计算机工程与科学 2012, 34(2) 13-18 DOI: ISSN: 1007--130X CN: 43-1258/TP

论文

基于粗糙集的入侵检测方法研究

史志才，夏永祥

（上海工程技术大学电子电气工程学院，上海 201620）

摘要：

为了改善入侵检测系统的性能，常采用特征提取的方法精简初始数据，以减轻系统的处理负荷，提高检测速度。本文首先采用粗糙集理论对入侵检测系统进行了形式化描述，以信息熵作为测度对连续数值属性进行离散化，使用知识约简对入侵检测的属性特征进行提取，通过信息增益控制属性特征的约简过程，有效剔除了冗余特征，减少了系统的处理负荷，提高了系统的检测时效。实验证实所提出的方法使系统对于PROBING、DoS等典型攻击的训练时间分别缩短2.8和3.2倍，而检测速度分别提高3.3和3.8倍。

关键词： 入侵检测 粗糙集 属性约简 信息熵

Research on an Intrusion Detection Method Based on Rough Sets

SHI Zhi cai，XIA Yong xiang

（School of Electronic and Electrical Engineering, Shanghai University of Engineering Science,Shanghai 201620，China）

Abstract:

In order to improve the performance of intrusion detection systems, the initial data are usually preprocessed by feature extraction so as to reduce the payload of the system and increase its detection speed. At first the rough set theory is used to give a formal description to the intrusion detection systems. Information entropy is applied to the discretization of continuous numerical attributes. Attribute features for intrusion detection are extracted by knowledge reduction. Information gain is used to control the reduction procedure of attribute features. The redundant features are eliminated effectively. The processing payload of the system is reduced and its detection effect is improved. The experiments justify that the proposed method makes the training time of the system to typical attacks for DoS and PROBING is reduced by 2.8 and 3.2 times. The detection speed of the system for two attacks is increased by 3.2 and 4.5 times.

Keywords: intrusion detection；rough set；attribute reduction；information entropy

收稿日期 2010-07-15 **修回日期** 2011-03-28 **网络版发布日期** 2012-02-25

DOI:

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

1. 陈勤, 林朝炽, 徐明.基于P2P的入侵警报发布/订阅系统[J]. 计算机工程与科学, 2009,31(12): 5-8
2. 缪嘉嘉, 张瞩熹, 贾焰, 吴泉源.一种基于数据流的网络威胁监控框架[J]. 计算机工程与科学, 2009,31(12): 23-26
3. 陈亮, 王加阳.基于粗糙集的负载均衡算法研究[J]. 计算机工程与科学, 2010,32(1): 101-104

4. 杨传健, 姚光顺, 马丽生.改进的差别矩阵及其快速求核算法[J]. 计算机工程与科学, 2010,32(3): 78-81
5. 邓辉，梁波，王锋 .基于多模匹配改进算法实现特征签名的动态协议探测技术[J]. 计算机工程与科学, 2010,32(4): 36-38
6. 任晓峰 董占球.基于网络的入侵检测系统弱点分析[J]. 计算机工程与科学, 2002,24(6): 20-22
7. 张瑞霞 王勇.入侵检测系统综述[J]. 计算机工程与科学, 2002,24(6): 27-31
8. 周永权 谢宁新 等.基于粗糙集团的神经网络函数逼近理论[J]. 计算机工程与科学, 2002,24(6): 88-90
9. 陈海涛 胡华平 等.网络入侵检测中高效散列模式树算法的研究[J]. 计算机工程与科学, 2002,24(5): 34-38
10. 徐果毅 朱宁波 朱晓林 卢晓阳.基于颜色直方图熵值及分块主色的图像检索[J]. 计算机工程与科学, 2008,30(9): 44-46
11. 张楠，张建华，陈建英.WSN中基于免疫Multi Agent的入侵检测机制[J]. 计算机工程与科学, 2010,32(5): 10-14
12. 孙波成，邱严峻，梁世庆.基于移动Agent的分布式入侵检测和决策系统[J]. 计算机工程与科学, 2010,32(5): 15-17
13. 张红莉，黄守明.一种基于MA的无线传感器网络IDS模型研究[J]. 计算机工程与科学, 2010,32(5): 18-20
14. 袁浩.基于量子蚁群算法的粗糙集属性约简方法[J]. 计算机工程与科学, 2010,32(5): 82-84
15. 陈凤娟，孙静.粗糙集信息观中的绝对约简[J]. 计算机工程与科学, 2010,32(5): 97-99
