机器学习算法在网络入侵检测中的应用综述

刘阚蓉，李　丹，裴梦迪，张家熹

(安徽工业大学　电气与信息工程学院，安徽　马鞍山　243002)

摘要:在当今的计算机科学中,机器学习是最流行的算法之一,并被广泛运用于各个领域.尽管其具备诸多良好性能,但算法和相关的训练数据依然易受到各种各样的网络威胁.因此,对于网络威胁和相关的机器学习防御技术的深层次研究是极其重要的.如今,许多学者已经研究了包括朴素贝叶斯、决策树、支持向量机、k-邻近算法等在内的学习算法以应对网络威胁.本文中首先从训练阶段和测试阶段这两个方面论述现有网络威胁,其次综述总结了在面对新威胁时被动防御和主动防御等几种改进的机器学习算法,最后对网络威胁和机器学习防御技术在今后的发展趋势进行了展望.

关键词:机器学习;网络入侵;安全

中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1673-260X(2018)12-0044-03

DOI:10.13398/j.cnki.issn1673-260x.2018.12.016

1　引言

近年来互联网技术的快速发展和大规模使用,使得互联网成为最有效的工具和最重要的信息源.易受攻击的网络安全已经成为一个重要的问题,网络安全(Network security)成为当代人们关注的主要问题之一.因此设计一个保护各种数据的网络安全系统以及迫在眉睫. 入侵检测系统 (IDS, Intrusion detection system) 正是一个适应于该需求的重大发明，网络管理者利用入侵检测系统来抵御恶意攻击，因此该系统已成为安全管理的重要组成部分.网络入侵检测系统能检测出对网络的任何企图和滥用的攻击，并能在大量恶意攻击爆发的情况下,保持网络正常性能的运行.

机器学习(ML, Machine Learning)广泛流行于运用于各个检测和识别领域中,在模式识别、图像划分、计算机视觉和网络入侵检测[1]等领域中有着大量的应用.其基本类型分为三种:监督学习、非监督学习和强化学习[2].作为未来智能化社会的基本技术,机器学习的理论研究和算法设计正在加速发展,其最终目标即是获得更加有效的性能、更低的算法复杂度、可靠的预测能力和精确地分类[3].由于代码的开源性、入侵的复杂变化多样性,机器学习其技术本身的安全性问题受到诸多限制,譬如对于一个面部识别系统[4]来说,一些攻击者可通过伪装来破坏其中关键敏感数据以达到入侵的目的,更有甚者,一些攻击者攻击自动驾驶系统和语音控制系统使得汽车无法识别信号灯并无法理解语音含义.因此对传统机器学习算法进行改进显得迫切需要,许多研究者在入侵领域里做出了许多工作,提出了许多有效防御技术算法、模型和系统.为表明时效性,本文选取近五年来机器学习在网络安全中几个改进的新算法加以综述.

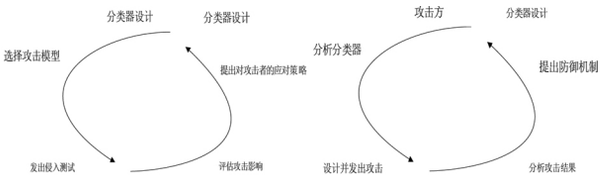
2　机器学习及其改进算法的应用

2.1　机器学习的防卫技术

在面对复杂的网络攻击问题时,传统的机器学习安全性能评估机制已经不适用于应对这些网络威胁.在现有的环境来看,大多数评估技术主要是量化评估各种机器学习的学习性能而非单独的安全性能评估,因而对其算法安全性能没有得到相应的重视.更进一步来说:防御机制的设计者可通过对分类器安全性能的缺陷来引入对抗假设,之后该设计者提出一个防御分类器的免受攻击的对抗措施,与传统被动式防御不同,该策略主动引入假象攻击策略并以积极应对,由此来看存在两种防御机制:被动防御(Reactive defense)与主动防御(Proactive defense).其阐述如图1所示:

收稿日期:2018-09-17

基金项目:国家级大学生创新创业计划训练项目(201810360052)



(a) 被动防御机制　　(b) 主动防御机制

图 1　两种防御机制

在被动防御机制中,常见的攻击者通过分析目标分类器以确认攻击策略并设计出和应用它,分类器设计者可通过分析新增的样本和攻击结果,以适应其攻击策略达到防卫的目的.

2.2　改进机器学习算法在网络入侵中的应用综述

2.1.1　支持向量机改进

传统的支持向量机 (SVMs, Support Vector Machines)算法广泛应用于如垃圾邮件检测、面部识别和温度预测[5]等问题的分类和预测中.该算法是利用已知标签的训练样本来进行预测或检测的监督学习算法. 与其他机器学习算法类似, 传统的 SVMs 也易受到利用系统来进行攻击的入侵者,需要利用多个传感器来进行集中式数据收集、通信和存储.而其应用的关键点在于需要对大规模问题进行大量计算,因此使得支持向量机的在线信息融合和处理能力有所欠缺[6].之后提出的分布式支持向量机(DSVM, Distributed Support Vector Machines)算法是将拥有多节点和智能体通过网络独立处理数据和通信训练信息能力聚集起来的 SVMs. 该体系结构可通过每个节点并行地学习自己的数据,并将学习结果从一个节点转到另一个节点以最终达到全局性能来解决大规模机器学习问题. 此外, DSVM 算法不需要一个融合中心来存储所有的数据,每个节点都执行其本地计算不必与其他节点共享数据内容[7].因此与传统的 SVMs 算法相比,有效地降低了内存开销和数据通信的开销.尽管 DSVM 算法提高了效率,但是分散式训练系统比集中式训练系统更容易受到攻击,DSVM 多一增加的攻击面可使网络中的每个节点都可以受到攻击.攻击者不仅可以选择几个节点来破坏他们的个体学习过程,也可发送错误信息影响其他节点导致最终影响整个 DSVM 网络.

为了解决以上问题,文献[8]提出了将博弈论与 DSVM 算法结合的网络入侵检测方法[9].由于某个攻击者可以使用诸如操控数据样本和改变测试数据这样的攻击,在文献中作者假设攻击者仅可采用修改训练数据标签的攻击方式.而对攻击者更进一步的认知则是体现在如下三个方面:

(1)攻击者的目标:其目的为了摧毁 DSVM 学习者的训练过程并使其分类错误增加;

(2)攻击者的知识储备:假设攻击者有完备的知识理论储备即满足 Kerckhoffs 准则;

(3)攻击者的能力水平:攻击者可通过手动删除数据以达到修改训练数据的目的.

2.2.2　决策树和 k 邻近算法混合检测

将多种机器学习算法结合以提高检测效应的方法备受如今研究者的关注.文献[10]提出了一种混合算法,将二进制分类器和 k–NN 算法结合起来以检测网络入侵. 本算法的检测步骤分为两步:在步骤 1 中, 将网络安全问题视为二进制分类问题.而当类别数过多时(即大于 2 时),此时则是多类别分类问题.事实上,网络入侵检测问题是一个多类别分类问题.在该算法中,应用多个独立的 BCs 来进行检测,通过将网络入侵检测问题转变成二进制问题,以减少由于入侵检测数据集不均衡造成的负面影响.一个 BC 用于检测一类,以此解决少数代表性类别的分类问题. 并采用决策树 C4.5 无参数算法去学习 BCs.如图 2 所示为该检测的流程框架:

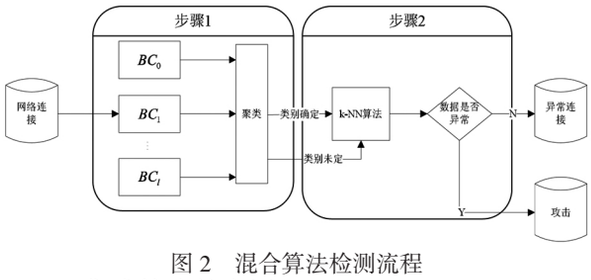


图 2　混合算法检测流程

2.2.3　集成策略的应用

之前所说的一系列传统的机器学习算法(包括对其的改进)均有自己的适应范围,譬如一些适合处理线性可分的问题,一些适合处理线性不可分问题.而随着网络在政府、商业和日常生活中有着广泛的应用,仅仅是单一的某种机器学习算法在网络安全领域不一定适用.对于一个复杂的系统,将机器学习的诸多算法有效结合起来的策略——集成方法被广泛运用.对于不同的问题,集成学习方法有着不同的算法,在分类问题中,投票数越多的类最终定为划分类;而在回归问题里,则是将最大的均值作为最终结果. 常见的分类算法有 Bagging 算法和 Boosting 算法等.文献[11]提出的 multi–perspective 机器学习(MPML:multi–perspective machine

learning)算法就是通过对数据集中创建有区别的特征子集来进行集成学习.MPML 的目的是通过将特征与称之为 perspectives 的已定义的群分类，以提高检测速率.其中每个 perspective 都是种类子集的具体特征，其自我特征在归类时也是互相关联的.因此 MPML 方法的问题关键在于：寻找一个策略利用每个 perspective 之间相互的关联以达到最优可能结果.考虑到某个有着 x 个类别的测试 T,那么测试 T 的特征可通过类别 x 的子集表达,并去 perspectives 中寻找影响力最大的特征.

3 未来与展望

现如今,机器学习作为大数据、云计算和人工智能的核心算法,以此各种各样的网络安全威胁和相应的对抗机器学习策略受到广泛的关注.机器学习在网络威胁中的应用和防御策略将面临以下几个问题:(1)新的基于机器学习的网络威胁将不断出现;(2)对现有机器学习算法面临网络安全威胁时进行可靠的安全性能评估;(3)机器学习算法中数据隐私问题;(4)安全的深度学习成为机器学习安全的关键点;(5)学习算法的优化、性能和损耗成为关注的重点.由此来看,面对网络威胁,机器学习算法的逐步改进会更加优化网络环境以面对各种未知的攻击.

参考文献:

〔1〕Kayacik H G, Zincir-Heywood A N, Heywood M I. Automatically evading IDS using GP authored attacks [C]. Proceedingsof the 2007 IEEE Computational Intelligence in Security & Defense Applications, Honolulu, 2007. Piscataway: IEEE, Apr. 1-5, 2007, pp. 153-160.

〔2〕闫友彪,陈元琰.机器学习的主要策略综述[J].计算机应用研究,2004,21(7):4-10.

〔3〕A. L´Heureux, K. Grolinger, H. F. Elyamany, M. A. M. Capretz. Machine learning with big data: Challenges and approaches [J]. *IEEE Access*, vol. 5, pp. 7776-7797, Jul. 2017.

〔4〕Biggio B, Didaci L, Fumera G, et al. Poisoning attacks to compromise face templates [C]. Proceedings of the 6th International Conference on Biometrics, Madrid, Jun. 4-7, 2013, pp. 132-145.

〔5〕倪凡.基于智能算法优化 SVM 的横向通风过程中温度场预测方法探究 [J]. 粮食储藏,2017,46(01):28-36.

〔6〕贾银山.支持向量机算法及其在网络入侵检测中的应用[D].大连海事大学,2004.

〔7〕R. Zhang and Q. Zhu. A game-theoretic defense against data poisoning attacks in distributed support vector machines [C]. *Decision and Control (CDC), 2017 IEEE 56th Conference on*, Melbourne, Australia. pp. 4582 - 4587, Dec. 2017.

〔8〕Rui Zhang and Quanyan Zhu. A Game-Theoretic Approach to Design Secure and Resilient Distributed Support Vector Machines [J]. arXiv:1802.02907v1 [stat.ML] Feb., 2018.

〔9〕Samuel Rota Bulò, Battista Biggio, Ignazio Pillai, Marcello Pelillo, and Fabio Roli. Randomized Prediction Games for Adversarial Machine Learning[J]. IEEE Transactions on neural networks and learning systems, vol. 28, no. 11, pp. 2466-2478, Nov. 2017.

〔10〕LONGJIE LI, YANG YU, SHENSHEN BAI, YING HOU, AND XIAOYUN CHEN. An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k-NN [J]. vol. 6, pp. 12060-12073, Mar.16,2018.

〔11〕Sean T Miller,and Curtis Busby-Earle."Multi-Perspective Machine Learning a Classifier Ensemble Method for Intrusion Detection," ACM,January 13, 1(2017),7-12.