

基于 Agent 的网络入侵检测专家系统

何 波

(重庆理工大学 计算机科学与工程学院, 重庆 400050)

摘 要: 大多数网络入侵检测专家系统采用单一的推理机制, 而基于规则推理和基于事例推理这两种推理机制各有优缺点, 采用单一推理机制会降低入侵检测的准确性. 文中提出了基于规则和事例的入侵检测混合推理机制, 在此基础上, 设计了一个基于 Agent 的网络入侵检测专家系统 (AIDES). 实验结果表明, 文中设计的 AIDES 是有效的.

关键词: 入侵检测; 基于规则的推理; 基于事例的推理; 专家系统

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)09-0093-03

Intrusion Detection Expert System of Network Based on Agent

HE Bo

(School of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400050, China)

Abstract: Most intrusion detection expert system of network adopted single reasoning mechanism. However, rule-based reasoning or case-based reasoning had advantages and disadvantages. The adoption of single reasoning mechanism would lead to inaccurate intrusion detection. The paper proposed mixed reasoning mechanism based on rule-based reasoning and case-based reasoning. On the base of this, the paper designed an intrusion detection expert system of network based on agent, namely AIDES. The experiments indicate that AIDES is effective.

Key words: intrusion detection; rule-based reasoning; case-based reasoning; expert system

1 引言

入侵检测系统 (Intrusion Detection System, IDS)^[1] 作为防火墙之后的第二道安全闸门, 是网络防护体系的重要组成部分, 能够检测出多种形式的入侵行为. 随着人工智能技术的迅速发展, 入侵检测与人工智能技术的结合成为一个重要的研究方向.

Agent^[2] 是可计算实体或程序, 它可以感知外界环境并自治运行, 实现其设计者和使用者的一系列目标. Agent 具有自治性、反应性和自适应性等特点.

专家系统^[2] 是人工智能的一个分支, 它是一个具有大量专门知识和经验的程序系统, 可根据某一领域内的专家知识和经验进行推理和判断, 模拟人

类专家的决策过程, 以解决那些需要专家解决的复杂问题.

目前已有少量的网络入侵检测专家系统, 但是仍然存在一些问题, 主要包括:

(1) 多数网络入侵检测专家系统采用单一的推理机制, 或者基于规则的推理, 或者基于事例的推理. 采用单一推理机制会造成入侵检测的不准确性;

(2) 多数网络入侵检测专家系统缺乏自学习能力, 难以实现知识和事例的有效更新.

文中提出了基于规则和事例的网络入侵检测混合推理机制, 设计了基于 Agent 的网络入侵检测专家系统 (AIDES). 该系统利用混合推理机制提高了入侵检测的准确性, 通过评价和学习机制增强了入侵检测的自学习能力.

2 网络入侵检测混合推理机制

2.1 基于规则的推理

传统的专家系统一般采用基于规则的推理 (rule-based reasoning, RBR) 方法. 在这种推理模式下, 知识被表示成产生式规则. 产生式规则的一般形式是:

if < 前提 > then < 结论 > (< 规则置信度 >)

其中前提部分表示能与数据匹配的任何模型, 结论部分表示满足前提时可以得出的结论; 如果有规则置信度, 则表示满足前提时得出结论的可信程度. 对带有规则置信度的规则进行推理是一种不精确推理技术.

基于规则的推理是先根据推理策略从规则库中选择相应的规则, 再匹配规则的前提部分, 最后根据匹配结果得出结论. RBR 在求解小规模的问题时, 效率较高; 但只能对事先预想到并能与规则前提匹配的事件进行推理, 存在知识获取的瓶颈问题.

2.2 基于事例的推理

基于事例的推理 (case-based reasoning, CBR) [3] 是利用以往求解类似问题的以事例形式表示的经验知识进行推理, 从而获得当前问题求解结果的一种推理模式. 一个有效的事例表示包括三个部分的内容: 事例发生的原因或背景; 事例的特点及过程; 事例的解决方法 and 结果. 事例推理的关键步骤包括事例检索、事例重用、事例修改/修正和事例保留等. CBR 避免了采用 RBR 方法进行知识获取时的瓶颈问题, 利用相关事例扩大了解决问题的范围, 简化了求解过程, 解的质量也得到提高. CBR 的缺点是在处理小规模问题时, 其推理效率不高.

2.3 基于规则和事例的混合推理机制

文中提出的基于规则和事例的网络入侵检测混合推理机制如下:

(1) 构建入侵监测知识库, 确定知识库中各个规则的规则置信度和优先级别; 同时, 构建入侵事例库, 对事例进行分类, 并确定每类中事例的优先级别. 转向(2);

(2) 按照规则优先级别的高低进行基于规则的不精确推理, 将事件与规则前提进行匹配, 得到规则前提与事件匹配值, 根据结论置信度 = 规则前提与事件匹配值 $\times$ 规则置信度, 可以推算出结论置信度. 如果该结论置信度大于或等于设定阈值, 则可直接

得出相应结论, 推理结束; 否则, 如果所有匹配规则的结论置信度都小于设定阈值, 则转向(3);

(3) 对基于规则推理不能确定的事件采用基于事例的推理. 首先进行事例检索, 从事例库中找到该事件所属的事例类, 再根据该类中事例的优先级别进行匹配, 得到事例与事件的匹配值, 根据事例的优先级别和事例与事件的匹配值确定最相似的事例; 再对该事例进行重用, 要利用到该事例中的解决方法 and 结果等内容; 然后根据事件的特点对原有事例进行修改或修正; 最后找出相应的解法, 推理结束.

3 入侵检测专家系统(AIDES)

文中采用 Agent 技术, 设计了一个既有专家知识库, 又有事例库, 具有自学习能力的网络入侵检测专家系统 (AIDES). AIDES 由四个部分组成: 用户界面模块、预处理模块、推理模块和评价学习模块. AIDES 的结构如图 1 所示.

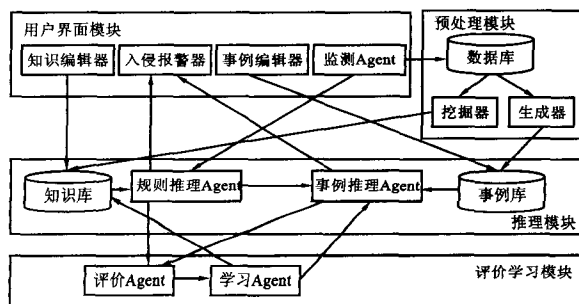


图1 基于 Agent 的入侵检测专家系统(AIDES)

用户界面模块是用户与系统交互的接口, 包括知识编辑器、事例编辑器、监测 Agent 和入侵报警器. 知识编辑器的作用是用户根据领域知识和专家经验来编辑入侵检测规则. 事例编辑器的作用是用户根据专家经验来编辑事例. 监测 Agent 的作用是将采集到的网络数据包和收集到的主机日志数据进行数据预处理和分析, 一方面将这些处理后的网络数据存放到数据库, 另一方面将对这些处理后的数据进行特征提取和转换, 提供给规则推理 Agent 进行处理. 入侵报警器的作用是将规则推理机和事例推理机推理出的入侵检测报警信息展示给用户.

预处理模块包括数据库、挖掘器和生成器. 数据库存放的是经过监测 Agent 收集处理的网络数据, 是生成知识库和事例库的基础. 挖掘器的作用是对数据库信息进行关联规则[4]的挖掘, 然后采用 SLIQ 算法[5]分类, 构建以规则形式表示的知识库. 生成器的作用根据数据库信息构建事例库.

推理模块是 AIDES 的核心部件,包括知识库、规则推理 Agent、事例库和事例推理 Agent。知识库是规则推理机进行规则推理的依据,知识库中的知识获取来自三个方面:其一,通过知识编辑器获取规则;其二,从挖掘器获取规则;其三,通过评价和学习机制,从学习 Agent 实现规则的动态更新。知识库中的规则均设置了规则置信度和优先级别。

规则推理 Agent 的作用是根据 2.3 节提出的混合推理机制的第(2)步骤进行基于规则的不精确推理。访问行为经过规则推理判断,有三种情况:一是正常访问行为;二是异常访问行为;三是不确定访问行为。对正常访问行为不报警,将规则前提与事件的匹配值提交给评价器;对异常的访问行为直接提交给入侵报警器,也将规则前提与事件的匹配值提交给评价器;对不确定访问行为交给事例推理 Agent 进行进一步处理。

事例库存放的是以往发生过的、典型的和有代表性的入侵事例,一个事例包括问题描述、事例特征、解决方案等。事例库中的事例需要进行分类,并确定每类中事例的优先级别。在利用知识库进行规则推理的基础上,进行基于事例的推理可以更大限度地提高入侵检测的准确性。事例的获取来自三个方面:一是通过事例编辑器获取事例;二是利用生成器从数据库中抽取事例;三是通过评价和学习机制,从学习 Agent 实现事例的动态更新。

事例推理 Agent 的作用是根据 2.3 节提出的混合推理机制的第(3)步骤进行推理。经过事例推理后,事例推理机将确定的入侵信息提交给入侵报警器;将事例与事件的匹配值提交给评价 Agent。

评价学习模块是实现自学习入侵检测的关键部件,包括评价 Agent 和学习 Agent。评价 Agent 的作用是对规则推理 Agent 和事例推理 Agent 提交的事件处理过程进行评价,将评价的信息提交给学习 Agent。评价 Agent 采用自动获取评价信息的方式,对匹配过规则的评价值由规则前提与事件的匹配值决定;对匹配过事例的评价值由事例与事件的匹配值决定。学习 Agent 的作用是根据评价信息更新知识库中的知识和更新事例库中的事例。学习 Agent 采用的是自学习方式,根据对规则的评价值来调整相应规则的规则置信度和优先级别;根据对事例的评价值来调整相应事例的优先级别。

4 原型系统及实验

编程工具为 Visual C# 2008,采用 Win-

dows2003 作为软件支持平台,SQL-Server2005 作为数据库管理系统。利用 AIDES 的原型系统对混合推理机制进行了模拟实验,实验的目的是将采用规则推理的入侵检测、采用事例推理的入侵检测和混合推理机制的入侵检测进行对比。对原型系统进行了 3 次测试,每次测试均是模拟 20 次正常事件和 20 次入侵事件。第 1 次是对规则推理的入侵检测进行测试,第 2 次是对事例推理的入侵检测进行测试,第 3 次是对混合推理机制的入侵检测进行测试。模拟实验结果如图 2 所示。

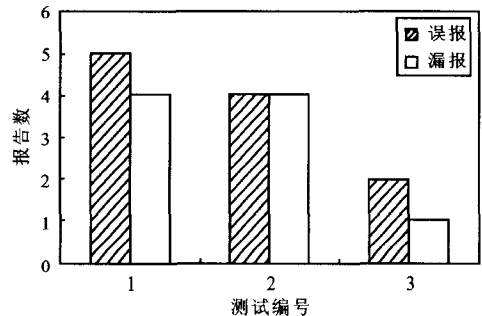


图 2 原型系统模拟实验结果

从测试结果看,第 1、2 次测试,漏报数或误报数较高;而第 3 次采用了论文提出的混合推理机制,漏报数和误报数都较低。实验表明,大多数入侵检测专家系统采用的单一的推理机制可能会造成严重的误报与漏报,而采用文中提出的混合推理机制,充分利用了两者的优点,可以降低漏报率和误报率。

5 结束语

文中提出了基于规则和事例的入侵检测混合推理机制,在此基础上,设计了基于 Agent 的网络入侵检测专家系统(AIDES)。实验表明,采用文中提出的混合推理机制,可以降低漏报率和误报率,文中设计的 AIDES 是有效的。

参考文献:

- [1] 金名. 密码学与网络安全 [M]. 2 版. 北京:清华大学出版社, 2009.
- [2] Jones M T. 人工智能 [M]. 北京:电子工业出版社, 2009.
- [3] Vong C M, Leungb T P, Wong P K. Case-based reasoning and adaptation in hydraulic production machine design[J]. Engineering Applications of Artificial Intelligence, 2002(15):567-585.
- [4] 俞勇. Web 数据挖掘 [M]. 北京:清华大学出版社, 2009.

(下转第 99 页)

(2) 基于MDA的云环境软件开发建模过程:由于云计算SaaS解决方案的复杂性(如服务范围的定义,每个服务的元素)和可用技术平台的多样性等,用MDA方法设计新模型是一个必须的工作.新的基于MDA的云环境下的建模方法应该加以研究.

(3) 云计算软件开发下MDA的PIM可靠准确转换成PSM的转换机制:MDA流程中最为关键并且困难的一步,是从PIM生成一个PSM.它要求对要应用的基础技术具有丰富且巩固的知识,另一方面,源模型(PIM)必须具备自动生成PSM所要求的足够信息量.在云计算这个特殊的环境下,研究模型转换规则,制定实现PIM到PSM的正确转换机制,需要进一步的技术研究.

(4) 基于云存储的MDA软件构件库的管理机制与构件检索算法:云计算中的SaaS强调用户可以根据需要自由定制软件功能,即云计算环境下的软件必须要满足能够让用户根据需要选择自己想要的功能,甚至软件本身的实现机制.构件技术正是对此种思想最强有力的支撑的技术之一.构件库的管理与构件的检索是需要研究的两个关键问题.

参考文献:

- [1] Ashley McNeile, Ella Roubtsova. Composition semantics for executable and evolvable behavioral modeling in

MDA[C]//ACM. New York, 2009.

- [2] Pekka Aho, Matti Mki, Daniel Pakkala, et al. MDA-based tool chain for web services development[C]//ACM, WEWST'09. New York, 2009.
- [3] Dean J, Ghemawat S. MapReduce: simplified data processing on large clusters[C]//Proceedings of the 6th Symposium on Operating System Design and Implementation. New York: ACM Press, 2004: 137-150.
- [4] Michael Cusumano. Cloud computing and SaaS as new computing platforms[J]. Communications of the ACM, 2010, 53(4): 27-29.
- [5] 王学斌, 王怀明, 吴泉源, 等. 一种模型转换的编织框架[J]. 软件学报, 17(6): 1423-1435.
- [6] 任铭亮, 刘勇. 基于MDA/PIM的组件自动生成技术的研究[J]. 微电子学与计算机, 2009, 26(5): 71-75.
- [7] 周相兵, 马洪江, 杨兴江. 一种基于云计算的语义Web服务组合模型研究[J]. 微电子学与计算机, 2009, 26(8): 206-210.
- [8] 袁梅冷. 面向构件与方面的MDA软件开发新模型初探[J]. 计算机工程, 2007, 28(17): 42-44.

作者简介:

解绍词 男, (1979-), 硕士, 讲师. 研究方向为分布式计算、通信软件等.

葛君伟 男, (1961-), 博士, 教授. 研究方向为分布式计算、软件工程等.

(上接第95页)

- [5] Manish Mehta, Rakesh Agrawal, Jorma Rissanen. SLIQ: a fast scalable classifier for data mining[C]//Proceedings of the 5th International Conference on Extending Database Technology. France: Avignon, 1996, 18-32.
- [6] 肖立中, 邵志清, 马汉华, France: Avignon, 网络入侵检测中的自动决定聚类数算法[J]. 软件学报, 2008, 19(8): 2140-2148.

- [7] 代伟, 刘敏, 余永武. 基于Ad Hoc网络的混合入侵检测算法[J]. 重庆理工大学学报: 自然科学版, 2008, 22(3): 75-78.

- [8] 何波, 程勇军, 涂飞, 等. 自适应入侵检测专家系统模型[J]. 计算机工程, 2007, 33(10): 158-160.

作者简介:

何波 男, (1978-), 副教授. 研究方向为信息安全、数据挖掘.