文章编号:1001 - 9081(2006)10 - 2338 - 03

基于 Mobile Agent 的协作式反垃圾邮件系统设计

张基温[1],刘英戈[1],陈广良[2],董建设[3]
(1. 江南大学 信息工程学院,江苏 无锡 214122;2. 解放军理工大学 指挥自动化学院,江苏 南京 210007;
3. 兰州理工大学 计算机通信学院,甘肃 兰州 730050)
(liuyingge80@yahoo.com.cn)

摘 要:提出一种基于 Mobile Agent 技术的协作式反垃圾邮件体系结构,并对由代理服务器、反垃圾邮件客户端、动态负载均衡层、Mobile Agent 层及反垃圾邮件服务器组成的五层结构进行阐述;代理服务器用来解决对邮件服务器的统一访问,降低由邮件服务器及客户端的多样性带来的系统复杂度;使用 Nilsimsa 算法实现相似邮件 Hash 过滤;最后对协作式反垃圾系统进行测试。

关键词:反垃圾邮件;协作式;移动代理;负载均衡
中图分类号: TP309.5;TP393.098 **文献标识码**:A

Design of collaborative antispam filter system based on the mobile Agent

ZHANG Ji-wen[1], LIU Ying-ge[1], CHEN Guang-liang[2], DONG Jian-she[3]
(1. *School of Information Technology, Southern Yangtze University, Wuxi Jiangsu* 214122, *China;*
2. *Department of Command Automation, University of Science and Technology, Nanjing Jiangsu* 210007, *China;*
3. *Department of Computer and Communication, Lanzhou University of Technology, Lanzhou Gansu* 730050, *China*)

Abstract: A collaborative antispam filter architecture based on the mobile agent was presented with key description of its architectural components including agent server, antispam client, dynamic load balance layer, mobile agent layer and antispam server. The agent server proposed here was for uniformed access to email servers, and brought down the complexity of filter systems resulted from the diversity of email severs and clients. Hash Filtration of similar emails was implemented by using Nilsimsa. Finally, the whole collaborative antispam filter system was tested.

Key words: antispam; collaborative; mobile agent; load balance

0 引言

协作式方法在垃圾邮件过滤中是一个相当新的概念,主要的协作式反垃圾邮件过滤系统有 Razor、Folsom、DCC 等。

Razor 包含一个垃圾邮件目录,客户端使用这个目录自动过滤已知的垃圾邮件。垃圾邮件通过报告代理被添加到目录中。Razor 可以和其他过滤系统协作完成垃圾邮件过滤。

Folsom 是对 Razor 的一种扩展,加入了身份认证和信用机制,主要依赖人工智能而非人工来识别垃圾邮件。

DCC 与 Razor 不同,它不是识别所有垃圾邮件,而是识别群发邮件,识别过程由管理员根据白名单实现。DCC 自动地将信息贴上“大量”的标签,而不需用户采取任何操作。

Razor 和 Folsom 的主要缺点是随着用户数量增加,系统效能下降很快。DCC 解决 Razor 和 Folsom 中的问题,但在解决假阳性、数据损坏、网络节点以及服务器过载存在明显的缺陷,且白名单的产生需要用户参与。

1 基于 Mobile Agent[3] 的协作式系统

1.1 协作式的基本思想

假设把反垃圾邮件中各种过滤手段的结果看成是知识,协作式的基本思想就是在全网内形成这些过滤知识共享,包括同一个节点内多种过滤手段之间的知识共享和不同节点间的协作学习、知识共享。

下面以协作式 Hash 过滤和协作式 Bayes 过滤作为切入点,设计一种基于 Mobile Agent 的协作式反垃圾邮件过滤系统框架。

1.2 协作式系统框架

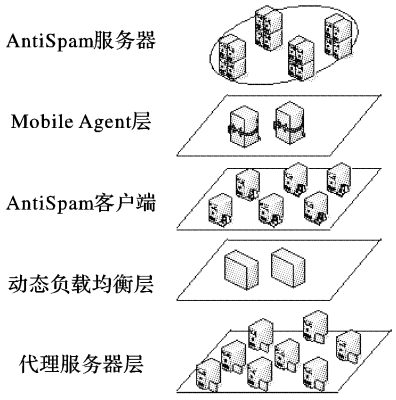

图 1 协作式反垃圾邮件系统

系统的网络示意图如图 1 所示。系统主要由五个部分组成:代理服务器层、动态负载均衡层、AntiSpam 客户端层、Mobile Agent 层、AntiSpam 服务器层。

代理服务器层:实现对邮件服务器的统一代理访问、邮件

收稿日期:2006 - 04 - 06 **基金项目**:国家自然科学基金资助项目(60403043)

作者简介:张基温(1943 -),男,山西临汾人,教授,主要研究方向:网络安全、电子政务; 刘英戈(1983 -),男,安徽庐江人,硕士研究生,主要研究方向:信息安全、反垃圾邮件网格; 陈广良(1978 -),男,安徽滁州人,硕士研究生,主要研究方向:协作式反垃圾邮件; 董建设(1971 -),男,河北赵县人,讲师,博士,主要研究方向:反垃圾邮件网格.

获取、邮件规则过滤等。引入代理服务器方案有效降低由邮件服务器及客户端多样性带来的复杂度。

动态负载均衡层:解决分布式系统中任务分配的问题,避免出现部分节点超载、部分节点空闲的状况。

AntiSpam 客户端层:接收代理提交的邮件进行 Hash 缓存过滤、Bayes 缓存过滤,并作为 Hash 过滤知识、Bayes 过滤知识的提供者和获取者。缓存过滤是指对近期访问的 Hash 及 Bayes 过滤最近访问的正常与垃圾关键字进行缓存,加快访问速度。

Mobile Agent 层:实现全局的过滤知识共享。

AntiSpam 服务器端:实现 Hash 统计更新、Bayes 过滤知识的数据共享。

1.2.1　Mobile Agent 技术

协作式方法最大的问题是如何使这些知识全局共享而不造成较大的网络流量,那种采用数据搬移、汇总的思想不太现实,所以引入了 Mobile Agent 来解决这个问题。Mobile Agent 能有效地降低分布式计算中的网络负载、提高通信效率、动态适应变化了的网络环境,并具有很好的安全性和容错能力。采用 Mobile Agent 可以避免大量数据在网络上的传输,其基本思路是将计算移到数据上去进行,而不是把数据移到计算中来。

如图 2 所示,本系统中 AntiSpam 服务器 MAE(Mobile Agent Environment)主要提供以下服务:

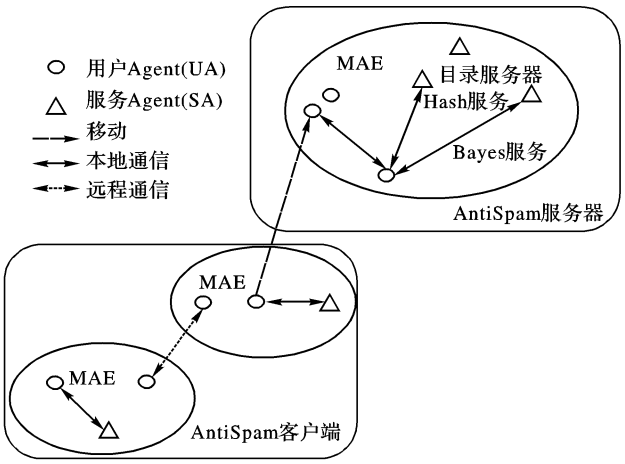

图 2　基于 Mobile Agent 的过滤知识共享

1.2.2　协作式系统的工作流程

协作式系统模块关系及数据流如图 3 所示。主要工作流程如下:

1)邮件到达 SMTP、POP3 或 HTTP 代理服务器的端口监听模块。

2)代理服务器获得邮件正文,调用“A 负载均衡”,根据动态负载均衡原则选择一个 AntiSpam 客户端,并将邮件正文投递给此客户端。

3)AntiSpam 客户端对邮件正文进行 MIME 邮件解析、Nilsimsa Hash 生成、中英文分词、特征项提取,具体过程如下:首先,检测本地缓存中有无曾经访问 AntiSpam 服务器带回的该 Hash 的统计情况,如果有则直接进行判断。本地缓存中存放三种阈值:Ham 阈值、LikelySpam 阈值和 Spam 阈值,若该 Hash 统计数超过 Spam 阈值则认为该邮件为垃圾邮件,检测结束;若统计数超过 LikelySpam 阈值,需要进行 Bayes 过滤;若统计数低于 Ham 阈值,根据策略可以继续检测也可以完成检测判定正常邮件。其次,利用本地缓存中的正常或垃圾邮件关键字库进行 Bayes 过滤,并结合 Hash 过滤结果作判断。第三,如果 Hash 过滤可以判断该邮件是否是垃圾邮件,Bayes 过滤则把该邮件作为训练邮件来进行学习。第四,如果 Hash 缓存过滤和 Bayes 缓存过滤均不能作判断,AntiSpam 客户端派出 User Agent,调用“B 负载均衡”,根据动态负载均衡原则选择一个 AntiSpam 服务器,并将该邮件的 Nilsimsa Hash 和 Bayes 过滤所需的特征项带出。

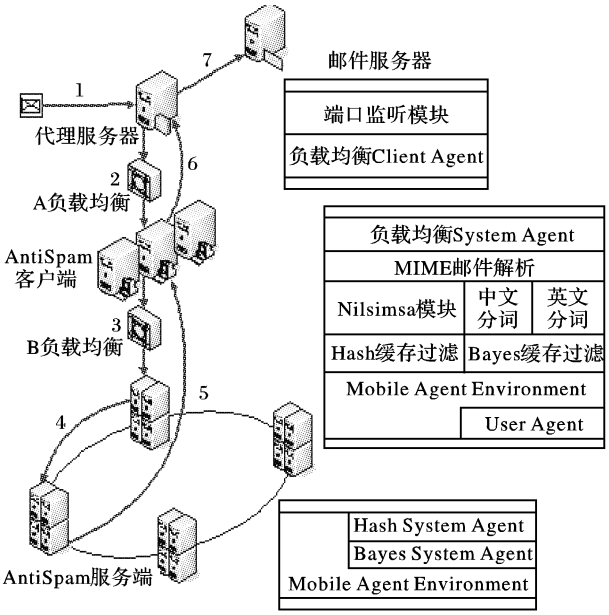

图 3　协作式反垃圾邮件模块关系及数据流图

4)User Agent 到达 AntiSpam 服务器后,在 Mobile Agent Enviorment 中调用 Hash Syste m Agent 和 Bayes System Agent,过程如下:首先,Hash System Agent 对 User Agent 带来的 Nilsimsa Hash 在 Hash 库中进行查询,如果有则该 Hash 的数目加 1;如果没有则在 Hash 库中增加此 Hash,置数目为 1;Hash 检测过程同上,即与 Spam、LikeSpam、Ham 阈值比较;其次,Bayes System Agent 对 User Agent 带来的特征项进行 Bayes 过滤,得出结果;第三,如果 Hash 过滤可以判断该邮件是否是垃圾邮件,Bayes 过滤则进行训练;第四,如果 Hash 过滤或 Bayes 过滤能够作判断,则 User Agent 直接带回判断结果;如果 Hash 过滤和 Bayes 过滤均不能作判断,则根据 User Agent 的策略,User Agent 转移到另一个 AntiSpam 服务器。

5)User Agent 到达另一个 AntiSpam 服务器后,执行过程同 4,但是 Hash 的更新与 Bayes 训练仅在第一次登录的 AntiSpam 服务器上面进行,这样可以保证数据的一致,其他的 AntiSpam 服务器仅为此 User Agent 提供查询服务。如果此 AntiSpam 服务器不能作判断,根据 User Agent 策略继续转移;否则将判断结果由 User Agent 带回 AntiSpam 客户端。

6)AntiSpam 客户端根据 Hash 过滤和 Bayes 过滤结果进行判断,根据结果进行标记发回给代理服务器。

7)代理服务器收到带标记的邮件后继续投递给邮件服务器。

2　系统测试

2.1　测试步骤及数据准备

对协作式反垃圾邮件系统的测试分成两步来进行,先对 Bayes 分类和 Nilsimsa 算法进行测试,使用 Nilsimsa 算法实现相似邮件 Hash 过滤在一些测试中证明了其在抵抗冲突和稳定性方面的优点,所以不再重复测试,沿用已知测试结论;然

后测试整个协作式反垃圾邮件系统。

对于 Bayes 分类和 Nilsimsa 算法,选用 Spamassassin 的开放语料集作为测试集。Spamassassin 语料库中共含有正常邮件 2 500 封,垃圾邮件 1 397 封。由于中文邮件没有开放语料库,均为自己收集,共 500 封,主要为垃圾邮件。

2.2 Bayes 分类[5]的测试标准及测试结果

在这里,定义合法邮件(Legitimate)被判为垃圾邮件(Spam)的错误为 $L \to S$,相反的则为 $S \to L$。

分类中两个常用的评价指标准确率(Acc)和错误率(Err)。在反垃圾邮件中,$WAcc = \frac{\lambda n_{L\to L} + n_{S\to S}}{\lambda N_L + N_S}$,$WErr = \frac{\lambda n_{L\to S} + n_{S\to L}}{\lambda N_L + N_S}$。($Err = 1 - Acc$)。$n_{L\to L}$ 和 $n_{S\to S}$ 为正确分类的合法邮件和垃圾邮件的数量。$n_{L\to S}$ 和 $n_{S\to L}$ 为把合法邮件判断为垃圾邮件、把垃圾邮件判断为合法邮件的数量。n_L 和 n_S 为待分类的垃圾邮件和合法邮件数目。

考虑到 $L \to S$ 和 $S \to L$ 分别会有不同的代价,并设 $L \to S$ 的代价是 $S \to L$ 代价的 λ 倍,下面定义两个新的评估目标,分别是 $WAcc$(加权的正确率)和 $WErr$(加权的错误率):

$$WAcc = \frac{\lambda n_{L\to L} + n_{S\to S}}{\lambda N_L + N_S},\ WErr = \frac{\lambda n_{L\to S} + n_{S\to L}}{\lambda N_L + N_S}$$

在没有过滤情况下,得到基准 $WAcc$ 和基准 $WErr$ 别为:

$$WAcc^b = \frac{\lambda N_L}{\lambda N_L + N_S},\ WRErr^b = \frac{N_S}{\lambda N_L + N_S}$$

定义 TCR 为过滤器与基准的比值,TCR 越大,过滤性能越好。若 TCR 小于 1,意味着过滤后的结果比没有过滤效果还差。

$$TCR = \frac{WErr^b}{WErr} = \frac{N_S}{\lambda N_{L\to S} + N_{S\to L}}$$

Bayes 算法中有两个重要的参数:1)用于训练的样本个数 n;2)在过滤中计算最终概率的特征数目 m。下面主要研究 R 和 n 以及 R 和 m 之间的相互关系。

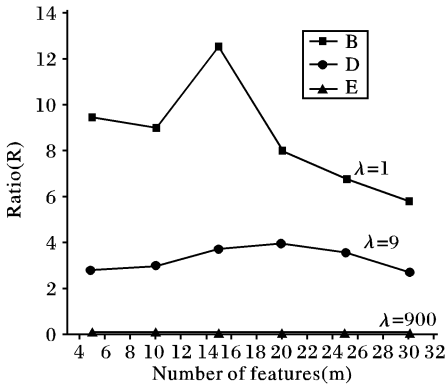

图 4 $R - m$ 关系

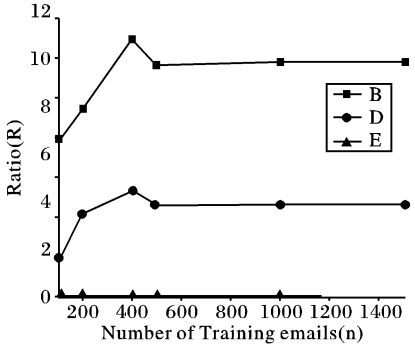

图 5 $R - n$ 关系

由图 2 可知,$\lambda = \frac{L \to S \text{ 的代价}}{S \to L \text{ 的代价}}$

当 $\lambda = 1$,最佳的特征项数目 m 为 15 个。

当 $\lambda = 9$,最佳的特征项数目 m 为 20 个。

当 $\lambda = 900$,R 远远小于 1,比没过滤还差。

根据图 4、5 决定选择 $\lambda = 1$,$m = 15$,即每封训练的特征项目数为 15 个,训练集选择为 400 封。

2.3 协作式反垃圾邮件系统测试

用 4 台机器作邮件群发机、4 台作 SMTP 代理服务器、4 台邮件服务器、2 台 AntiSpam 客户端、2 台 AntiSpam 服务器。

邮件群发机仿真正常、垃圾邮件比例向邮件服务器发送邮件,SMTP 代理服务器截取正文后提交给 AntiSpam 客户端及 AntiSpam 服务器端进行监测。

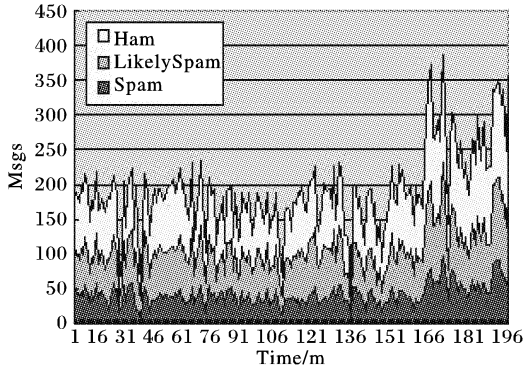

图 6 协作式 Hash 系统测试结果

图 6 记录了系统稳定后的协作式 Hash 过滤系统监测到的邮件的分布情况:最上方区域为正常邮件(Ham)即接受者数目少于 20 的邮件;中间区域为近似垃圾邮件(LikelySpam)即接受者数目在 20 与 100 之间的邮件;最下方区域为垃圾邮件(Spam)即接受者数据超过 100 的邮件。

协作式 Hash 过滤系统监测出来的近似垃圾邮件继续进行协作式 Bayes 过滤,如果 Bayes 过滤判断为垃圾邮件的则归入垃圾邮件。结果表明过滤系统监测到的邮件分布与邮件群发机发送的分布情况相同,垃圾邮件识别率达到 95% 以上,说明这种基于 Mobile Agent 技术的协作式过滤方案过滤效果还是很好的。

3 结语

设计并实现了一种基于 Mobile Agent 技术的协作式过滤系统框架,较好地解决了分布式反垃圾邮件系统的数据搬移问题;采用的代理服务器方案能够解决对邮件服务器的统一访问,降低邮件服务器及客户端的多样性带来的过滤系统的复杂度;利用 RMI 技术初步解决了分布式系统的负载均衡问题。然而还存在一些地方还需要进一步改进和完善,针对协作式反垃圾邮件系统,文中是以协作式 Hash 和协作式 Bayes 为切入点来实现的,下一步需要加入更多的过滤算法,并且需要着重考虑协作式系统中各个节点及算法间的协作信任机制问题。

参考文献:

[1] 曹麒麟,张千里. 垃圾邮件与反垃圾邮件技术[M]. 北京:人民邮电出版社,2003.

[2] http://www.spam.com.cn/,2006.

[3] KOTZ D, GRAY R. Mobile code: The future of the internet[A]. In workshop mobile agents in the context of competition and cooperation at autonomous agents'99[C]. Seattle: Mobile Agents in the Context of Competition and Cooperation, 1999.6 - 12.

[4] GRAHAM P. A Better Bayesian Filtering[A]. At the 2003 spam conference[C]. January 2003.

[5] 詹川. 反垃圾邮件技术的研究[D]. 电子科技大学,2005.