基于机器学习方法的入侵检测技术的研究

邓安远
(九江学院信息科学与技术学院　江西九江 332005)

摘　要　入侵检测技术是近20年来才出现的一种有效保护网络系统免受网络攻击的新型网络安全技术。随着网络技术的迅速发展、安全问题的日益突出,传统的入侵检测系统已难以满足对越来越复杂的网络攻击的检测任务,将机器学习的技术引入到入侵监测系统之中以有效地提高系统性能,已成为入侵检测技术的研究热点。本文主要介绍了入侵检测系统的基本结构以及几种机器学习方法在入侵检测中的应用,其中包括:基于贝叶斯分类的方法、基于神经网络的方法、基于数据挖掘的方法与基于支持向量机的方法。

关键词　机器学习,入侵检测,网络安全

On Intrusion Detection Technology Based on Machine Learnign Method

DENG An-Yuan
(Faculty of Information Science and Technology, Jiujiang University, Jiujiang 332005)

Abstract　Intrusion Detection (ID) is a new emerging network security technology in the recent 20 years, which can protect the network system from the network attacks effectively. With the rapid development of the network technology and the fast increasing of intrusion problems, the traditional intrusion detection methods cannot work well with the more and more complicated intrusions. So introducing machine learning into intrusion detection systems to improve the performance has become one of the major concerns in the research of intrusion detection. This paper introduces the basic structure of the intrusion detection system and the application of machine learning in intrusion detection, including the Bayes-based method, the neural network-based method, the data mining-based method and the SVM-based method.

Keywords　Machine learning, Intrusion detection, Network security

1　引言

伴随着网络技术的迅速发展,人们的工作和生活已经和网络紧密联系在一起,但与此同时,网络也成为了攻击者进行攻击的主要平台和目标,安全一直是网络世界的一个永恒的话题。早在1988年,Internet的前身NSFNet上就发生了第一次网络蠕虫的攻击。近年来,信息保密性和网络安全性得到了越来越多的重视。然而,各种攻击事件发生的次数逐年增加,并且造成的损失也愈加严重。传统的防火墙隔离技术等静态安全防御技术对日新月异的网络环境下的攻击手段缺乏主动的反应,其主要的局限性表现在:第一,入侵者可以寻找防火墙背后可能敞开的后门;第二,不能阻止内部攻击;第三,不能主动跟踪入侵者;第四,对网络环境和攻击手段的变化缺乏自适应能力。因此,随着攻击者知识的日趋成熟,攻击手段和工具的日趋复杂多样,单纯的防火墙隔离策略已经无法满足对安全高度敏感的部门的需要,网络安全必须采取一种纵深的、多样的、自适应的方法,入侵检测系统IDS(Intrusion Detection System)应运而生。

入侵检测技术是近20年来出现的一种新型网络安全技术,它作为防火墙后的第二道安全闸门,能够检测出多种形式的入侵行为,是现代计算机网络安全体系的一个重要组成部分。入侵检测这一概念最早是由Anderson在1980年提出的,文中首次提出了利用审计数据发现入侵行为的思想[1]。其后,在1987年,SRI(Stanford Research Institute)的Denning提出了一种通用的入侵检测模型,成为入侵检测发展的基础[2]。1990年,Heberlein首次提出了网络入侵检测的概念并开发了第一个网络入侵检测系统NSM(Network Security Monitor)[3]。由此,入侵检测系统的两种基本结构——基于主机和基于网络的入侵检测系统被确定下来,并在其基础上,已出现了各种各样的基于机器学习技术入侵检测技术。本文主要描述了机器学习基于贝叶斯分类方法、基于神经网络和基于关联规则挖掘等入侵检测技术。

2　网络入侵检测系统

2.1　入侵检测模型

随着入侵检测技术的发展,各种入侵检测系统相继出现,DARPA(Defense Advanced Research Projects Agency)于1997年3月发起了入侵检测系统的标准化工作,建立了公用入侵检测框架模型CIDF(Common Intrusion Detection Framework),其目的是开发出一套规范,它定义了入侵检测系统表达检测信息的标准语言以及系统组件之间的通信协议,使得符合CIDF规范的入侵检测系统之间能够共享检测信息,相互通信,协同工作,还可以与其它系统配合实施统一的配置响应和恢复策略。

CIDF将入侵检测系统需要分析的数据统称为事件(event),它可以是基于网络的入侵检测系统从网络中提取的数据包,也可以是基于主机的入侵检测系统从系统日志等其它途径得到的数据信息。

邓安远　硕士,副教授,研究方向:数据库与信息系统,现代计算机网络技术,嵌入式系统应用开发。

CIDF组件之间的交互数据使用通用入侵检测对象GIDOs(Generalized Intrusion Detection Objects)的格式，一个GIDO可以表示在一些特定时刻发生的一些特定事件，也可以表示从一系列事件中得出的一些结论，还可以表示执行某个行动的指令。

同时，它也定义了一个通用的系统模型，如图1所示。

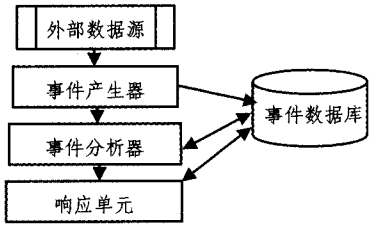

图1 CIDF模型

CIDF模型的基本组件包括[4]：

1)事件产生器(Event generator)：从入侵检测系统所在的整个计算机系统中获取原始数据，如：审计数据、网络数据包、系统日志等，并以gido格式的事件提供给其他组件。

2)事件分析器(Event analyzer)：对从其他组件处收到的事件结合历史信息进行分析，并把分析的结果提交给响应单元。

3)事件数据库(Event database)：存放事件的地方，可以是复杂的数据库，也可以是简单的文本文件。

4)响应单元(Response unit)：对事件分析器的分析结果做出反应，报警或终止入侵。

CIDF对各种入侵检测系统的结构进行了抽象，对各组件的通讯和API进行了标准化，虽然数据源或有不同，各种入侵检测系统基本采用了相似的处理结构。

2.2 入侵检测系统

根据数据来源的不同，入侵检测系统可以分为基于主机的入侵检测系统(Host-Based Intrusion Detection System，HIDS)和基于网络的入侵检测系统(Network-Based Intrusion Detection System，NDIS)[5]，分别以主机和网络作为数据源。从基于主机的入侵检测系统中又可以细分出一类——基于应用的入侵检测系统，其数据源是系统上运行的应用。这一分类是基于它们各自的数据采集单元，即事件产生器。基于不同数据源的各种入侵检测系统有各自的优缺点，适用于不同的场合。

根据数据来源的不同，各种入侵检测系统有其固有的优缺点。其中，基于网络的入侵检测系统由于其安装部署容易且对现有网络影响小的优点，在应用中较为广泛。但是基于网络的入侵检测系统需要对网络中所有的通讯量进行监听和分析，为达到一定的性能目标，必须有较高的处理能力，这是亟需解决的问题。基于主机的入侵检测系统只对目标设备的数据日志进行分析，因此对性能的要求不高，同时能检测出基于网络的入侵检测系统漏过的攻击，并判断攻击是否成功。但其运行在被保护的主机上，本身易受攻击，并影响主机的性能。基于应用的入侵检测系统针对性更强，可仍然继承了基于主机的入侵检测系统的优缺点。

因此，比较有效的入侵检测系统大多采用多种数据源，把三种入侵检测系统有层次地结合在一起，通过对多种数据源的综合分析来得到更好的检测结果，达到互补的效果。当这三种数据来源结合在一起的时候，通常采用应用-主机-网络的层次结构，同时一个入侵检测系统的分析结果可以被同一或更高层的其他入侵检测系统利用。

3 基于机器学习的入侵检测方法

入侵检测系统中的事件分析器负责对事件进行分析，做出该事件是否为攻击行为的判断。由此可见，对事件分析技术的研究是入侵检测技术研究的主要内容。

入侵检测方法大致可以分为两类，误用检测(Misuse Detection)和异常检测(Anomaly Detection)[6]。

误用检测又被称为基于特征(Signature-based)或者基于知识(Knowledge-based)的入侵检测[7]。它的基本前提是已知的攻击行为可以用一种模式识别和表示，误用检测系统的目标就是利用已有的特征知识库中的知识，对获得数据使用各种模式识别算法进行匹配，检测主体的活动是否符合已知的入侵模式。误用检测的优点是误报率低，由于模式识别的理论和研究已经相当成熟，运行效率较高，因此大多数商用入侵检测系统采用这种技术。但是，由于只能检测已知模式的攻击行为，对现有攻击的简单变形都可能被忽略，误用检测的漏报率较高；而且，建立并维护和更新一个完备和精确的入侵特征库是相当困难的。

异常检测又被称为基于行为的入侵检测。它假设入侵行为是异常行为的子集，与系统的正常行为不同。因此，异常检测系统通过建立系统用户正常的行为轮廓(Profile)，比较当前系统和用户的行为是否偏离了正常的范畴，从而判断是否发生了入侵。异常检测与系统相对无关，通用性强，而且可以检测出未知模式的攻击行为，这是它最大的优势，也是研究的热点所在。但是异常检测的误报和漏报率都较高，因为系统本身的"正常"行为的轮廓、阈值等难以界定；入侵者在已知异常检测系统存在的前提下，可以通过对正常行为模式缓慢偏离的方式使系统逐渐适应，从而发生漏报。

入侵检测的事件分析方法繁多，许多方法既可以用于误用检测，又可以用于异常检测。例如，基于神经网络的方法可以使用正常数据进行训练，又可以使用异常数据，前者是对正常行为进行建模，属于异常检测，而后者则是误用检测。

3.1 基于贝叶斯分类的方法

贝叶斯定理是贝叶斯理论中最重要的一个公式，它将事件的先验概率和后验概率巧妙地联系了起来，利用先验信息和样本数据确定事件的后验概率：

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$$

入侵检测的基本任务就是判断观察到的事件是入侵还是正常行为，所以可以看作是一个分类的过程。因此，国内外不少研究者选择贝叶斯分类器对事件进行分类，来实现入侵检测的功能。

朴素贝叶斯分类器是各种贝叶斯分类器中最简单直观的一种。它与其他贝叶斯分类器最大的不同就是朴素贝叶斯分类器对事件所有属性的独立性假设。这一假设大大简化了系统的复杂性，并在一定的场合取得了比较好的结果。斯坦福研究院的Valdes和Skinner等用朴素贝叶斯分类器对网络流量进行分析，并设计了称为eBayes的入侵检测系统[8]。Barbara等在其论文中也提出了使用朴素贝叶斯分类器对事件进行分类的入侵检测系统ADAM[9]。然而，朴素贝叶斯的独立性假设在实际情况中不可能完全满足，事件的属性之间必然存在一定的依赖关系。贝叶斯网络根据属性之间的概率关

系建立图论模型，来刻画出属性之间的相互依赖。Kruegel 等人在其系统中使用贝叶斯网络刻画各个检测模型的置信度和相互之间的依赖关系，从而降低了系统的误报率[10]。

3.2 基于神经网络的方法

神经网络是一种非参量化的分析技术，它由大量模拟大脑神经元的简单计算单元构成，单元之间通过带有权值的连接来进行交互。神经网络本质上是输入到输出的映射，其输出值是由输入数据、神经元之间的连接权值和传递函数决定的。神经网络具有较强的学习和自适应能力，K. Fox 等人使用神经网络来进行入侵检测，对异常检测和误用检测分别采用了多层感知机（Multi-Layer Perception）和多层 BP（Back Propagation）的神经网络模型[11]。Ghosh 和 Schwartzbard 基于 1998 年 DARPA 数据研究了神经网络在两类入侵检测中的应用，他们的实验结果表明基于神经网络的入侵检测方法在误用检测中的效果较好，在低误警率下可以识别出绝大多数已知的攻击方式，但对未知攻击模式的识别不佳[12]。

3.3 基于数据挖掘的方法

1999 年，Wenke Lee 在文[13]中给出了用数据挖掘技术建立入侵检测模型的过程。数据挖掘是从海量数据中抽取、“挖掘”出未知的、有价值的模式和知识的复杂过程[14]。而入侵检测正是从大量的网络数据中提取和发现异常的入侵行为，因此，数据挖掘中的多种技术都可以应用于入侵检测系统，例如：分类、聚类、关联分析、序列分析等。

分类技术把观察到的事件映射到预先定义好的类别中去。常见的分类算法包括：判定树、贝叶斯分类器、神经网络等。使用分类技术进行入侵检测的基本思想是首先使用带类标的训练数据集对分类器进行训练，使其能够对正常和异常至少两类事件进行区分，然后使用训练好的分类器对需要检测的事件进行分类，从中发现异常行为。

聚类是将物理或抽象对象的集合分组成为由类似的对象组成的多个簇（cluster）的过程。同分类不同的是，聚类对要划分的类是未知的。分类器的训练通常需要大量的有类标示的训练数据，但在实际情况下，提供这样的数据集是相当困难的。基于聚类的无监督异常检测方法的基本思想就是假设入侵行为和正常行为的差异很大并且数量较少，因此它们能够在检测到的数据中呈现出比较特殊的属性。Portnoy 和 Eskin 等人提出了一种使用无类标示数据的基于聚类的无监督异常入侵检测方法，其方法是使用一个简单的基于距离的度量方法来形成簇[15]。该方法的优点在于对不需要对训练集进行分类，但漏报率较高，主要原因是该方法的性能主要依赖于训练集的好坏。

关联规则挖掘的目的就是为了发现大量数据中项集（itemset）之间的关联或相关联系。用于入侵检测系统中，关联规则挖掘可以分析标示用户的行为特征，发现正常行为数据之间的关联，并将其作为用户正常行为的轮廓，可以对异常行为进行检测。Lee 等人将 Agrawal 等人于 1994 年提出的关联规则的算法 Apriori[16] 使用在入侵检测中[17]。该方法的优点在于不需要专业知识，算法的实现较简单，但对训练集的要求也较高。

序列模式挖掘是指挖掘相对时间或其他模式出现频率较高的模式。序列模式挖掘有几个重要的参数，如时间序列的持续时间，事件重叠窗口和被发现模式之间的时间间隔等。Lee 等人提出的入侵检测系统在关联规则挖掘 Apriori 算法的基础上增加了事件发生的时间间隔的约束条件，把序列分析[17]的方法运用到入侵检测中。

3.4 基于支持向量机的方法

支持向量机（SVM）是由 Vapnik 等人于 1995 年提出的一种比较新颖的机器学习算法[18]。SVM 是通过寻找一个使训练集的分类间隔（margin）达到最大的最优分类超平面来进行分类。SVM 不需要降维来防止发生过配现象，而且它的分类复杂度与属性空间的维数无关，因此 SVM 非常适用于解决入侵检测问题。Mukkamala 等采用 SVM 在 DARPA 设计的 KDD 竞赛数据库上的实验取得了出色的效果[19]。Sung 和 Mukkamala 采用 SVM 来筛选出入侵检测中重要的输入属性[20]。随后，也有学者把 SVM 和其他算法相结合提出效果更好的入侵检测算法。例如：Wu 等人把向量量化技术和 SVM 结合，先采用向量量化技术把网络审计数据库减小，生成一个训练编码本，然后采用 SVM 在这个训练编码本上建立入侵检测模型[21]；Kim 等把遗传算法和 SVM 融合一起来寻找一个“最优的检测模型”，该方法不仅能找到 SVM 的“最佳参数”而且还能找到整个属性集中“最优的属性子集”[22]。实验分析表明，在入侵检测应用中，与其他常用的算法相比，SVM 可以在较短的训练时间内达到一个很好的性能。

讨论和结束语 入侵检测系（IDS）从实验室原型研究到推出商业化产品、走向市场并获得广泛认同，已经走过了二十多年的风雨坎坷路。从 20 世纪 90 年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足的进展。1980 年 4 月，James P. Anderson 为美国空军做了一份题为《Computer Security Threat Monitoring and Surveillance》（计算机安全威胁监控与监视）的技术报告，第一次详细阐述了入侵检测的概念。这份报告被公认为是入侵检测的开山之作。从 1984 年到 1986 年，乔治敦大学的 DorothyDenning 和 SRI/CSL（SRI 公司计算机科学实验室）的 Peter Neumann 研究出了一个实时入侵检测系统模型，取名为 IDES（入侵检测专家系统）。1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，并开发出了一个 IDES。1990 年是入侵检测系统发展史上的一个分水岭。这一年，加州大学戴维斯分校的 L. T. Heberlein 等人开发出了 NSM（Network Security Monitor）。入侵检测系统的两大阵营正式形成：基于网络的 IDS 和基于主机的 IDS。1988 年的莫里斯蠕虫事件发生之后，网络安全才真正引起了军方、学术界和企业的高度重视。开展对分布式入侵检测系统（DIDS）的研究，DIDS 是分布式入侵检测系统历史上的一个里程碑式的产品。这些产品各有各的特色，也有各自的局限性。特别是作为商业产品，这些系统较为保守，使用的入侵检测分析技术和系统结构虽然成熟，但检测结果不能令人满意，对网络环境的依赖性较大，能检测的攻击手段有限，对未知攻击的分析和检测能力较差。

在学术界，有许多入侵检测的项目正在进行，其中以加州大学戴维斯分校的 GrIDS[23]，普度大学的 IDIOT[24] 以及 SRI 公司承担的 EMERALD[25] 等项目影响较大。

虽然近年来，入侵检测的研究取得了重大的发展，但是面对日益严峻的网络安全环境和复杂多变的攻击手段，现有的入侵检测系统仍然存在一些问题，等待解决：

• 传统的基于主机或网络的入侵检测系统局限于单一的结构，对异构以及大型的网络检测能力明显不足，对网络系统的改变缺乏适应性。一些所谓的“分布式”检测系统也仅仅是在数据采集上实现了分布式。因此，为解决这一问题，必须发

展分布式入侵检测技术，从检测系统结构设计上适应大型、高速且异构的平台环境。这里的分布式入侵检测技术包含两层含义：第一层含义即针对分布式网络攻击的检测方法；第二层含义即使用分布式的方式来检测分布式的攻击，其中的关键技术为检测信息的全局处理和入侵攻击全局信息的提取。

·误报率和漏报率仍不能达到实用的要求。入侵检测系统组件中的时间分析器的分析检测能力是入侵检测系统能力的关键。无论商业化的产品，还是处于研究阶段的原型，尽管引入了包括人工智能、数据挖掘在内的一系列成熟技术，入侵检测方法的智能化仍然有进一步提高的要求，以应付越来越复杂的攻击方法，提高检测能力。特别是在异常检测方面，如何对未知攻击的进行分析和检测成为入侵检测方法的研究热点。

本文叙述的基于机器学习方法的网络入侵检测技术是解决上述问题的一种很有效的途径，可以使入侵系统具有学习机制和智能化，可以大大提高入侵系统的效率和识别率。

参 考 文 献

1 Anderson. Computer Security Threat Monitoring and Surveillance:[Technical report]. 1980
2 Denning D E. An Intrusion-Detection Model. IEEE Transaction on Software Engineer, 1987
3 Heberlein L T, Dias G, Levitt K, Mukherjee B, Wood J, Wolber D. A Netork Security Monitor. In:Proceedings of 1990 Symposium on Research in Security and Privacy, 1990
4 Common Intrusion Detection Framework Working Group. Common Intrusion Detection Framework Specification. http://www.gidos.org, 2000
5 Bace R, Mell P. NIST Special Publication on Intrusion Detection Systems. 2001
6 Boyer R S, Moore J S. A Fast String Searching Algorithm. Communications of the ACM, 1977
7 Roesch M. Snort: Lightweight Intrusion Detection for Networks. In:Proceedings of the USENIX LISA Systems Administration Conference, 1999
8 Valdes A, Skinner K. Adaptive, Model-based Monitoring for Cyber Attack Detection. In:Proceedings of RAID 2000, 2000
9 Barbara D, Wu N, Jajodia S. Detecting Novel Network Intrusions Using Bayes Estimators. In:Proceedings of the First SIAM International Conference on Data Mining, 2001
10 Kruegel C, Mutz D, Roberston W, Valeur F. Bayesian Event Classification for Intrusion Detection. In:Proceedings of the 19th Annual Computer Security Applications Conference, 2003
11 Fox K, Henning R, Reed J. A Neural Network Approach Towards Intrusion Detection. In: Proceedings of the 13th National Computer Security Conference, 1990
12 Ghosh A K, Schwartzbard A. A Study in Using Neural Network for Anomaly and Misuse Detection. In: Proceedings of the 8th USENIX Security Symposium, 1999
13 Wenke Lee, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Models. In: Proceedings of the 1999 IEEE Symposium on Security and Privacy, 1999
14 Han Jiawei, Kamber M. Data Mining: Concepts and Techniques. Morgan Kaufmann, 2001
15 Portnoy L, Eskin E, Stolfo S J. Intrusion Detection with Unlabeled Data Using Clustering. In:Proceedings of ACM CSS Workshop on Data Mining Applied to Security, 2001
16 Agrawal R, Srikant R. Fast algorithms for mining association rules. In:Proceedings of the 20th VLDB Conference, 1994
17 Lee Wenke, Stolfo S J. Data Mining Approaches for Intrusion Detection. In:Proceedings of the 7th USENIX Security Symposium, 1998
18 Vapnik V N. Statistical learning theory. Adaptive and learning systems for signal processing, communications and control, New York: Wiley, 1998
19 Mukkamala S, Janoski G, Sung A H. Intrusion Detection Using Neural Networks and Support Vector Machines [C]. In: Proceedings of IEEE International Joint Conference on Neural Networks, IEEE Computer Society Press, 2002. 1702～1707
20 Sung A H, Mukkamala S. Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks [C]. In:2003 Sympsium on Applications and the Interuet, Orlando, Florida, 2003, 1:209～216
21 Yang W, Yun X, Li J. An improved Network Intrusion Detection Method based on VQ-SVM. In: Proceedings of International Conference on Parallel and Distributed Computing Systems, 2005. 583～587
22 Kim D, Nguyen H, Park J. Genetic Algorithm to Improve SVM Based Network Intrusion Detection System. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, 2005. 155～158
23 Chen S S, Cheung S, Crawford R. GrIDS-A Graph Based Intrusion Detection System for Large Networks. In: The 19th National Information Systems Security Conference (NISSC), 1996
24 Kumar S, Spafford E H. A pattern matching model for misuse intrusion detection. In: Proceedings of the 17th National Computer Security Conference, 1994
25 Porras P A, Neumann P G. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: Proceedings of the 20th National Information Systems Security Conference, 1997

(上接第 63 页)

(8)第二类分组丢失概率

1)只有工作队列时的丢失概率：

因门限丢失概率：$\pi_{class2\ lost}=\sum_{\substack{j=TH\\0\leqslant i\leqslant K-TH-1}}\pi_{ij}$

因容量丢失概率：$\pi_{class2\ lost}=\sum_{\substack{0\leqslant j\leqslant TH\\i+j=K}}\pi_{ij}$

2)工作队列和备用队列同时存在时的丢失概率：

因门限丢失概率：$\pi_{class2\ lost}=\sum_{\substack{i+j=K+TH+1\\K-TH+1\leqslant i\leqslant K}}\pi_{ij}+\sum_{\substack{j=TH\\K+1\leqslant i\leqslant K+TH-1}}\pi_{ij}$

因容量丢失概率：$\pi_{class2\ lost}=\sum_{\substack{i+j=2K\\K+TH\leqslant i\leqslant 2K}}\pi_{ij}$

结论 本文对共享缓存分组交换机提出了 DDQQT 缓存管理策略。动态的双队列能有效提高公平性以及缓存器的利用率。通过对低优先级分组设置门限，给高优先级分组以提供更大的缓存空间，从而区分了不同优先级分组的丢失率。双队列的设计保证了各类分组最低的丢失率，达到了提高 QoS 的要求。通过建立强占型优先权的 $M_1+M_2/M/K+(K)$ 排队模型，利用矩阵几何解方法对该模型求解，给出了系统的稳态概率以及相关的重要指标，这也给缓存的优化设计提供了理论依据。

参 考 文 献

1 Braden B, et al. Recommendations on queue management and congestion avoidance in the Internet [J]. IETF RFC 2309, 1998, 4
2 Floyd S, Jacobson V. Random early detection gateways for congestion avoidance [J]. IEEE/ACM Transaction on Networking, 1993, 81(4): 397～413
3 Hayes D, Rumsewicz M, Andrew L. Quality of service driven packet scheduling disciplines for real-time applications: Looking beyond fairness [J]. IEEE Infocom, 1999. 405～412
4 Boxma O, Dwon D. Dynamic server assignment in a two-queue model [J]. European Journal of Operational Research, 1997, 103: 595～609
5 Feng W, Kowada M, Adachi K. A two-queue model with Bernoulli service schedule and switching times [J]. Queueing Systems, 1998, 30: 405～434
6 Takahashi M, Osawa H, Fujisawa T. On a synchronization queue with two finite buffers [J]. Queueing Systems, 2000, 36: 107～123
7 Jang J, Shim S, Shin B. Analysis of DQLT scheduling for an ATM multiplexer [J]. IEEE Communications, 1997(1): 175～177
8 Bedford A, Zeephongsekul P. On a dual queueing system with preemptive priority service discipline [J]. European Journal of Operational Research, 2005, 161: 224～239
9 The ATM Forum Technical Commute Traffic Management Specification [S]. Version4. 0, 1996, 4