第33卷 第10期 计 算 机 工 程 2007年5月
Vol.33 No.10 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)10—0158—03 文献标识码：A 中图分类号：TP311

自适应入侵检测专家系统模型

何 波，程勇军，涂 飞，杨 武
(重庆工学院计算机科学与工程学院，重庆 400050)

摘 要：大多数入侵检测系统不能适应网络环境的变化，即不具备自适应性。针对此情况，提出了自适应策略，该策略由状态空间和策略空间构成，状态空间用来描述网络环境，策略空间用来描述采用的策略。对于状态空间中的某一具体的环境状态，在策略空间存在唯一的策略与之对应。在构建自适应策略的基础上，将基于规则的推理和基于事例的推理相结合，设计了自适应入侵检测专家系统模型(AIDESM)。AIDESM 既有专家知识库，又有入侵事例库，利用自适应策略和评价学习机制，能够实现自适应入侵检测。实验结果表明，该自适应策略是比较有效的。

关键词：入侵检测；数据挖掘；专家系统；自适应

Adaptive Intrusion Detection Expert System Model

HE Bo, CHENG Yongjun, TU Fei, YANG Wu
(Department of Computer Science and Engineering, Chongqing Institute of Technology, Chongqing 400050)

【Abstract】 Most intrusion detection system can not adapt to the variation of network environment. Aiming at this problem, this paper proposes an adaptive strategy which composed of state space and strategy space. The former described network environment and the latter described the strategies. There is an exclusive strategy corresponds to a certain environment state in state space. On the base of the adaptive strategy, it designs an adaptive intrusion detection expert system model based on rule-based reasoning and case-based reasoning, namely, AIDESM, which had expert knowledge database and intrusion case database. It takes advantage of adaptive strategy and evaluation & learning mechanism to realize adaptive intrusion detection. The experiments indicate that adaptive strategy is effective.

【Key words】 Intrusion detection; Data mining; Expert system; Adaptive

随着Internet的迅速发展，信息保密性和网络安全性变得越来越重要。入侵检测系统[1,2]作为防火墙之后的第2道安全闸门，能够检测出多种形式的入侵行为，是安全防御体系的一个重要组成部分。目前已存在很多入侵检测系统，但这些系统基本不具备自适应性，当网络环境发生改变时，系统难以适应环境的变化，导致对入侵行为的大量漏报和误报。专家系统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。

本文提出了自适应策略，在此基础上，将基于规则的推理和基于事例的推理相结合，设计了自适应入侵检测专家系统模型(AIDESM)。该模型能自动适应复杂多变的网络环境，通过评价学习机制增强了自学习能力，利用专家系统提高了入侵检测的准确性。

1 自适应策略

1.1 自适应策略的必要性

现在很多入侵检测系统只有一种检测策略，对任何环境都用这个策略来检测，在检测强度与范围上没有什么变化。这使得入侵检测系统的误报与漏报比较严重，使得系统的可信度降低，也降低了用户对入侵检测系统的信心。解决的主要方法是构建自适应策略，让检测策略随着网络环境的改变而调整，通过不同的策略来应对不同的环境。

1.2 自适应策略的描述

自适应策略解决的问题是如何表述入侵检测系统的网络环境变换，以及在某种环境下采取什么样的策略。引入状态空间和策略空间来描述自适应策略。状态空间用来描述网络环境，策略空间用来描述可能采用的策略。对于状态空间中的某一具体的环境状态，在策略空间存在唯一的策略与之对应。

网络环境状态C可表示为

$$C=(e_1,e_2,\ldots,e_n) \quad (1)$$

其中，$e_i(1\le i\le n)$表示某个环境变量，网络环境状态是由多个环境变量决定。典型的环境变量有CPU的占用情况，单位时间的网络连接数等。

状态空间是若干个网络环境状态的集合。状态空间S可表示为

$$S=\{C_1,C_2,\ldots,C_m\} \quad (2)$$

其中，$C_k(1\le k\le m)$表示某个网络环境状态。

策略空间是由各种策略组成的集合。策略空间D可表示为

$$D=\{d_1,d_2,\ldots,d_p\} \quad (3)$$

其中，$d_j(1\le j\le p)$表示某个具体的策略。

传统的IDS是让所有的网络环境状态C_k对应于一个策

基金项目：教育部科技基金资助重点项目(03115)；重庆市科委科技攻关基金资助项目(CSTC.2004AA2001-8277-9)
作者简介：何 波(1978－)，男，硕士、讲师，主研方向：信息安全，数据挖掘，信息推荐；程勇军、涂 飞，硕士、助教；杨 武，博士生、教授
收稿日期：2006-06-17 **E-mail：**hebo@cqit.edu.cn

略，不具备自适应性。自适应策略是在构建状态空间和策略空间的基础上，采用基于神经网络的函数拟合来建立从状态空间S到策略空间D的映射关系，即f:S→D。基于神经网络的函数拟合是通过神经网训练来拟合输入-输出的非线性映射函数，具有自学习性，能够较好地构建状态空间到策略空间地映射关系。通过评价和学习机制，实现自适应策略的动态更新。

1.3 状态空间的构建

由式(1)、式(2)可知，要确定状态空间，需要确定系统可能存在哪些网络环境状态，确定网络环境状态需要环境变量的参与。Agent 具有反应性和自适应性，利用 Agent 技术监控网络环境的状态及变化情况，同时对网络数据进行分析和特征提取，进而构建状态空间。

1.4 策略空间的构建

策略空间包括若干策略。论文采用关联规则算法和时序序列算法从大量的数据中挖掘出若干模式，进行模式比较就可以得到入侵模式，根据入侵模式的特征指导训练集的构造，再使用分类器进行分类，最后生成策略空间。策略空间的构建流程如图 1 所示。

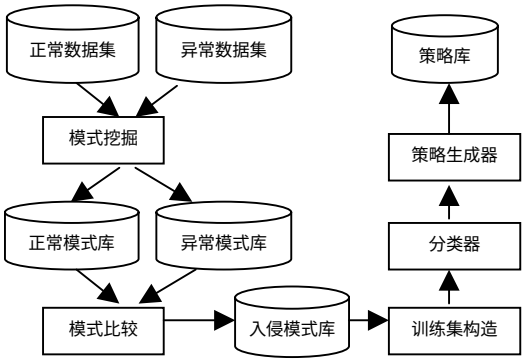

图 1 策略空间构建流程

(1)模式挖掘

通用挖掘算法没有考虑专业领域知识。解决的方法是在挖掘的过程中考虑入侵检测领域知识，根据这些知识来确定哪些属性对于挖掘模式是有效的。将需要挖掘的数据集分为正常模式集和异常模式集，没有入侵行为的数据集称为正常数据集，存在入侵行为的数据集称为异常数据集。对正常数据集挖掘获得正常模式，正常模式的集合构成正常模式库。对异常数据集进行挖掘获得异常模式，异常模式的集合构成异常模式库。

(2)模式比较

因为异常模式库中的异常模式并非都是入侵模式，而是包含入侵模式和正常模式；所以为了得到入侵模式，需要将正常模式与异常模式进行比较，与正常模式差别较大的异常模式被认为是入侵模式。利用函数HEOM(Heterogeneous Euclidean-Overlap Metric)[4]来量化模式之间的差别，这需要将比较的模式转换为向量的形式。HEOM函数是基于基本欧基里德函数的一种改良版本，它很好地计算向量之间距离。

(3)训练集的构造

训练集可用于指导分类。训练集的质量直接影响分类的效果，因此要求训练集中的模式应该是基本完全的，所有可能出现的模式都应该尽量包含在训练集中。

(4)分类器的构建

分类，属于有导师学习，即利用给定的训练集建立分类规则，再通过分类规则对新的数据进行分类。

采用分类算法SLIQ(Supervised Learning In Quest)[5]来进行分类器的构建。SLIQ是一个能够处理连续及离散属性的决策树算法，算法能够处理大规模的数据集，并能对具有大量的类、属性与样本的数据集分类，算法能以较小的代价生成紧凑而精确的树。

(5)策略库的生成

经过分类器分类，可以得到形如 if…then…的规则。对这些规则进行处理，并且利用领域知识和专家经验来增添规则，就可以生成策略库。策略库中包括多个策略，每个策略由多个 if…then…的入侵规则组成，由于获得的入侵监测规则往往是不精确的，因此对每个策略中的各个规则设置相应的规则置信度。为了规则推理的需要，对每个策略中的各个规则设置优先级别。

2 自适应入侵检测专家系统模型

2.1 基于规则和事例的混合推理机制

基于规则的推理和基于事例的推理各有优点。将二者有机的结合起来，可以利用二者的优势进行更为准确的推理。论文设计的基于规则和事例的混合推理机制如下：

(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×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和结果等内容；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。

2.2 模型结构

在建立了基于规则和事例的混合推理机制的基础上，利用自适应策略设计了一个既有专家知识库，又有入侵事例库，具有自学习、自适应的能力的入侵检测专家系统模型，模型的结构如图 2 所示。

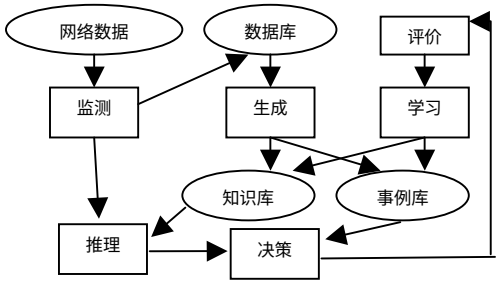

图 2 AIDESM 结构框图

AIDESM 可用一个九元组描述如下：

AIDESM=<DB, KB, CB, INSP, REAS, DECI, EVAL, LEAR, GENE>

其中：DB 为数据库；KB 为知识库；CB 为事例库；INSP 为

监测 agent；REAS 为推理机；DECI 为决策 agent；EVAL 为评价 agent；LEAR 为学习 agent；GENE 为生成 agent。

数据库 DB 存放的是经过监测 agent 处理的网络数据，包括构建自适应策略所需的各种数据集，是生成知识库和事例库的基础。

知识库 KB 包括自适应策略的状态空间、策略空间以及状态空间与策略空间的映射关系。其中策略空间中知识的获取来自 3 个方面：

(1)利用领域知识和专家经验来获取规则；

(2)根据论文第 1 部分的自适应策略，利用数据库获取规则；

(3)通过评价学习机制，实现规则的动态更新。

一个策略中的规则均设置了规则置信度和优先级别。知识库是推理机进行规则推理的依据。

事例库 CB 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。

INSP 作为监测 agent，其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；另一方面对这些处理后的数据进行特征提取和转换，提供给推理机进行处理。

推理机 REAS 是 AIDESM 进行基于规则推理的关键部件。其主要作用是利用监测 agent 处理过的网络数据与知识库中的状态空间进行匹配，确定当前的状态，利用状态空间与策略空间的映射关系，确定当前应当采用的策略。推理机根据 2.1 节设计的混合推理机制的第(2)步骤进行基于规则的不精确推理。访问行为经过推理机的推理判断，可能有 3 种情况：

(1)它是正常访问行为；

(2)它是异常访问行为；

(3)它是不确定访问行为。

对正常访问行为不报警；对异常的访问行为直接报警；对不确定访问行为交给决策 agent 进行进一步处理。

DECI 作为决策 agent，也是 AIDESM 进行基于事例推理的关键部件。决策 agent 主要是根据 2.1 节设计的混合推理机制的第(3)步骤对不确定访问行为进行处理，而正常访问行为和异常访问行为直接提交给评价 agent。

EVAL 为评价 agent，是实现具有自学习能力入侵检测的关键。其主要作用是对入侵检测的处理进行评价。

LEAR 为学习 agent，是实现具有自学习能力入侵检测的关键。其主要作用是根据评价的结果更新知识库中的知识和增添事例库中的事例。

GENE 是生成 agent，其主要作用是根据数据库中的各种数据集，利用第 1 部分内容构建知识库，同时构建事例库。

3 相关实验

AIDESM 是一个复杂的系统模型，主要针对提出的自适应策略进行了模拟实验，实验的目的是将采用固定策略的入侵检测和采用自适应策略的入侵检测进行对比。数据来源于 GIAC(全球信息安全认证，http://www.giac.org)，选取了 20 个正常数据集，20 个异常数据集，根据第 1 部分相关内容构建了一个简单的自适应策略 a，包括 3 种网络状态构成的状态空间，b1、b2 和 b3 3 个策略构成的策略空间和从状态空间到策略空间的一对一映射关系。

对模拟系统进行了 4 次测试，每次测试均是进行 20 次正常访问和 20 次攻击访问。第 1 次是采用策略 b1 进行测试，第 2 次采用策略 b2 进行测试，第 3 次采用策略 b3 进行测试，而第 4 次采用自适应策略 a 进行测试，模拟系统的入侵检测结果如图 3 所示。

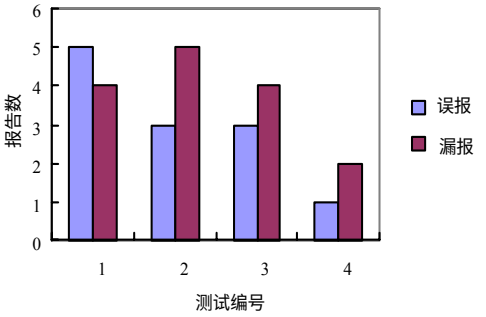

图 3 模拟系统的入侵检测结果

从测试结果看，第 1、2、3 次测试，漏报数或误报数较高；而第 4 次采用了自适应策略 a 进行测试，漏报数和误报数都较低。

实验结果初步表明，大多数入侵检测系统采用的单一的检测策略可能会造成严重的误报与漏报，而采用论文提出的自适应策略，让检测策略随着网络环境的改变而调整，这样可以降低误报率和漏报率。

4 结束语

本文提出了自适应策略，将基于规则的推理和基于事例的推理相结合，设计了自适应入侵检测专家系统模型。

初步实验结果表明，该自适应策略是比较有效的。下一步工作是对 AIDESM 的评价学习机制进行深入研究。

参考文献

1 戴英侠, 连一峰, 王　航. 系统安全与入侵检测[M]. 北京: 清华大学出版社, 2002.

2 Andrew H, Andrew H, Eleazar E. Adaptive Model Generation: An Architecture for Deployment of Data Mining-based Intrusion Detection Systems[R]. Department of Computer Science, Columbia University, New York, 2002.

3 Han J, Kamber M. Data Mining: Concepts and Techniques[M]. Beijing: High Education Press, 2001.

4 Wilson R, Martinez T. Improved Heterogeneous Distance Functions[J]. Journal of Artifcial Intelligence Reaearch, 1997, 6(1): 1-34.

5 Manish M, Rakesh A, Jorma R. SLIQ: A Fast Scalable Classifier for Data Mining[C]//Proceedings of the 5th International Conference on Extending Database Technology. 1996.