

分级结构的AdaBoost入侵检测方法研究

王勇^{1, 2}, 陶晓玲¹

(1. 桂林电子科技大学 网络中心, 广西 桂林 541004;

2. 北京航空航天大学 计算机学院, 北京 100083)

收稿日期 修回日期 网络版发布日期 2008-3-28 接受日期

摘要 针对目前智能入侵检测方法存在不能同时满足检测精度和检测速度的要求问题, 提出一种分级结构的智能入侵检测方法. 该方法将改进的AdaBoost算法用于入侵特征的选择及构造每一级的Ada-域值分类器, 并通过级连多个分类器来共同完成检测任务. 设计并实现了Linux实时入侵检测实验平台, 在此平台上训练和测试分级结构的智能入侵检测器. 实验结果表明, 该方法降低了运算复杂度; 在保证高的检测率的同时, 降低了虚警率; 提高了处理速度, 更适合入侵检测系统的实时处理要求.

关键词 [入侵检测](#) [AdaBoost算法](#) [特征选择](#) [Ada-域值分类器](#) [分级结构](#)

分类号 [TP393](#) [TP181](#)

Study of the intrusion detection method based on AdaBoost with a hierarchical structure

WANG Yong^{1, 2}, TAO Xiao-ling¹

(1. Network Information Center, Guilin Univ. of Electronic Technology, Guilin 541004, China;

2. School of Computer Science and Eng., BeiHang Univ., Beijing 100083, China)

Abstract

An intelligent hierarchical intrusion detection method is proposed for getting both high precision and high speed. With this method, an improved AdaBoost algorithm is used in selecting intrusion features and constructing an Ada threshold-classifier at every level, and several hierarchical classifiers are combined for detection. A Linux IDS experimental platform is designed and implemented to train and test the intelligent intrusion detector. Experimental results show that the method reduces the complexity of computation, and that the false negative rate is reduced greatly while maintaining the high detection rate. Moreover, the method improves the processing speed and is especially appealing for the real-time processing of the intrusion detection system.

Key words [intrusion detection](#) [AdaBoost algorithm](#) [feature selection](#) [Ada threshold-classifier](#) [hierarchical structure](#)

DOI:

通讯作者 王勇 ywang@guet.edu.cn

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(796KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [复制索引](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“入侵检测”的 相关文章](#)

▶ [本文作者相关文章](#)

· [王勇](#)

·

· [陶晓玲](#)