基于两级分段模型的异构数据处理与网络攻击检测

李超鹏 1,2 ，王劲林 1

（1 中国科学院声学研究所，北京，100190；2 中国科学院大学，北京，100049）

摘　要：由于网络数据存在着异构特性，在网络攻击检测中，需要使用合理的方法对异构数据进行整合.我们在文章中提出了两级分段模型对异构数据进行整合并建模分析，同时讨论了模型在多核条件下的模型分布式并行训练.在实验部分，本文介绍了使用的 DARPA 1998 网络攻击数据集，并分析了不同分段方式下的攻击检测性能.同时，本文介绍说明模型在多核条件下的并行性能.结果显示，在面向异构数据时，两级分段模型相比于无分段的全连接神经网络模型有着更好的检测准确率和召回率.

关键词：攻击检测；两级分段模型；异构数据

Heterogeneous data processing and network attack detection based on two-level and multi-segment model

LI Chao-peng 1,2 , WANG Jin-lin 1

(1 Institute of Acoustics Chinese Academy of Sciences, Beijing 100190, China; 2 University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract：Because of the heterogeneous character of network data, a reasonable method is required to integrate the heterogeneous data in network attack detection. In this paper, we propose a two-level and multi-segment model for network attack detection. Meanwhile, the parallel training method is also involved. In the experiments, DARAP 1998 dataset has been used which is a public cyber attacks dataset. The experimental result shows that when facing the heterogeneous data, the two-level and multi-segments model has an effective performance that the proposed model obtains a better detecting accuracy and recall than the fully connected neural network.

Key words：

作者简介：

李超鹏　男，（1990-），博士研究生.研究方向为网络安全和深度学习.E-mail:licp@dsp.ac.cn.

王劲林　男，（1964-），研究员.研究方向为数字信号处理、信源编码和信道编码、网络中基于媒体流的应用技术以及 5G 通信.