Internet 流分类方法的比较研究

彭 芸 刘 琼
(中国科学院 软件研究所 北京 100080)

摘 要 Internet 流分类是网络测量、流量监控中的一个重要环节。本文分析了几种典型的流分类方法:基于特定端口号、基于应用层特征字段和基于传输层的方法,其中第二种方法专门用于识别当前日益增多的对等网络应用流量。从准确性、完整性、实时性以及可扩展性等方面对这三种方法进行了比较,分别指出它们的优势和不足。最后提出了一种实用型流分类方案,并对流分类领域的发展提出了看法。

关键词 流分类,应用层特征字段,主机行为,统计特征

Comparison Research on the Methods of Internet Traffic Classification

PENG Yun LIU Qiong
(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract Internet traffic classification has always been an important part of network measurement and control. We first analyzed some typical methods of traffic classification, which separately based on default port numbers, application signatures and transport layer characteristics. Then we showed the advantages and disadvantages of each method through the comparison of their veracity, integrality, the peculiarity of real-time and expansibility. Finally, we presented a practical traffic classification scheme and gave some suggestions for the development of this field.

Keywords Traffic classification, Application signature, Host behavior, Statistic characteristic

1 引言

近年来,Internet 流分类在学术和应用领域备受重视,已形成一个相对独立的研究领域。用户对各类 Internet 业务的服务质量要求越来越精细;网络管理者需要对各种业务流进行实时的监控与管理;网络服务提供商在规划和建设网络时需要了解网络各类业务流的状况;Internet 研究人员需要关注网络中各种流的特征及相应的用户行为等,这些都离不开 Internet 流分类技术。

通过监控各类应用的网络流量,管理员可以及时发现设备故障,链路拥塞,用户带宽的使用状况等。此外,随着互联网的日益普及,网上传播病毒的种类与数量也越来越多,由此造成的危害也在不断升级。所以,如何有效遏制病毒传播是目前 Internet 急需解决的难题之一。Thomas 等人在文[1]中提到,如果一台主机利用一个或多个源端口扫描多台主机的同一个端口;或者是一台主机利用多个端口扫描另一台主机的多个端口,则这台主机发出的流很可能是攻击流。由此可见,通过识别可疑流,可以及时进行网络管理告警,达到预防病毒泛滥的目的。

网络服务提供商通过流分类,可以获悉各类网络应用所占比例,预测网络业务的发展趋势。传统技术采用尽力而为的方式进行包转发,对吞吐量、延迟、延迟抖动和丢包率没有任何保障,把传输损失都留给终端系统来处理,这对于过去以电子邮件传输和网页浏览为主的网络来说基本没有问题。最近几年,Internet 通信无论是在流量还是应用类型方面,都保持着飞速增长。同时音频,视频以及其它实时应用的加入,更是从根本上改变了人们对于 Internet 的使用方式。为了适应电话、视频、对等网络应用(P2P, Peer-to-Peer)等新型业务的大量普及,要求新一代的互联网必须能够为不同应用提供不同级别的服务质量(QoS, Quality of Service)保障,使用户得到更好的上网体验,因此,流分类已成为提供服务质量中不可缺少的重要手段。

对于研究人员,在 P2P 应用出现之前,网络传输基本上都是遵循客户端/服务器(C/S, Client/Server)模式,从链路带宽设计考虑,他们自然而然地选择了某种数字用户线路(xDSL, x Digital Subscriber Line)模式,即上行带宽小,下行带宽大。然而,最近几年的研究报告表明[2],P2P 已成为当前网络带宽的"杀手级"应用,其上传/下载比趋近于 1,造成传统 xDSL 网络的上行链路极易拥塞。所以,流分类的另一个重要性在于能够及时了解网络上各种应用流量所占的带宽比例及其趋势,帮助研究人员更合理地规划网络资源,为用户提供更好的服务质量。

为此,本文将对 Internet 流分类方法进行比较研究,全文内容安排如下:第 2 部分介绍分析几种典型的流分类方法及其适用范围,比较它们之间的优缺点;第 3 部分介绍一种实用型流分类方案;最后对流分类的方法提出了初步的改进建议,并对全文进行了总结。

2 流分类方法的分析与比较

随着网络带宽的不断提高,实时音频/视频,网络游戏,P2P 文件共享等新应用不断出现,很大程度上改变了用户对于 Internet 的使用方式,导致网络应用流量的比例发生了根本性变化。传统的网络应用(如 Http、FTP、TELNET 以及 SMTP 等)具有统一的标准和规范,在实现运行中大多采用固

彭 芸 硕士研究生,主要研究方向为网络测量、网络服务质量;刘 琼 CCF 会员,研究员,博士生导师,研究方向为多媒体通信、网络测量。

定端口号进行通信，因此，对于这类应用协议，早期的网络管理员等可以根据数据包头截取的端口号直接分类流量，并针对不同的应用执行不同操作，达到优化网络、提高服务质量的目的。然而，近年来一些新型应用协议基于安全性、灵活性等考虑，越来越多地使用动态端口号进行通信，如上述提到的流媒体，网络游戏和 P2P 文件共享等。因此，原有的流分类方法已不再适用，流分类算法的研究面临着新的挑战。

2.1 基于端口号的流分类方法

对于采用固定端口号进行通信的应用，流分类方法非常简单，通过截取数据包头的 5 元组，将其中的端口号与应用类型一一对应起来即可，并且其准确性和实时性都较为令人满意，属于确定性的分类方法，即根据某些标准直接判断出数据包所属的协议。然而，随着各种新型应用的不断出现，网络地址转换(NAT，Network Addresses Transformation)以及代理技术的使用等，端口号已经无法作为识别流量的唯一标识。但即使这样，基于端口号的流分类方法因为实现原理简单，技术成熟，适用于高速网络上的实时流分类，目前还未被完全淘汰。例如，在很多关于 P2P 流量特征的研究中[3~5]仍然使用默认端口号作为 P2P 流量的识别方法。

2.2 基于特征字段的流分类方法

该方法主要用于识别 P2P 协议流量，此类流量占网络总流量的比例逐年增加，在很多网络中甚至超过了 50%，所以，一旦能准确识别出 P2P 流量，则流分类问题可谓已解决了一大半。

表 1 几种流行 P2P 协议的特征字段

协议名	特征字段
Gnutella	"GNUTELLA","GIV","GET/uri-res","GET/get/", "X-Dynami","X-Query", "X-Ultrap","X-Max", "X-Quess","X-Try","X-Ext","X-Degree", "X-Versio","X-Gnutel", "GND"
FastTrack	"Get/. hash","GIVE", "X-Kazaa", 0x270000002980,0x280000002900, 0x29000000, 0xc028,0xc1,0x2a
eDonkey	0xe3,0xc5
Direct-Connect	"$ Send","$ Search", "$ Connect","$ Get", "$ MyNick","$ Direction", "$ Hello","$ Quit", "$ Lock","$ Key","$ MyInfo", "$ SR","$ Pin"
Bit-Torrent	"GET/announce? info_hash", "GET/torrents/", "GET TrackPak","0x13BitTorrent", 0x00000005,0x0000000d, 0x00004009

为了避免被检测和限制，目前大多数主流 P2P 协议都使用随机端口号[6]进行通信，甚至有些 P2P 应用为了躲避网络管理员的封杀，使用 80 端口(Http 使用的端口)来伪装自己的流量。为此，Sen 等人[7]在研究了几种当时流行的 P2P 协议(Gnutella，KaZaa，DirectConnect，BitTorrent，eDonkey)的信令流和数据流之后，主要针对数据流中的 TCP 流进行了详细的分析，在这些数据包的有效载荷中找到了具有代表性的唯一的特征字段及其位置。为了验证他们方法的有效性，Sen 等人提出从 3 个方面来对流分类技术进行评价：(1)准确性：分类结果的正、负错误率都很低；(2)实时性：即能够同时处理几百万条连接的数据，但计算量却相对较小；(3)健壮性：即这种流分类方法对于常见的路由不对称，丢包等网络现象不敏感。Sen 等人的实验结果表明基于特征字段的这种方法在上述 3 个方面都做得很好：(1)准确性方面，首先假设通过 P2P 默认端口的流量都是 P2P 流量，然后用基于特征字段的方法对这些流进行再判断，如果不属于 P2P 流，那么定义为一个负错误，结论显示该方法的负错误率一般小于 5%，只有 BitTorrent 协议的负错误率较高，约 9.9%；(2)实时性方面，经实验统计，只需要检查一条流的前 3～4 个包，即可捕获 99% 以上的 P2P 流量(实验设备已根据 5 元组将包汇聚成流)，因此认为实时性方面也基本没有问题；(3)健壮型方面，由于大多数 P2P 报文(包括信令流和数据流)都带有特征字段(除 BitTorrent 协议的特征字段一般仅出现在信令流中)，所以该方法在路由非对称或者少量丢包的情况下同样有效。Holger 等人在[6]中也做了类似的研究，并总结了当时几种流行 P2P 协议的特征字段，例如表 1 所示。(注，由于各种 P2P 协议都在不断更新，表中的特征字段仅作参考，并没有包括全部)

另外，不同 P2P 协议的特征字段都不相同，因此利用这种方法还可以进一步识别出各种 P2P 协议类型。基于特征字段的方法也属于确定性的分类方法。目前市场上多数流量监控系统中采用这种方法来专门识别 P2P 流量。

2.3 基于传输层的流分类方法

为了克服上述两种分类方法的不足，发展了基于传输层的流分类方法，这种方法属于概率分类方法(即根据衡量的指标不同，判断流属于某类应用的概率)。

2.3.1 BLINC 流分类方法 Thomas 等人[1]首先提出利用主机在传输层表现出的行为模式来对当今日益复杂的 Internet 流量分类，该方法的三个最大特点是：(1)无需解读数据包的负载，从而不会牵涉到用户隐私问题；(2)不需要知道与端口号相关的信息，因此不易被其所误导；(3)只需要获得一般网络监控设备能够提取的信息，不需要额外的设备开销，因此这种分类方法也被称为 BLINC(Blind Classification)。此外，该方法还有一特色，即用户可以根据实际情况在流分类的准确性和完整性之间进行折中，所谓完整性是指分类方法可以识别出的流量占网络总流量的比例。BLINC 方法的工作原理如下：(1)观察 Internet 上单个主机的行为特点，例如是否同时与多台主机通信，或者同时扫描另一台主机的多个端口；(2)从三个层次对主机行为进行分析，即反映主机连通度的社会层(Social)、反映服务提供者或消费者行为的功能层(Functional)以及表示传输层拓扑连接的应用层(Application)；(3)将观察到的主机群行为模式与已知的应用特征进行匹配，即根据事先构造好的图表进行匹配(例：如图 1 所示)。最后，利用由统计数据或凭经验得到的启发式进一步改善算法性能。Thomas 等人对采集到的不同数据集进行了实验验证，结论表明 BLINC 方法的准确性高达 90% 以上，同时完整性可达 80%～90%(针对不同的数据集)。Thomas 的这种基于传输层的流分类方法完全避开了对报文内容的检查，开创性地将研究焦点转移到网络主机的行为上，被誉为是流分类领域的一个新里程碑。

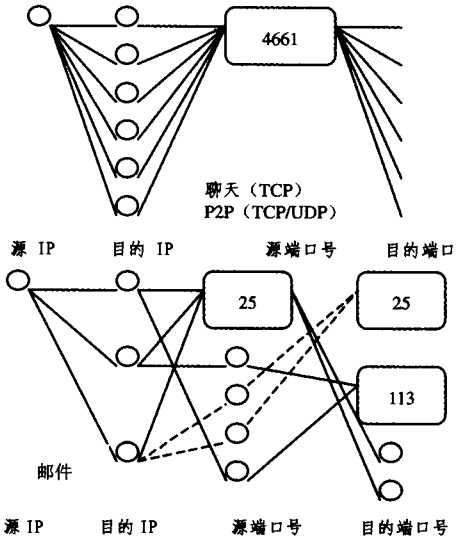

图 1　BLINC 方法中的部分匹配图表

2.3.2　*利用统计特征的流分类方法*　Zander[8] 等人凭借数据挖掘技术，将贝叶斯分类理论引入流分类领域，统计流量的各种特征，利用机器学习，对 Internet 上的流量进行分类。图 2 是他们的原型系统：

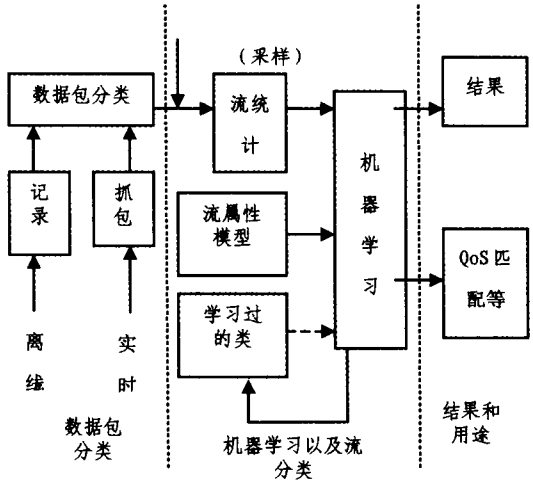

图 2　基于机器学习的流量分类[8]

这种方法使用 NetMate 工具[9] 根据 5 元组将数据包划分为不同的流，并分别计算流的各项参数，例如平均包长、平均包间隔时间、流持续时间等。在上述过程中，为进一步提高执行速度，还可以对每条流的数据进行适当采样[10]。之后，将流的统计数据以及初始的流属性模型用于自分类的机器学习算法[11]，即无人监督的贝叶斯分类方法。机器学习的时间越长，则分类的准确性越高，一旦达到某个标准，就可以对后续的输入数据流自动分类。最后，对流的分类结果进行评估，或是进入后续操作，例如 QoS 匹配等。实验结果显示根据被测数据集的不同，该方法分类的准确性会有所变化，但基本都高于 80%，平均值为 86.5%。

在整个系统中，最重要的部分莫过于流属性集合的选择。作者采用了顺序前进法（SFS，Sequential Forward Selection）来挑选最佳的流属性集合，该方法是目前最简单的自下而上搜索算法[12]。实验结果表明集合中属性数目越多，应用与类别之间的一一对应关系就越好，直到达到一个上限为止。Zander 等人充分利用了网络流量之间的内在关联，挖掘不同应用流量属性的统计特征，为流分类领域又开辟了一个全新的探索方向。

值得注意的是即使对一个简单应用来说，流属性的分布也非常复杂，因此不可能为每种应用都构建一个流属性模型。但是，从另一角度来看，如果一种应用符合多个流属性模型，则能对此应用有更深入的理解，例如，Web 应用通常还包含各种具体的内容，包括块传输，流媒体等等，所以其流量可能与多个流属性模型匹配，发现这一点有助于对 Web 应用进行更细致的划分。

上述两种基于传输层的流分类方法由于计算复杂，需要获取大量的网络流量或拓扑结构信息，目前还未能用于高速网络上流量的实时分类，但从它们对事先收集好的流记录的实验结果来看，在准确性、完整性方面都做得非常好，并且不用检查数据包的负载内容，不会牵涉到隐私等问题。

2.4　流分类方法的比较

首先，与其它两类方法相比，基于端口号的分类方法原理和实现都非常简单，可以满足高速网络上的实时分类要求，不涉及用户的隐私，不需要繁复的计算，可以用硬件实现；但另一方面，也正是由于其原理的简单，研究人员很容易设计出新型的通信协议逃避端口号检测，最常见的就是利用随机动态端口号通信或是使用其它应用的端口号来伪装自身流量，据不完全统计目前大约有 55% 的 P2P 流量使用随机端口号进行通信，因此，这种方法正逐步退出历史舞台。

而基于应用层特征字段的方法准确性较高，并且已经可以用于实时的流分类系统，是目前绝大多数流量监控系统选择使用的方法；但其弱点也显而易见，首先是完整性，它只能对现有已知的 P2P 应用进行识别，无法识别新型应用，而实际上 P2P 协议的更新周期是非常短的，新型版本不断涌现，如果是私有协议，则特征字段的破解开销较大，其次，该方法需要获取用户数据包的有效载荷，涉及到用户隐私问题；此外，这种方法对载荷加密的流量也束手无策。

基于传输层的流分类方法克服了前两种方法无法解决的难点，其共有的优点在于准确率高、完整性好，可以识别新型应用，还能提醒用户检查那些疑似的病毒攻击流。Thomas 等人设计的方法根据传输层主机的行为模式等信息识别各种应用，不易受到网络动态的影响，例如拥塞、延迟等。还能根据使用者的要求在分类准确性和完整性之间进行折中，但缺点是其准确性会受 NAT 等端口/IP 地址转换技术或监测设备位置的干扰，另外由于该方法还依赖于凭经验提出的启发式，留有漏洞使攻击者容易设计新协议逃避这种分类方法。

Zander 和 Thomas 的方法都属于概率分类方法，并且主要基于传输层分类。Zander 等人基于流量统计特征的方法，优势在于不依赖流的 IP 地址或端口号，因此不受 NAT 等技术的干扰，但缺点则是有些特征对网络动态变化极其敏感，例如包的到达间隔、流的持续时间等，并且到目前为止，还没有找到一套完整的与各种应用类型一一对应的流量属性集合。此外，Zander 和 Thomas 方法还有一个共同的缺点，计算量非常大，尚不能用于高速网络进行实时的流量分类。

从实现上来说，上述几种方法都属于网络测量中的被动测量方法，在流分类过程中基本不会对网络产生任何影响。而它们的主要缺点在于无法深入了解某些应用的网络行为，例如目前非常流行的 P2P 文件共享系统。另外，由于被动测量要求对数据包进行截取和检测，随着网络速度的迅猛发展，这些方法的实现代价将越来越高。

3 一种实用型流分类方案

在比较、分析了上述几种有代表性的流分类方法后，我们综合基于端口号和基于特征字段的方法，提出了一种实用型流分类方案，并准备利用自行设计的3层以太网交换机实现这个方案，如图3所示。

具体实现过程如下：利用交换机自带的端口镜像功能，将流经交换机任意端口的数据包复制到一个特定端口，并使这些数据包通过交换机内部的快速过滤(FFP，Fast Filter Processor)模块，与常用协议(例如Http、SMTP、DNS等)的默认端口号进行匹配，如果成功，则打上所属协议的标签，存入数据库中。如果没有匹配成功，则剩下的数据包通过另一个FFP模块，逐一进行特征字段的匹配，用于P2P协议流量的识别。如果识别成功，则在这个包上打一个表示所属P2P协议的标签，接着，所有包(无论是否匹配成功)都进入刷新流表模块。最后，将结果存入数据库。而对于那些直到最后都无法判断其协议的流量，则都归入未知协议，留待以后分析。

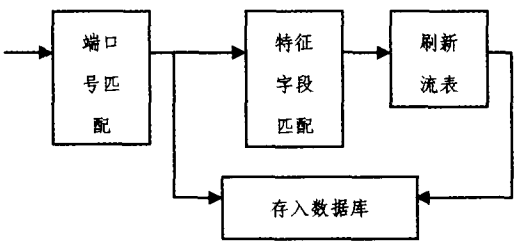

图3 流分类系统框图

刷新流表模块的主要工作包括：(1)创建流表项，每个表项包括源/目的IP地址、源/目的端口号、流的包数统计值以及开始/结束时间戳；(2)删除过期流表项，每次输入一个新的数据包，将其时间戳与所有表项的结束时间戳比较，超过某个特定值，例如64秒，则将那个表项存入数据库，然后从表中删除；(3)刷新表项，判断输入的数据包是否属于P2P流，以及它所属流的流表项是否已经存在，更新相应的流表项内容。

该方案目前正处于实施阶段，它利用端口号匹配，减少了后续特征字段匹配模块的数据输入，提高了处理速度。同时，其原理简单，易于工程实现。此外，根据CacheLogic公司近年来的报告[13]指出，P2P、Http协议的流量比例已经占总流量的70%以上，而目前我国国内占主导地位的两种P2P协议BitTorrent和eMule均开放源代码，有条件采集到它们的特征字段。因此，认为该方案有较好的完整性；在准确性方面，根据前文分析，特征字段匹配的准确性非常高，而Http和电子邮件等传统应用至今都仍使用固定端口号，所以，通常情况下其准确性也应该能得到保障。最后，在刷新流表模块中还可以加入Hash算法进一步提高执行速度。但正如前文所提到的那样，这种流分类系统的可扩展性较差，无法识别Skype等负载加密的P2P协议。

此外，我们对流分类方法的进一步研究还在继续中，例如探索如何实现并改进基于传输层的流分类方法，使之能在高速网络上进行实时的流分类，或开发一种效率更高、实用性更强的新型流分类方法。

总结与展望 由于端口跳变、负载加密等流量隐藏技术的发展，可以预见，基于端口和应用层特征字段的方法将被逐步淘汰。而目前的研究热点-基于传输层的流分类方法，虽然在准确性和完整性方面可以达到较高的要求，在实时性方面却仍然差强人意。从上述分析可以看出，未来流分类技术的发展趋势将具有以下几个特点：(1)逐步避免依赖端口号；(2)无需检测用户数据包的负载内容；(3)可扩展性好，能迅速得到新型应用的识别特征；(4)高准确率以及高完整性；(5)能在高速网络上实时运行；(6)对网络各种动态变化不敏感。因此，如何将基于传输层的流分类方法运用于高速网络是目前各方急需攻破的难点。文中介绍的Thomas和Zander等人的方法，前者利用的是网络中用户主机的行为模式以及它们之间的连接拓扑结构信息，而后者更多利用了流量的隐藏特征。一般而言，流量的隐藏特征较难以被用户自行更改，所以更不容易被设计回避。一旦能够找到有效的流属性集合，或者提出一种更好的机器学习算法来提高学习速度，都将会极大地推动流分类领域的发展。

进入21世纪后，Internet已经成为人们日常工作，学习以及娱乐等各方面必不可缺的工具。因此，越来越多的人开始关注于网络资源的有效利用，思考如何为用户提供更好的网络服务等问题，而要做到这些，准确的流分类技术是必不可缺的。从目前的趋势来看，比较有发展前景的还是基于传输层的方法，它挖掘出流量的各种隐藏特征，对主机的行为模式进行统计和归类；即使遇到新开发的应用协议，也能自动获得该应用的流量特征或主机行为模式，可扩展性较好。从最初基于端口号到目前基于传输层的方法，可以看出流分类技术将随着应用协议的发展而不断进化。

参 考 文 献

1 Karagiannis T, Papagiannaki D, Faloutsos M. BLINC: Multilevel Traffic Classification in the Dark [C]. ACM SIGCOMM, Philadelphia, PA, USA, August 2005

2 Plissonneau L, Costeux J L, Brown P. Analysis of Peer-to-Peer Traffic on ADSL [J]. Passive and Active Network Measurement, 2005, 3431: 69～82

3 Gerber A, Houle J, Nguyen H, et al. P2P The Gorilla in the Cable [C]. National Cable & Telecommunications Association, National Show, Chicago, IL, June 2003

4 Saroiu S, Gummadi K P, Dunn R. J, et al. An Analysis of Internet Content Delivery Systems [C]. In: Proceedings of the 5th Symposium on Operating Systems Design and Implementation, 2002

5 Sen S, Wang J. Analyzing peer-to-peer traffic across large networks [C]. In: Proceedings of ACM SIGCOMM Internet Measurement Workshop, Marseilles, France, November 2002

6 Bleul H, Rathgeb EP. A Simple, Efficient and Flexible Approach to Measure Multi-protocol Peer-to-Peer Traffic [J]. Networking-ICN 2005, 2005, 3421:606～616

7 Sen S, Spatscheck O, Wang D. Accurate, Scalable In-network Identification of P2P Traffic Using Application Signatures [C]. In: Proceedings of the 13th international conference on World Wide Web, New York, 2004

8 Zander S, Nguyen T, Armitage G. Automated Traffic Classification and Application Identification using Machine Learning [C]. In: Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary, 2005

9 NetMate [EB/OL] (http://sourceforge. net/projects/netmate-meter/)(August 2005)

10 Zander S, Nguyen T, Armitage G. Self-learning IP Traffic Classification Based on Statistical Flow Characteristics [J]. Passive and Active Networking Measurement, 2005,3431:325～328

11 Cheeseman P, Stutz J. Bayesian Classification (Autoclass): Theory and Results [A]. In: Fayyad U, et al, eds. Advances in Knowledge Discovery and Data Mining [C], Menlo Park, CA: AAAI Press, 1995

12 CacheLogic Research. The True Picture of P2P File Sharing [EB/OL]. (http://www. cachelogic. com/home/pages/research/p2p2004. php)(March 2006)

13 Yu Lei, Liu Huan. Feature selection for high-dimensional data: A fast correlation-based filter solution [C]. In: Proceedings of the Twentieth International Conference on Machine Learning, 2003