文章编号:1000 - 582X(2005)08 - 0060 - 04

# 基于 Agent 和数据挖掘的自适应入侵检测系统*

杨 武[1,2],何 波[1],程勇军[1],李 波[1]
(1. 重庆工学院 计算机系,重庆 400050; 2. 重庆大学 计算机学院,重庆 400050)

**摘 要**:入侵检测系统是网络安全保护体系中的一个重要组成部分,目前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. 针对这种情况,提出了一种入侵检测系统的自适应策略,该自适应策略由条件空间和策略空间构成,条件空间用来描述网络环境,策略空间用来描述采用的策略. 对于条件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,利用 Agent 和数据挖掘技术,设计了一个自适应入侵检测系统. 模拟实验表明了该自适应策略的有效性.

**关键词**:入侵检测系统;数据挖掘;智能体
**中图分类号**:TP393 **文献标识码**:A

随着因特网的迅速发展,信息保密性和网络安全性变得越来越重要. 入侵检测系统(Intrusion Detection System, IDS)[1]作为防火墙之后的第二道安全闸门,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.

Agent 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. 数据挖掘[2]技术是一种知识发现技术,其目的是从海量数据中抽取潜在的、有价值的知识.

论文提出了自适应策略,在此基础上,设计了一个基于 Agent 和数据挖掘的自适应入侵检测系统(简称为 AAIDS). 该系统能自动适应复杂多变的网络环境,能通过自我学习提高入侵检测能力. 模拟实验结果表明,该自适应策略是比较有效的.

## 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. 论文引入条件空间和策略空间来描述自适应策略. 条件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. 对于条件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 $C$ 可表示为公式(1).

$$C = f(e_1, e_2, \cdots, e_n), \tag{1}$$

其中 $e_i(1 \leqslant i \leqslant n)$ 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.

条件空间是若干个网络环境状态的集合. 条件空间 $S$ 可表示为公式(2).

$$S = \{C_1, C_2, \cdots, C_m\}, \tag{2}$$

* 收稿日期:2005 - 04 - 15
基金项目:教育部科技重点项目(03115);重庆市科技公关项目(CSTC2004AC2018)
作者简介:杨武(1965 - ),湖北武汉人,男,重庆工学院副教授,重庆大学博士研究生,主要研究方向:发布式处理、信息安全.

其中 $C_k(1\leqslant k\leqslant m)$ 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 $D$ 可表示为公式(3)

$$D = \{d_1, d_2, \cdots, d_p\}, \tag{3}$$

其中 $d_j(1\leqslant j\leqslant p)$ 表示某个具体的策略.

传统的 IDS 是让所有的网络环境状态 $C_k$ 对应于一个策略,不具备自适应性. 自适应策略是在构建条件空间和策略空间的基础上,建立从条件空间 $S$ 到策略空间 $D$ 的映射关系,即 $f: S\rightarrow D$.

### 1.3　条件空间的构建

由公式 1、2 可知,要确定条件空间,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 技术可以监控网络环境的状态及变化情况,从而构建条件空间.

### 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学习集的构造,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.

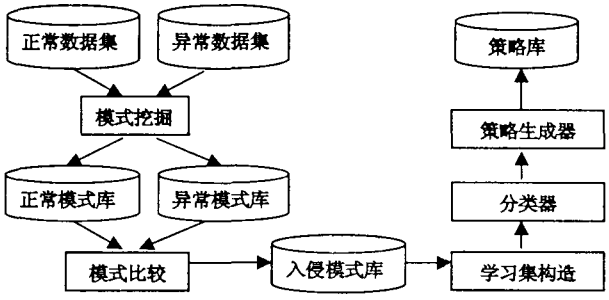


图 1　策略空间构建流程图

#### 1.4.1　模式挖掘

关联规则和时序序列已有一些通用算法,比如 Apriori 等,但是直接利用它们挖掘很可能出现过多无关的属性而生成无用的规则,原因是这些通用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. 论文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.

#### 1.4.2　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. 论文利用函数 HEOM ( Heterogeneous Euclidean - Overlap Metric)[3] 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,它可以很好地计算向量之间距离. HEOM 函数表示如下:

$$d_a(x,y) = \begin{cases} 1 & x \text{ or } y \text{ is unknown} \\ \text{overlap}(x,y) & \text{otherwise} \end{cases}, \tag{4}$$

$$\text{overlap}(x,y) = \begin{cases} 0 & x = y \\ 1 & \text{otherwise} \end{cases}, \tag{5}$$

$$\text{HEOM}(x,y) = \sqrt{\sum_{a=1}^{m} d_a(x_a,y_a)^2}. \tag{6}$$

其中,$x$ 与 $y$ 均为向量,$x_a$ 和 $y_a$ 为对应向量中的属性,$m$ 为向量中属性的个数. HEOM$(x, y)$ 值越小,向量 $x$ 与 $y$ 越相似.

但是模式中的属性的重要性并不相同,因此论文对 HEOM 函数进行了修改:用权值 $\theta$ 来衡量每个属性的重要性,$\theta$ 越大属性越重要. 在保留公式(4),(5)的基础上,修改公式(6),则向量 $x$ 与 $y$ 之间的差别可用公式(7)表示

$$\text{dis}(x,y) = \sqrt{\sum_{a=1}^{m} \theta_a d_a(x_a,y_a)^2}, \tag{7}$$

其中 $\theta_a$ 为属性对应的权重,且 $\sum_{a=1}^{m} \theta_a = 1$. dis$(x, y)$ 值越小,向量 $x$ 与 $y$ 越相似.

假设 $x$ 为某个正常模式对应的向量,$y$ 为某个异常模式对应的向量,设置阈值 $\varepsilon$,利用公式(4),(5),(7)计算出的 dis$(x,y)$ 值,如果该值大于 $\varepsilon$ 说明 $y$ 对应的异常模式为入侵模式.

#### 1.4.3　学习集的构造

学习集也称训练集,从学习集得到的规则将用于指导分类. 学习集的质量直接影响分类的效果,因此要求学习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学习集中.

#### 1.4.4　分类器的构建

分类,属于有导师学习,即利用给定的学习集建立分类规则,再通过分类规则对新的数据进行分类. 论文采用分类算法 SLIQ( Supervised Learning In Quest)[4] 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.

1.4.5 策略库的生成

经过分类器分类,可以得到形如 if 条件 1 and 条件 2 and … and 条件 $n$ then intrusion 的规则. 对这些规则进行处理以后,就可以生成策略库. 由于误用检测和异常检测需要的规则集不同,前者是根据已知的入侵模式进行检测,后者是根据入侵行为与正常模式之间的差异进行检测,所以策略库由误用策略和异常策略组成.

## 2 基于 Agent 和数据挖掘的自适应入侵检测系统(AAIDS)

AAIDS 采用 Agent 和数据挖掘技术构建入侵检测系统,具有较好的自适应性[5]. AAIDS 的整体结构如图 2 所示,包括控制中心、监控 Agent、分析 Agent 和决策 Agent 4 个部分.

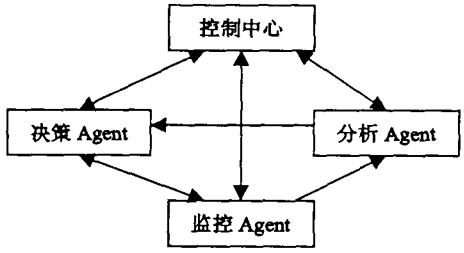


图 2 AAIDS 系统结构

### 2.1 控制中心

控制中心是 AAIDS 中最高层控制单元,其主要功能是对系统中各 Agent 进行监控和管理,是用户与系统交互的接口. 用户通过控制中心可以监测各 Agent 的活动情况以及对各 Agent 进行控制. 例如,根据监控 Agent 和分析 Agent 上传的一些信息,适当地启动或停止一些 Agent,以便更好地对入侵行为进行控制.

### 2.2 监控 Agent

监控 Agent 是 AAIDS 的重要部分,其主要功能是检测当前的网络状况和对入侵行为进行控制处理. 监控 Agent 的内部结构如图 3 所示.

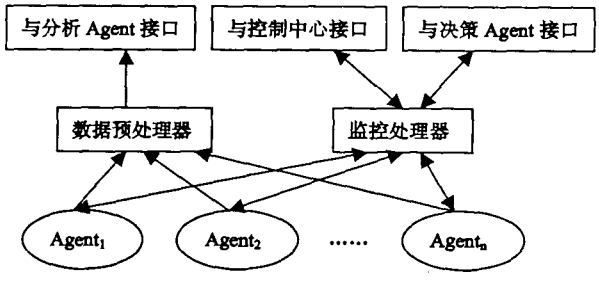


图 3 监控 Agent 结构

监控 Agent 中包含多个独立 Agent. 各独立 Agent 的任务是收集网络数据或主机日志;并且根据监控处理器的指令对入侵行为进行处理.

数据预处理器的任务对各独立 Agent 收集到的原始数据进行预处理,提取相应的特征信息;并且将这些特征信息通过接口提供给分析 Agent 的数据仓库.

监控处理器的任务是将各独立 Agent 收集的网络实时信息通过接口分别提供给控制中心和决策 Agent;并且根据控制中心和决策 Agent 的相关指令对各独立 Agent 进行控制.

### 2.3 分析 Agent

分析 Agent 是 AAIDS 系统的核心部分,也是实现系统自适应性的关键部分,其主要功能是生成并定期更新自适应策略和根据当前的网络环境状态确定采取的策略. 分析 Agent 的内部结构如图 4 所示.

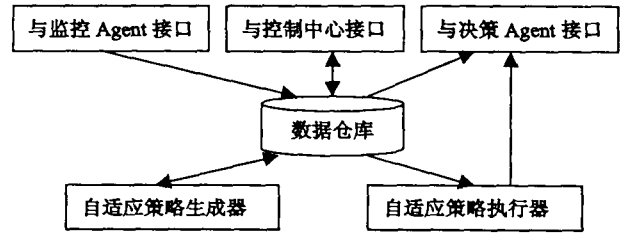


图 4 分析 Agent 结构

数据仓库中存储的数据包括各接口获取的数据和生成的自适应策略.

自适应策略生成器的任务是根据论文第二部分中的相关内容生成条件空间和策略空间,建立从条件空间到策略空间的映射关系,即生成自适应策略;并且每隔一段时间动态更新自适应策略.

自适应策略执行器的任务是根据当前的网络环境状态确定采取的策略;并且将该策略通过接口提供给决策 Agent 的实时策略库.

### 2.4 决策 Agent

决策 Agent 是 AAIDS 系统的决策部分,其主要功能是根据网络的实时情况和相应策略进行决策[6]. 决策 Agent 的内部结构如图 5 所示.

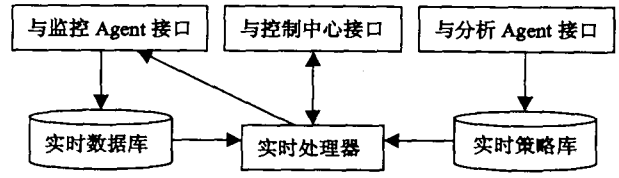


图 5 决策 Agent 结构

实时数据库存储的是监控 Agent 提供的网络实时情况数据.

实时策略库存储的是分析 Agent 提供的当前策略. 由于误用检测和异常检测采用的策略不同,实时策略库的策略包括误用策略和异常策略.

实时处理器的任务是根据实时数据库提供的网络实时情况和策略库提供的当前策略进行实时处理. 如果发现入侵行为,则通过接口向监控 Agent 发出控制指令,同时向控制中心发出警报信息.

## 3 模拟实验

主要针对自适应策略进行了模拟实验. 实验的目的是对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,根据论文第二部分相关内容构建了一个简单的自适应策略 a,包括 3 种网络状态构成的条件空间,由策略 b1、b2、b3 构成的策略空间和从条件空间到策略空间的一对一映射关系.

进行了 4 次模拟测试,每次模拟测试均是进行 10 次正常访问和 10 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 6 所示.

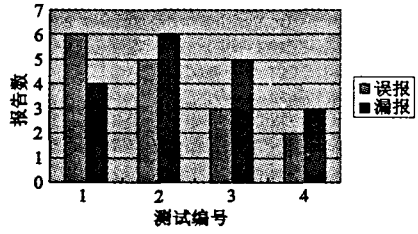


图 6　模拟实验的入侵检测结果

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. 模拟实验结果初步表明,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

论文提出了入侵检测自适应策略,该自适应策略以条件空间和策略空间为基础,建立从条件空间到策略空间的映射关系. 在构建自适应策略的基础上,利用 Agent 和数据挖掘技术,设计了一个自适应入侵检测系统. 初步模拟实验结果表明,该自适应策略是比较有效的. 但是策略空间的构建以及条件空间与策略空间之间的映射关系需要进一步深入研究.

**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] HAN J, KAMBER M. Data Mining: Concepts and Techniques [M]. Beijing: High Education Press, 2001.

[3] WILSON R, MARTINEZ T. Improved Heterogeneous Distance Functions[J]. Journal of Artificial Intelligence Research, 1997, 6:1 - 34.

[4] MANISH MEHTA, RAKESH AGRAWAL, JORMA RISSANEN. SLIQ: A Fast Scalable Classifier for Data Mining[Z]. Proceedings of the 5th International Conference on Extending Database Technology. Avigonon, 1996,18 - 32.

[5] 孙玉星,文巨峰,赵燕飞,等. 新型的基于已用 Agent 自适应入侵检测系统研究[J]. 计算机应用与软件, 2004, 21(11):105 - 107.

[6] ANDREW HONIG, ANDREW HOWARD, ELEAZAR ESKIN. Adaptive Model Generation: an Architecture for Deployment of Data Mining-based Intrusion Detection Systems[A]. Data Mining for Security Applications [C]. [s. l.]: Kluwer Press, 2002.

# Adaptive Intrusion Detection System Based on Agent and Data Mining

*YANG Wu*[1,2], *HE Bo*[1], *CHENG Yong-jun*[1], *LI Bo*[1]

(1. Department of Computer Science, Chongqing Institute of Technology, Chongqing 400050, China;
2. College of Computer Science, Chongqing University, Chongqing 400030, China)

**Abstract**: Intrusion detection system is an essential component of network security protection mechanisms. Most intrusion detection system can not adapt the variation of network environment. Aiming at this problem, an adaptive strategy that composed of condition space and strategy space is proposed. The condition space describes the network environment and the strategy space describes the strategy. There is an exclusive strategy corresponds to a certain environment state in condition space. On the base of the adaptive strategy, an adaptive intrusion detection system based on agent and data mining is designed. The simulation experiments indicate that the adaptive strategy is effective.

**Key words**: IDS; data mining; agent

(编辑　张小强)