Abstract： Aiming at the intrusion detection method of deep neural network, there are two problems of data imbalance and feature redundancy in the training process, resulting in low detection rate and high false positive rate. Based on Twice Decision Deep Learning model(TDDL) is proposed: The model is a combination of Deep Stack Autoencoder(DSAE) and neural network, including two-stage feature learning, in which the first stage uses DSAE to compress features and add probability value features that distinguish abnormal data, and the second stage uses neural networks(NN) receives the characteristics of the first stage and trains, thereby reducing the feature redundancy and balance bias on normal data to improve the detection effect. The experimental results of KDDCUP99 dataset show that the model can effectively improve the effect of deep neural network on feature detection of intrusion detection data, so that it has higher accuracy and lower false positive rate.

Key words： deep learning;intrusion detection;self-encoder;feature learning

作者简介：

江泽涛 男，（1961），博士生导师，教授.研究方向为访问控制与信息安全及计算机视觉.

翟振宇(通信作者) 男，（1994），硕士研究生.研究方向为信息安全.

E-mail: 731877986@qq.com