软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

机器学习在入侵检测中的应用*

袁孝健

(中国矿业大学 计算机科学与技术学院,江苏 徐州 221116)

通讯作者: 袁孝健, E-mail: 06172151@cumt.edu.cn

摘 要: 入侵检测系统(IDS)是一种监控单个计算机或整个网络中是否存在恶意活动(攻击)的软件,当今IDS使用的大多技术无法很好的应对网络攻击中的动态性和复杂性;而各种机器学习技术的应用则可以提高检测率,降低误报率并合理的计算开销.在本文中,我们研究比较了几种方案的性能,并将它们分为基于经典人工智能(AI)的方法和基于计算智能(CI)的方法.最后,我们解释了如何使用 CI 技术的特性来构建智能 IDS.

关键词: 入侵检测;机器学习;人工智能;计算智能;网络安全

中图法分类号: TP309

中文引用格式: 袁孝健. 机器学习在入侵检测中的应用.软件学报. http://www.jos.org.cn/1000-9825/ 0000.htm

英文引用格式: Yuan XJ. Application of machine learning in intrusion detection. Ruan Jian Xue Bao/Journal of Software, 2016 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Application of Machine Learning in Intrusion Detection

YUAN Xiao-Jian

(School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China)

Abstract: An Intrusion Detection System (IDS) is a software that monitors whether there are malicious activities (attacks) in a single or a network of computers, most techniques used in today's IDS cannot cope with the dynamics and complexity of cyber attacks on computer networks. While various techniques of machine learning can improve detection rates, reduce false alarm rates and reasonable computation costs. In this paper, we compare the performance of several such schemes and divide them into methods based on classical artificial intelligence (AI) and methods based on computational intelligence (CI). Finally, we explain how to build efficient IDS using various characteristics of CI techniques.

Key words: intrusion detection; machine learning; artificial intelligence; computational intelligence;network security

如今,政治和商业实体越来越多地参与到复杂的网络战中,以破坏、扰乱或审查计算机网络[6]中的信息内容.在设计网络协议时,需要确保可靠性,防止强大攻击者的入侵,这些攻击者甚至可以控制网络中的一小部分.被控制方既可以发起被动攻击(如窃听、不参与),也可以发起主动攻击(如、干扰、消息丢弃、损坏和伪造).

入侵检测是动态地监视计算机系统或网络中发生的事件,分析它们以发现可能发生的事件的迹象,并经常阻止未经授权的访问[4]的过程.这通常是通过自动地从各种系统和网络来源收集信息,然后分析这些信息以发现可能的安全问题来完成的.

传统的入侵检测和预防技术,如防火墙、访问控制机制和加密.在全面保护网络和系统免受日益复杂的攻击(如拒绝服务)方面有几个限制.此外,基于这种技术构建的系统大多存在较高的假阳性和假阴性检测率,且缺乏持续的自适应能力.没有改变恶意行为.然而,在过去的十年里,一些机器学习(ML)这些技术已经被应用于入侵检测问题,以期提高检测率和适应性.这些技术经常被用来保持攻击知识库的更新和全面.

本文研究了几篇在分布式计算机系统中使用 ML 方法检测恶意行为的论文.在这一领域有大量的研究与文

收稿时间: 2019-10-18; 修改时间: 2019-10-18; 采用时间: 2019-10-18; jos 在线出版时间: 2019-10-18
CNKI 在线出版时间: 2019-10-18

献,因此,我们决定根据两个因素谨慎地选择几篇论文:多样性和引文数量.所谓多样性,即大多数用于 IDS 的 ML 技术都已涵盖,但只有一篇论文是从使用相同技术的一组论文中挑选出来的. 此外,论文的选择是基于它们的引用计数,因为这个因素很大程度上显示了相应的工作对社区的影响有多大.所有的非调查论文被引用至少 100 次.

在第二部分,我们简要陈述了入侵检测面临的主要挑战,并描述了解决这些问题的两种一般方法;第三部分,我们回顾了几种基于传统 AI 的入侵检测技术;第四部分,我们介绍了计算智能的各种核心方法,并描述了文献中提出的几种基于 CI 的算法.

1 挑战和方法

IDS 通常需要处理大量的网络流量、高度不均匀的数据分布、难以实现正常和异常行为之间的决策边界、需要不断适应不断变化的环境[14]等问题.一般来说,挑战在于有效地捕获和分类计算机网络中的各种行为.网络行为的分类策略一般分为两类:误用检测和异常检测[4].

误用检测技术使用签名匹配算法检查网络和系统活动中已知的误用实例.这种技术在检测已知的攻击方面是有效的.但是,新的攻击常常被忽略,从而导致假阴性.IDS 可能会生成警报,但是对每个警报的响应都会浪费时间和资源,导致系统不稳定.为了克服这个问题,IDS 不应在检测到 RST 症状时立即启动消除过程,而应耐心地收集警报和根据它们的相关性来决定.

异常检测系统依赖于构造一个被认为是正常的用户行为模型. 这是通过使用统计或机器学习方法的组合来检查网络传输或系统调用和过程来实现的. 由于任何异常行为都被认为是一种入侵行为, 因此使用异常检测方法可以更有效地检测出新的攻击. 然而, 在一个大的动态系统中, 正常的行为是不确定的, 它会随着时间而改变. 这通常会导致大量的误报, 即假阳性. 基于网络的 IDS 查看传入的网络传输模式, 以确定每个子系统是否正在探测网络以查找易受攻击的计算. 由于响应每个警报会消耗相对大量的时间和资源, 因此 IDS 不应响应它生成的每个警报. 忽视这一事实可能会导致自己造成的的拒绝服务. 为了克服这个问题, 警报应该聚合并相互关联, 以产生更少但更具表现力的显著警报.

我们将基于 ML 的入侵检测方法分为两类:基于人工智能的入侵检测方法((AI)基于计算智能(CI)方法的技术和方法. 人工智能技术是指来自于经典人工智能领域的方法, 如统计建模, 而 CI 技术是指自然启发的方法. 用于处理经典方法无法解决的复杂问题. 重要的 CI 方法有进化计算、模糊逻辑、人工神经网络和人工免疫系统. CI 不同于众所周知的 AI 领域. AI 处理符号知识表示, CI 处理信息的数字表示. 虽然这两个类别之间的界限并不总是清晰的, 文献中也提出了许多混合方法, 但以往的大多数工作主要是基于这两个类别中的任何一个进行设计. 此外, 了解基于自然的技术与传统方法相比有多好是非常有用的.

2 AI 技术

Laskov 等人开发了一个用于检测恶意活动的监督(分类)和非监督学习(聚类)技术比较分析的实验框架.本文提出的监督方法包括决策树、k 近邻(kNN)、多层感知器(MLP)和支持向量机(SVM).无监督算法包括 γ -algorithm、k - means 聚类和单链接聚类.他们定义了两个场景来评估上述两类学习算法.在第一个场景中,他们假设培训和测试数据来自相同的未知分布.在第二个场景中,他们考虑测试数据来自 new(即(看不见)攻击模式. 这个场景帮助我们了解 IDS 在多大程度上可以将其知识泛化为新的恶意模式,这对于 IDS 系统通常是非常重要的, 因为当今成熟的对手往往使用几种入侵模式来逃避现代 IDS.

实验结果[7]表明, 在已知攻击的情况下(第一种情况),监督算法总体上具有更好的分类精度.在这些算法中,决策树算法取得了最好的结果(95%真阳性率,1%假阳性率).接下来的两个最佳算法是 MLP 和 SVM,然后是 k 近邻算法.但是,如果测试数据中存在不可见的攻击,则监督方法的检测率显著下降.这就是无监督技术表现更好的地方,因为它们在可见攻击和不可见攻击的准确性上没有显著差异.图 1 显示了在[7]中评估的所有方法的平均真/假阳性率.如图所示,尽管非监督方法在两种情况下都给出了更健壮的结果,但监督技术通常表现得更好.

Zanero 和 Savaresi[17]描述了一个基于非监督学习的 TCP/IP 网络中的异常的两层 IDS 架构:第一层是一个非监督的集群算法,它从网络数据包的有效负载构建小型模式. 换句话说,TCP 或 UDP 数据包被分配到代表正常和异常流量的两个集群. 第二层是经过优化的传统异常检测算法,该算法通过提高数据包有效载荷内容的可用性进行了改进. 这项工作背后的动机是,无监督学习通常比监督学习更有效地传播攻击模式. 方法:因此,我们希望这样的架构能够更有效地抵抗多态攻击.

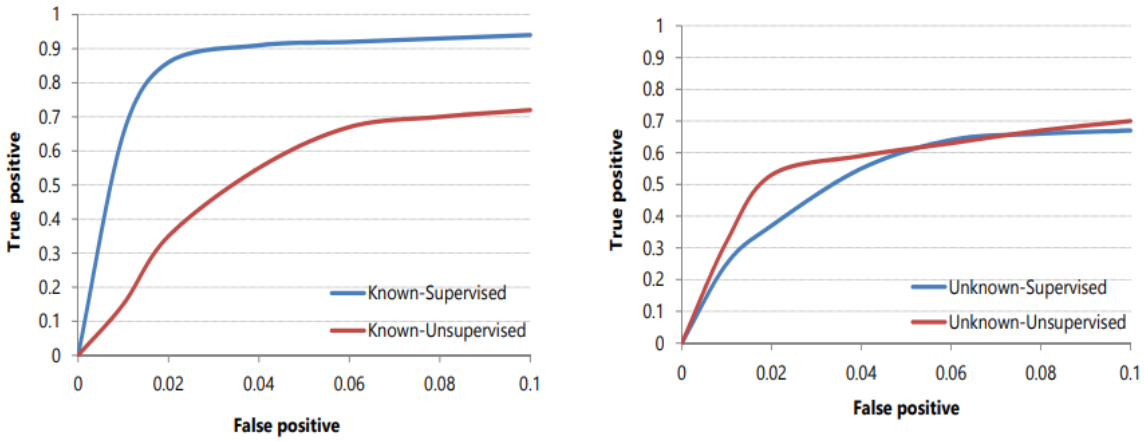

Fig 1 Average of detection rates for methods evaluated in [7] in two scenarios: test data contains only known attacks (left) and test data contains unknown attacks (right)

图 1:两种情况下[7]中评估方法的平均检出率:测试数据只包含已知的攻击(左)和包含未知攻击的测试数据(右)

Lee 和 Solfo[8]使用数据挖掘技术构建了一个分类器来检测网络中的异常.它们实现了两种通用的数据挖掘算法,这两种算法对于描述程序或用户的正常行为至关重要.他们提出了一种基 agen 的入侵检测系统体系结构,其中学 agent 不断地计算并向 agent 提供更新的检测模型.他们对 Sendmail1 系统调用数据和网络 tcpdump 数据进行了实验,以证明他们的分类模型在检测异常方面的有效性.最后,他们认为在入侵检测中使用数据挖掘方法最重要的挑战是,他们需要大量的审计数据来计算概要规则集.

Sommer 和 Paxson[13]研究了基于 mlb 的入侵检测的大量研究与缺乏此类系统的操作部署之间的不平衡.它们识别了网络入侵检测面临的特殊挑战,并为今后加强基于 mlb 的入侵检测的研究提供了一套指导方针.更具体地说,他们认为基于异常的 IDS 需要异常值检测,而 ML 的经典应用是一个分类问题,用于发现活动之间的相似性.的确,在某些情况下,离群点检测问题可以建模为一个分类问题,其中分为正常和异常两类.在机器学习中,需要训练一个系统的所有类的训练模式,而在异常检测中,只能训练正常的模式.这意味着异常检测更适合于发现已知攻击的变体,而不是以前未知的恶意活动.这就是为什么 ML 方法比入侵检测更有效地应用于垃圾邮件检测.

3 基于 CI 技术

在这一部分中,我们介绍了几种基于计算智能的核心技术的算法;遗传算法(第 4.1 节)、人工神经网络(第 4.2 节)、模糊逻辑(第 4.3 节)和人工免疫系统(第 4.4 节).

3.1 遗传算法(GA)

遗传算法的目标是寻找问题的最优解.每个问题的可能解都被表示为一个称为基因组或染色体的位(基因)序列.遗传算法从一组基因组(群体)和一个称为度量每个基因组质量(优度)的评价函数开始.该算法使用两个称为交叉算子和变异产生新的后代(解),然后对其进行评估.交叉决定了群体中父母的各种特性如何被后代所继承.变异是单个基因的自发改变.

Sinclair 等人[12]利用遗传算法和决策树为入侵检测专家系统创建规则.它支持分析人员从正常网络传输中识别异常网络活动的工作.本文利用遗传算法对网络传输进行了简单规则的进化.每条规则由一个基因组表示,基因组的初始种群是一组随机规则.每个基因组由 29 个基因组成:8 个为源 IP,8 个为目的 IP,6 个为源端口,6 个为目的端口,1 个为协议.

适应度函数基于每个规则在预先分类的数据集上的实际表现.分析师将包含连接的数据集标记为正常或异常.该系统使用分析人员创建的训练集进行规则开发和分析人员决策支持.如果一个规则完全匹配一个不正常的连接,那么它将得到一个奖励,如果它匹配一个正常的连接,那么它将受到惩罚.因此,代会倾向于只匹配入侵连接的规则.一旦遗传算法达到一定的世代数,它就会停止,并产生最好的基因组(即基因组).,规则)被选择.生成的规则集可以作为 IDS 内部的知识,用来判断网络连接和相关行为是否是潜在的入侵

传统的遗传算法倾向于收敛于一个称为全局极大值的单一最优解.因为[12]的算法需要一组最佳的唯一规则,这是一种受自然启发的技术,称为小生境,它试图创建在局部极大值上收敛的子种群.各种小生境技术的细节在[10]中进行了描述.

3.2 人工神经网络

神经网络由一组被称为神经元的处理单元组成,这些处理单元按照给定的拓扑结构高度互连.神经网络具有通过示例学习并从有限的、有噪声的和不完整的数据中进行概括的能力.它们已成功地应用于广泛的数据密集型应用中.

Mukkamala 等人[11]描述了使用神经网络和支持向量机(SVM)进行入侵检测的方法,其目的是发现描述用户行为的模式或特征,从而建立分类器来识别异常.SVM 是一种有监督的学习机器,它在高维特征空间中表示训练向量,并按其类别对每个向量进行标记,SVM 在不同类别之间的间隔(间隔)上确定一个上界,以使泛化误差最小,泛化误差是指对未知向量进行分类时的误差量,SVM 通过确定一组训练数据来对数据进行分类,这些训练数据称为支持向量,它们在特征空间中近似于一个 Hy 平面.

Mukkamala 等人[11]使用支持向量机对入侵检测系统中的特征向量进行非线性分类.使用 7312 个数据点对 SVM 进行训练,使用来自 KDD4 的 6980 个测试点进行测试.每个点都位于 41 维空间中,训练使用径向基函数(RBF)5 完成.该方法利用径向基函数逼近非线性超平面,将正常类和异常类分离开来.利用该支持向量机对测试点进行分类,准确率达到 99.5%.他们还使用三个多层前馈神经网络对相同的测试点进行分类.使用相同的 7312 点训练集对神经网络进行训练,对不同神经网络结构进行实验的最佳结果是检测率为 99.25%.虽然支持向量机的识别率比人工神经网络的识别率高,但它只能用于二分类,这对于需要多个类的识别来说是一个很大的限制.

3.3 模糊逻辑

模糊逻辑是一种基于真度的计算方法,而不是通常的真或假布尔逻辑.对于模糊空间,模糊逻辑允许一个对象同时属于不同的类.这使得模糊逻辑成为入侵检测的一个很好的选择,因为安全本身就包含了模糊性,并且正常和异常之间的边界没有很好的定义.此外,入侵检测问题涉及到采集数据中的许多数值属性和各种派生的统计度量.直接在数值数据上建立模型通常会导致较高的检测误差.仅仅轻微偏离模型的行为可能不会被检测到,或者正常行为的微小变化可能导致假阳性.使用模糊逻辑,可以对这些小偏差进行建模,从而使假阳性率/负性率保持较小.每个模糊规则都有以下一般形式,

IF condition THEN conclusion [weight],

其中,条件(condition)是使用模糊与和模糊或等模糊逻辑运算符定义的模糊表达式,结论(conclusion)是原子

表达式,权值(weight)是[0,1]中表示规则置信度的实数.

Gomez 和 Dasgupta [2]表明, 使用模糊逻辑可以降低判断侵入性活动的误报率. 他们定义了一组模糊规则来定义计算机网络中的正常和异常行为,以及一个模糊推理引擎来确定入侵.他们使用一种遗传算法来生成模糊分类器,这是一组定义在上述形式中的模糊规则.每个模糊规则由一个基因组表示,利用遗传算法寻找最佳的基因组(模糊规则)加入到模糊分类器中.作者利用 KDD 评估数据进行了实验,将 22 种不同类型的攻击分为 4 类:拒绝服务(DoS)、来自远程计算机的未授权访问(R2L)、对本地超级用户(root)特权的未授权访问(U2R)和探测(PRB).结果表明,该算法的总体真阳性率为 98.95%,假阳性率为 7%.

3.4 人工免疫系统(AIS)

自然免疫系统由分子、细胞和组织组成,这些分子、细胞和组织建立了机体对细菌、病毒和寄生虫等病原体感染的抵抗力.它们将病原体与自身细胞区分开来,并消除病原体.这为计算机安全系统,特别是 IDS 提供了一个巨大的灵感来源.人工免疫系统是基于自然免疫系统行为的计算智能系统.

Hofmeyr 和 Forrest[3]提出了适用于各种计算机安全问题的 RST 免疫启发模型.它们的模型专门用于检测基于 TCP/IP 的局域网中的入侵行为.它们构建一个包含正常系统调用序列的数据库,这些系统调用序列充当程序正常行为的自身定义.并以此作为异常检测的基础.每个 TCP 连接由一个三元组来建模,它编码发送者的地址、接收者的地址和接收者的端口号.检测器通过负选择算法(NSA)随机产生.除了 NSA 产生的刺激或耐受免疫反应的信号外,他们还使用了第二种信号(称为协同刺激).对通过 NS 程序检测到的异常进行校正.在该系统中,为了减少系统的虚警(自动免疫),需要人工产生这种信号.

Kim 等人[5]介绍和分析了免疫计算机安全领域的主要进展,并对未来的发展提出了建议.他们总结了六个理想的免疫特性:分布式、多层、自组织、轻量级多样化和一次性.他们解释说,人类的免疫系统是通过免疫网络分布的,它产生独特的抗体集,以提供前四个需求.它是通过基因库进化、负选择和克隆来实现自组织的.最终它是轻量级的,通过近似的结合,记忆细胞,和基因表达来提高效率.

Zamani 等人[15,16]描述了一种基于危险理论的分布式系统入侵检测的社会免疫算法.危险理论是一种免疫模型,其思想是免疫系统不识别自我和非自我,而是识别造成破坏的事件.作者提出了一个多智能体环境,通过计算模拟自然免疫系统的行为,有效地降低了假阳性率.通过对无线传感器网络中分布式拒绝服务攻击检测问题的研究,表明了该模型在实际应用中的有效性.

Dasgupta[1]提出了一种基于 AIS 的多智能体 IDS.他定义了三种类型的代理;监控代理,漫游在网络和监控各种复健同时在多个水平(用户数据包级别),沟通者代理用于扮演免疫细胞之间的信号称为淋巴因子和决定/行动代理人做出决定基于收集当地的警告信号.每种类型的代理的角色都是惟一的,尽管它们可以协作工作.遗憾的是,这项工作没有提供任何实验结果,这使得读者很难将该系统的性能与其他基于 ML 的 IDS 进行比较.

4 结论

本文综述了几种基于机器学习技术的入侵检测算法.ML 技术的特点使得能够设计出检测率高、误报率低的入侵检测系统,同时系统自身能够快速适应不断变化的恶意行为.我们将这些方案分为两类:基于人工智能(AI)和基于计算智能(CI).虽然这两类算法有许多相似之处,但基于 CI 的技术的一些特点,如适应性、容错性在面对噪声信息时具有较高的计算速度和抗误码能力,符合建立智能入侵检测系统的要求.

References:

[1] Dipankar Dasgupta. Immunity-based intrusion detection system: A general framework. In Proceedings of the 22nd National Information Systems Security Conference (NISSC). Arlington, Virginia, USA, 1999.

[2] Jonatan Gomez and Dipankar Dasgupta. Evolving fuzzy classifiers for intrusion detection. In Proceedings of the 2002 IEEE Workshop on Information Assurance, West Point, NY, USA, 2002.

[3] Steven A. Hofmeyr, Stephanie Forrest, and Anil Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, 6(3):151–180, August 1998.

[4] Peter Mell Karen Scarfone. Guide to intrusion detection and prevention systems (idps). National Institute of Standards and Technology, NIST SP - 800-94, 2007. Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50951.

[5] Jungwon Kim, Peter J. Bentley, Uwe Aickelin, Julie Greensmith, Gianni Tedesco, and Jamie Twycross. Immune system approaches to intrusion detection – a review. Natural Computing, 6(4):413–466, December 2007.

[6] Andrew F. Krepinevich. Cyber warfare: A nuclear option?, 2012. Center for Strategic and Budgetary Assessments, Washington, DC, USA, 2012.

[7] Pavel Laskov, Patrick Dssel, Christin Schfer, and Konrad Rieck. Learning intrusion detection: Supervised or unsupervised? In Image Analysis and Processing ICIAP 2005, volume 3617 of Lecture Notes in Computer Science, pages 50–57. Springer Berlin Heidelberg, 2005.

[8] Wenke Lee and Salvatore J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium - Volume 7, SSYM'98, pages 6–6, Berkeley, CA, USA, 1998.

[9] Wei Li. Using genetic algorithm for network intrusion detection. In Proceedings of the US DoE Cybersecurity Conference, Kansas City, KS, USA, 2004.

[10] Brad Miller and Michael Shaw. Genetic algorithms with dynamic niche sharing for multimodal function optimization. In Proceedings of IEEE International Conference on Evolutionary Computation, pages 786–791, 1996.

[11] Srinivas Mukkamala, Guadalupe Janoski, and Andrew Sung. Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 International Joint Conference on Neural Network (IJCNN), volume 2, pages 1702–1707, 2002.

[12] Chris Sinclair, Lyn Pierce, and Sara Matzner. An application of machine learning to network intrusion detection. In Proceedings of the 15th Annual Computer Security Applications Conference, ACSAC '99, Washington, DC, USA, 1999.

[13] Robin Sommer and Vern Paxson. Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the IEEE Symposium on Security and Privacy, 2010.

[14] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Review: Intrusion detection by machine learning: A review. Expert Syst. Appl., 36(10):11994– 12000, December 2009.

[15] Mahdi Zamani, Mahnush Movahedi, Mohammad Ebadzadeh, and Hossein Pedram. A DDoS-aware IDS model based on danger theory and mobile agents. In Proceedings of the 2009 International Conference on Computational Intelligence and Security - Volume 01, CIS '09, pages 516–520, Washington, DC, USA, 2009. IEEE Computer Society.

[16] Mahdi Zamani, Mahnush Movahedi, Mohammad Ebadzadeh, and Hossein Pedram. A danger-based approach to intrusion detection. CoRR, abs/1401.0102, 2014.

[17] Stefano Zanero and Sergio M. Savaresi. Unsupervised learning techniques for an intrusion detection system. In Proceedings of the 2004 ACM symposium on Applied computing, SAC '04, pages 412–419, New York, NY, USA, 2004.

附中文参考文献:

[1] 许戈静.基于机器学习方法的入侵检测技术[J].信息通信, 2015(12):127-128.

[2] 颜谦和,颜珍平.遗传算法优化的神经网络入侵检测系统[J].计算机仿真,2011(04):141-144

[3] 王晟,赵壁芳.基于模糊数据挖掘和遗传算法的网络入侵检测技术[J].计算机测量与控制,2012(03):660-663.