基于深度自编码和决策树的恶意域名检测

赵　宏，常兆斌，王伟杰

（兰州理工大学 计算机与通信学院，甘肃 兰州 730050）

摘　要： 针对目前恶意域名检测方法特征提取过程复杂和检测准确率不高的问题，提出一种基于深度自编码和决策树（Deep Auto Encoder and Decision Tree, DAE-DT）的恶意域名检测算法.该算法首先将每一域名按照域名词法组成与结构等属性进行特征映射，并进行正则化处理;然后将正则化处理后的无标签域名数据随机置 0 作为模型的输入，域名字符统计特征作为输出，构造深度自编码网络模型.并通过计算模型输出值与未处理数据之间的重构误差，实现各层参数与权值的优化，以增强模型的鲁棒性;最后依据提取的域名字符统计特征构造恶意域名判定的决策树.通过在 Alexa 和 Malware domain list 等标准数据集上进行测试.实验结果表明，该模型的检测准确率、精确率、假阴性率和假阳性率值分别为 95.21%、94.17%、2.41%和 3.63%.

关键词： 恶意域名检测；深度自编码；决策树；域名统计特征；重构误差

Malicious domain name detection based on deep auto-encoder and decision tree

ZHAO Hong, CHANG Zhao-bin, WANG Wei-jie

(School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China)

Abstract： Aiming at the problem that the existing malicious domain name detection methods are not effective enough in performance of accuracy rate and the process of feature extraction, a malicious domain name detection algorithm based on deep auto-encoder and decision tree (DAE-DT) is proposed. According to lexical composition and structure of domain name, each domain name is firstly mapped into the feature space and it is normalized. Then the normalized unlabeled domain names are randomly set to 0 as the input of the model, and the statistical features of domain name are used to as the output to construct the deep auto-encoder network model, and the reconstruction error of the unprocessed data and output data is computed to achieve the purpose of optimizing the parameters and weights so that the model is more robust. Finally, a decision tree for malicious domain name detection is constructed based on the statistical features of domain name. In the experiments on Alexa and malware domain list, the proposed detection algorithm yield an accuracy rate of 95.21%, a precision rate of 94.17%, a false negative rate of 2.41%, and a false positive rate of 3.63%.

Key words： malicious domain name detection; deep auto-encoder network; decision tree; statistical feature of domain name; reconstruction error

作者简介：

赵　宏 男，（1971-），博士，教授. 研究方向为并行与分布式处理、自然语言处理、深度学习.

常兆斌（通讯作者） 男，（1995-），硕士研究生. 研究方向为深度学习、空间网络安全、自然语言处理.

E-mail: 1510998508@qq.com.

王伟杰 女，（1994-），博士研究生. 研究方向为深度学习和语音识别.