

图书基本信息

书名：<<支持向量机理论及其在网络安全中的应用>>

13位ISBN编号：9787560625522

10位ISBN编号：7560625525

出版时间：2011-3

出版时间：西安电子科技大学出版社

作者：肖云，王选宏 著

页数：174

字数：150000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<支持向量机理论及其在网络安全中的应>>

内容概要

本书是关于支持向量机理论及其在网络安全中应用的专著。

全书共分为7章。

前两章介绍了网络安全的基本概念, 统计学习理论和支持向量机中的重要概念、原理、特点; 第3~6章介绍了支持向量机在入侵检测、入侵报警过滤、网络安全风险评估和态势预测、病毒程序检测、计算机键盘用户验真、垃圾邮件过滤等网络安全方面的具体应用; 第7章展望了支持向量机理论的发展趋势。

本书理论体系完整, 材料取舍得当, 内容全面新颖, 充分反映近年来支持向量机理论在网络安全中应用的研究动态, 适合从事支持向量机理论研究和网络安全研究的专业技术人员和教师参考, 也可以作为相关学科专业的研究生教材。

书籍目录

第1章 绪论

- 1.1 支持向量机概述
- 1.2 网络安全
 - 1.2.1 网络安全的定义
 - 1.2.2 p2dr动态安全模型
 - 1.2.3 网络安全防护措施
- 1.3 支持向量机在网络安全中的应用

第2章 统计学习理论基础

- 2.1 统计学习理论基础
 - 2.1.1 机器学习
 - 2.1.2 统计学习理论
 - 2.1.3 统计学习理论的发展历程
- 2.2 最优分类超平面
 - 2.2.1 最优超平面
 - 2.2.2 一间隔分类超平面
 - 2.2.3 构造最优超平面
- 2.3 支持向量机
 - 2.3.1 高维空间中的推广能力
 - 2.3.2 核函数
 - 2.3.3 构造支持向量机
 - 2.3.4 支持向量分类机
 - 2.3.5 支持向量回归机
- 2.4 小结

第3章 支持向量机在入侵检测中的应用

- 3.1 入侵检测系统概述
 - 3.1.1 入侵检测系统的基本结构
 - 3.1.2 入侵检测技术分类
 - 3.1.3 入侵检测系统在安全防卫体系中的位置
 - 3.1.4 入侵检测的研究特征
 - 3.1.5 入侵检测的发展历程
- 3.2 支持向量机应用于入侵检测的可行性分析
- 3.3 基于多分类支持向量机的入侵检测方法
 - 3.3.1 c-支持向量分类机
 - 3.3.2 多分类支持向量分类机的构造方法
 - 3.3.3 异构数据集上的核函数
 - 3.3.4 类rbf核函数的修正
 - 3.3.5 基于类rbf核函数的多分类支持向量机
 - 3.3.6 入侵检测实验和结果分析
- 3.4 c-支持向量分类机和最小二乘支持向量分类机在入侵检测中的性能对比
 - 3.4.1 最小二乘支持向量分类机理论
 - 3.4.2 属性约简
 - 3.4.3 性能对比实验和结果分析
- 3.5 one-class支持向量分类机在入侵检测中的应用
 - 3.5.1 one-class支持向量分类机理论
 - 3.5.2 不平衡类别数据的入侵检测实验和结果分析

<<支持向量机理论及其在网络安全中的应>>

3.6 小结

第4章 支持向量机在入侵报警过滤中的应用

4.1 入侵报警过滤概述

4.1.1 入侵检测系统中的误报警及产生的原因

4.1.2 误报警过滤方法的研究现状

4.2 支持向量机应用于入侵报警过滤的可行性分析

4.3 基于支持向量机的入侵报警过滤方法

4.3.1 基本报警属性

4.3.2 误报警过滤的评价指标

4.3.3 基于支持向量机的误报警过滤方法

4.3.4 误报警过滤实验和结果分析

4.4 小结

第5章 支持向量机在网络安全风险评估和态势预测中的应用

5.1 网络安全风险评估和态势预测概述

5.1.1 网络安全风险评估基础理论及研究现状

5.1.2 网络态势预测基础理论及研究现状

5.2 支持向量机应用于网络安全风险评估和态势预测的可行性

5.2.1 支持向量机应用于网络安全风险评估?可行性

5.2.2 支持向量机应用于网络态势预测的可行性

5.3 基于支持向量机的网络安全风险评估方法

5.3.1 基于二叉树的多类分类方法

5.3.2 基于支持向量机的网络安全评估模型

5.3.3 网络安全风险评估实验和结果分析

5.4 基于支持向量机的网络态势预测方法

5.4.1 一支持向量回归机

5.4.2 基于支持向量机的网络态势预测模型

5.4.3 网络态势预测实验和结果分析

5.5 小结

第6章 支持向量机在网络安全其他方面的应用

6.1 支持向量机在病毒程序检测中的应用

6.1.1 计算机病毒防治概述

6.1.2 支持向量机理论应用于病毒程序检测的可行性分析

6.1.3 基于支持向量机的病毒程序检测方法

6.1.4 病毒程序检测实验和结果分析

6.1.5 总结与分析

6.2 支持向量机在计算机键盘用户身份验真中的应用

6.2.1 身份验真概述

6.2.2 支持向量机应用于身份验真的可行性

6.2.3 基于支持向量机的计算机键盘用户验真方法

6.2.4 计算机键盘用户验真实验和结果分析

6.2.5 总结与分析

6.3 支持向量机在垃圾邮件过滤中的应用

6.3.1 垃圾邮件过滤概述

6.3.2 支持向量机应用于垃圾邮件过滤的可行性分析

6.3.3 基于支持向量机的中文垃圾邮件过滤方法

6.3.4 中文垃圾邮件过滤实验和结果分析

6.3.5 总结与分析

6.4 小结

第7章 总结与展望

7.1 总结

7.2 展望

7.2.1 支持向量机理论的未来展望

7.2.2 支持向量机在网络安全中应用的未来展望

参考文献

章节摘录

版权页：插图：4.虚拟机查毒法该技术专门用来对付多态变形计算机病毒。

用软件仿真技术成功地仿真CPU执行，在DOS虚拟机下伪执行计算机病毒程序，安全并确实地将其解密，使其显露本来的面目，再加以扫描。

5.实时反病毒技术该技术为计算机构筑起一道动态、实时的反病毒防线，时刻监视系统当中的病毒活动、系统状况，时刻监视软盘、光盘、因特网、电子邮件上的病毒传染，将病毒阻止在操作系统外部。

优秀的反病毒软件由于采用了与操作系统的底层无缝连接技术，实时监视器占用的系统资源较小，用户不仅完全感觉不到对机器性能的影响，而且不用考虑病毒的问题。

6.1.2 支持向量机理论应用于病毒程序检测的可行性分析病毒程序检测方法主要应用特征来帮助检测，这些特征包括很多不同的属性（如文件名、内容字符串或字节等），并且多从排除恶意程序所产生的漏洞的角度来获得系统的安全性。

但是现实的情况是一个新的病毒程序可能不包括已知的特征。

事实上目前每天大约就能产生8到10个病毒，其中大部分是无法检测出来的，除非获得了它们的特征。病毒程序检测的一个关键问题是要使设计出的检测系统能够检测出未知的病毒程序。

编辑推荐

《支持向量机理论及其在网络安全中的应用》由西安电子科技大学出版社出版。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>