垃圾邮件综合举报关键技术

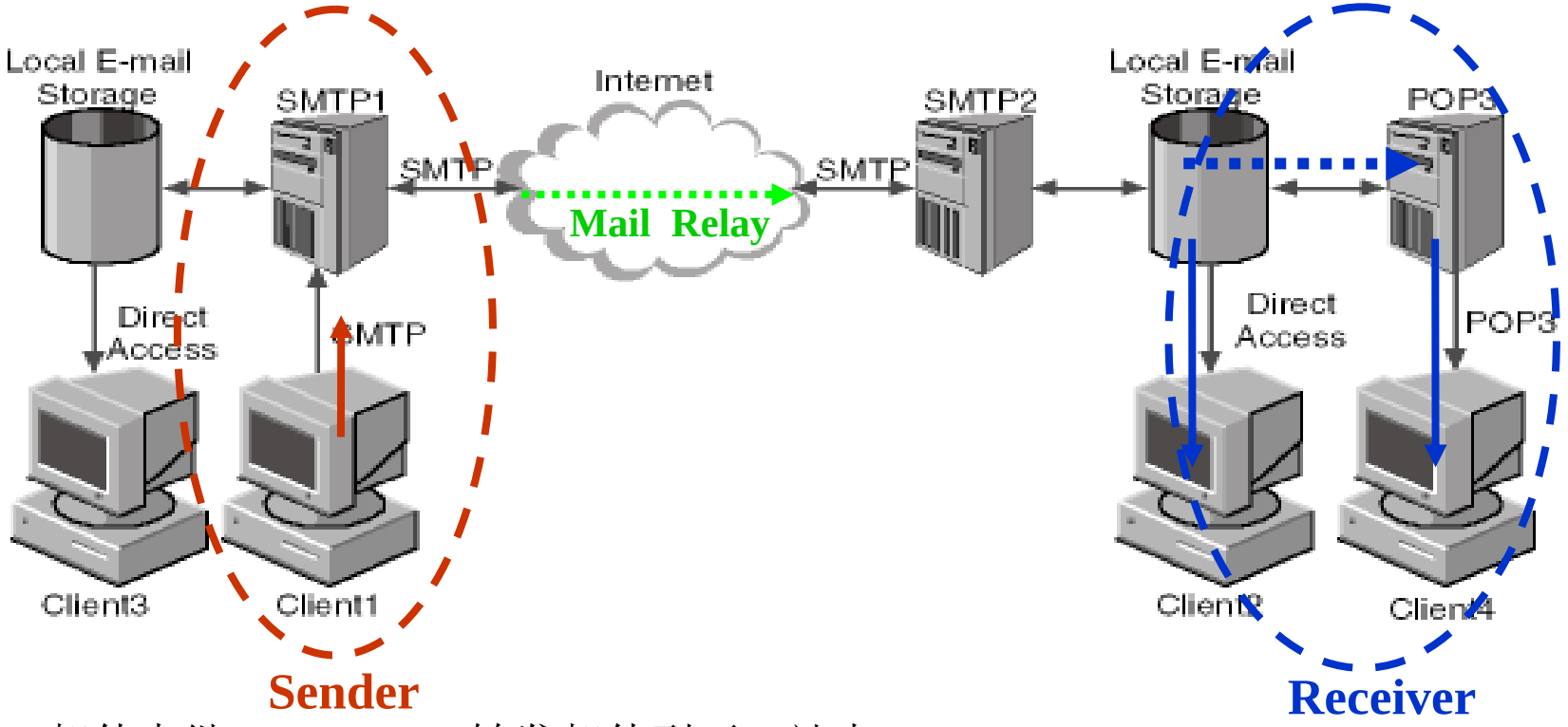
报告人：王兴伟
所在单位：东北大学

主要内容

- 电子邮件
- 垃圾邮件
- 传统反垃圾邮件技术
- 垃圾邮件综合举报关键技术
- 系统实现

电子邮件

电子邮件是互联网的基础应用和关键应用之一



- 邮件中继Mail Relay: 转发邮件到下一站点
- 传输路径包括多个中继

SMTP

- **SMTP：Simple Message Transfer Protocol 简单邮件传输协议，基于RFC 524发展而来，RFC524是在1973年提出的**
- **一些 SMTP 命令:**

MAIL FROM: <reverse-path>

Repeated for each recipient:

RCPT TO: <forward-path>

RCPT TO: <forward-path>

If unknown recipient: response “550 Failure reply”

DATA

email headers and contents

.

VRFY username

250 (user exists) or 550 (no such user)

SMTP

- SMTP协议的天生缺陷
  - 设计时考虑在可信环境下使用
  - MAIL FROM字段的数据完全由发送者控制，缺少验证机制
  - 对于接收者所在的电子邮件服务器仅仅能看到和它直连的传输服务器的IP地址，缺少发送服务器真伪的辨别能力

SMTP

- Received字段和From字段的不可信

From someone@mail.neu.edu.cn (202.118.1.83) ...

From relays:
Received: from cs-smtp-1.tsinghua.edu.cn
Received: from smtp3.tsinghua.edu.cn
Received: from anothernone.tsinghua.edu.cn

- ✓ Received 字段由邮件中继写入——不可信赖
- ✓ From 字段由接收者所在邮件服务器写入——缺少认证

电子邮件

- 小 结
  - **SMTP基于1973年提出的RFC524**
  - **SMTP协议安全性存在不足**
  - 垃圾邮件泛滥根本原因

垃圾邮件

- 垃圾邮件的出现
  - 1985 年8 月一封通过电子邮件发送的链锁信，一直持续到1993 年，这是首次关于垃圾邮件的记录
  - 1993 年6 月在Internet 上出现了名为“Make Money Fast”的电子邮件
  - 1994 年4 月Canter &Siegel 的法律事务所把一封移民顾问服务广告邮件发到6000 多个新闻组，一时间群情激奋

    ——首次用spam称呼垃圾邮件
  - 1995 年5 月出现第一个专门的垃圾邮件群发软件Floodgate

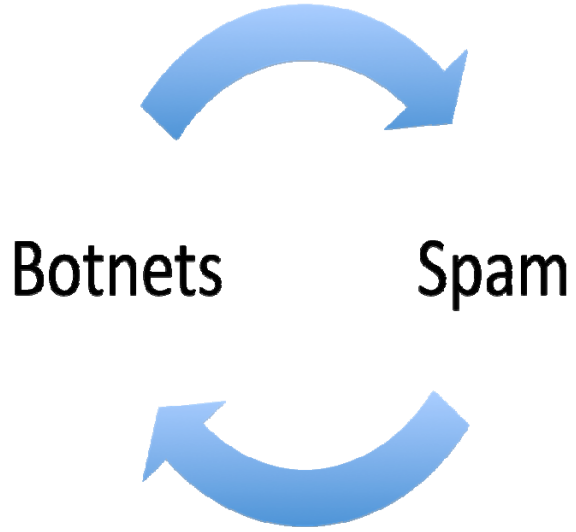
垃圾邮件

- 垃圾邮件的演化
  - ✓ 2001年1月
    - 8% （全美国电子邮件流量中垃圾邮件的比例）
  - ✓ 2003年1月
    - 42%
  - ✓ 2003年底
    - 超过 50%
  - ✓ 2008年底
    - 超过 80%
  - ✓部分企业甚至占到每天接收邮件总数的95%

数据来源 Symantec Brightmail

垃圾邮件

- 常见垃圾邮件类型
  - ✓ 商业
  - ✓ 政治
  - ✓ 色情
  - ✓ 病毒



垃圾邮件

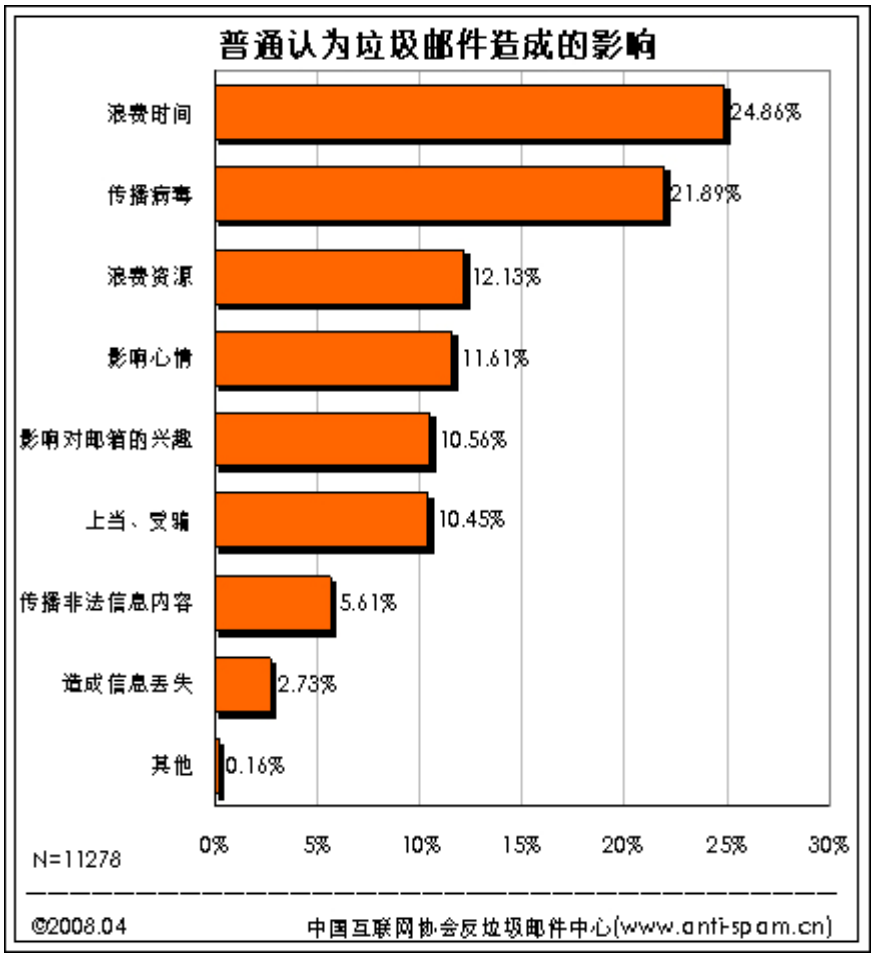
- 垃圾邮件的危害
  - 调查显示，垃圾邮件已成为互联网用户的最大烦恼，垃圾邮件的病毒率高达47%
  - 统计表明，垃圾邮件给美国企业造成的损失落实到每位职员身上折合约为874美元
  - 2003年我国处理垃圾邮件浪费的GDP高达48亿元人民币
  - 2008年，中国网民平均每周收到垃圾邮件的数量为17.64封

垃圾邮件

- 垃圾邮件的危害
  - 国家层面：政治、经济、文化
  - 用户层面：学习、工作、生活
  - 还包括：
    - 网络安全性、稳定性、高效性
    - 占用带宽、存储空间
    - 被列入各种黑名单
    - 声誉、国际影响

垃圾邮件

- 垃圾邮件的危害
  - ✓浪费时间
  - ✓传播病毒
  - ✓浪费资源
  - ✓影响心情
  - ✓影响对邮箱的兴趣
  - ✓上当、受骗
  - ✓传播非法信息内容
  - ✓造成信息丢失等



垃圾邮件

- 垃圾邮件的定义

  目前为止，垃圾邮件还没有一个准确的定义，一般认为垃圾邮件是：

  - 没有意义的电子邮件
  - 未经同意的大量邮件

    (UBE, Unsolicited Bulk E-mail)
  - 未经同意的商业邮件

    (UCE, Unsolicited Commercial E-ma

垃圾邮件

- 垃圾邮件的定义

《中国互联网协会反垃圾邮件规范》里的定义

（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件

（二）收件人无法拒收的电子邮件

（三）隐藏发件人身份、地址、标题等信息的电子邮件

（四）含有虚假的信息源、发件人、路由等信息的电子邮件

垃圾邮件

- 小结
  - 垃圾邮件的演化
  - 垃圾邮件的危害
  - 垃圾邮件的定义
  - 反垃圾邮件技术已经成为网络与信息安全领域的重要研究内容之一

垃圾邮件发送技术

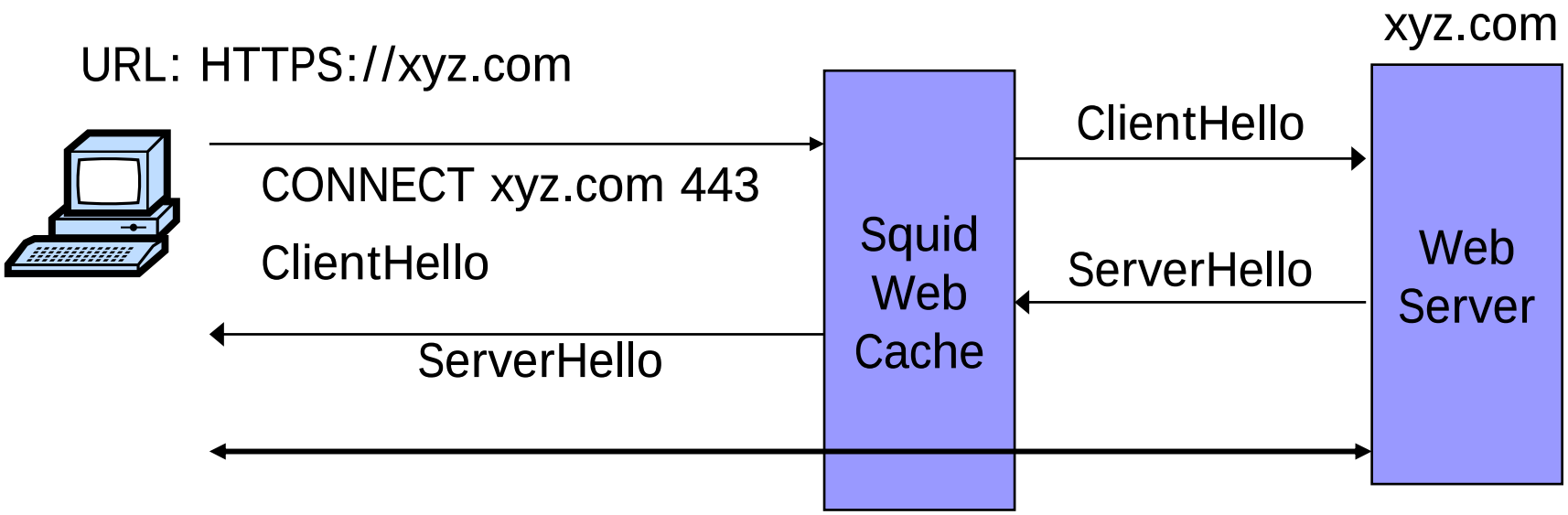
- 利用开放中继（Open Relay）
  - ✓ 利用SMTP协议使用中继方式传输邮件
    1. 群发工具建立和中继间的SMTP连接 (25端口)
    2. 传送收件人列表信息 (通过RCPT TO 命令)
    3. 传送邮件体——一次给所有收件人
    4. 开放中继不加验证地中继这些邮件
  - ✓ 正常中继在邮件头中添加 Received字段信息以标识其IP地址，非法中继则不这么做

垃圾邮件发送技术

- 一个发送垃圾邮件的例子：bobax蠕虫
  - 通过网络干扰计算机
    - 利用微软的LSASS.exe的缓冲区溢出漏洞攻击
  - 慢速扩散
    - 通过被感染机器执行自我复制程序
    - 随机扫描有漏洞的计算机
  - 一旦主机被感染(执行垃圾邮件僵尸程序spam zombie)
    - 在该主机上安装Open Relay程序，用来发送垃圾邮件
    - 如果该主机被加入了RBL（实时黑名单），则蠕虫将感染其他主机继续发送垃圾邮件

垃圾邮件发送技术

- 利用开放代理（Open Proxies）
  - 网页缓存代理程序 (基于HTTP/HTTPS的代理)
    -- 如squid



  - 垃圾邮件发送者可以通过连接该代理的25端口执行SMTP命令，这时的Squid 被变成了一个邮件转发代理

垃圾邮件发送技术

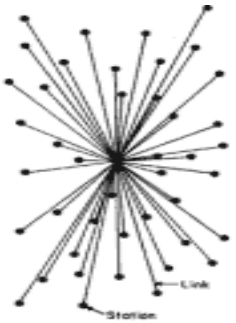
- 搜索开放中继和开放代理
  - 已经存在这类提供开放中继和开放代理列表的服务:
    - http://www.multiproxy.org/
      http://www.stayinvisible.com/
      http://www.blackcode.com/proxy/
      http://www.openproxies.com/ (每月20美元)

垃圾邮件发送技术

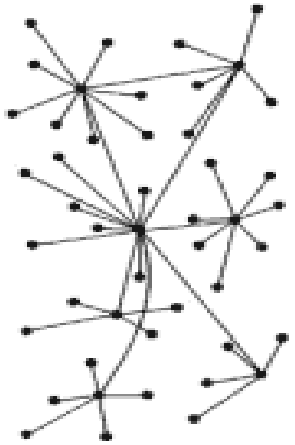
- 垃圾邮件群发工具（spamware)
  - 获取大量邮件发送目标地址列表
    - 推销目标关键字搜索
    - 广泛的网络搜索以发现合法的电子邮件地址
    - 目录获取攻击（Directory Harvest Attacks）
    - 压力攻击（ Brute force sequence attacks）
    - 字典粉碎攻击（ Dictionary mashing attacks）
  - 采用匿名方式批量发送邮件

垃圾邮件发送技术

- 垃圾邮件发送方式的演化



- One to many
  - 利用垃圾邮件群发工具
  - 购买邮件地址列表



- Many to many
  - 基于僵尸网络(Zombies-networks)发送
  -同病毒(Virus)、钓鱼(Phishing)、间谍(Spyware)等程序结合

垃圾邮件发送技术

- 小结

  - ✓早期——利用协议漏洞

    利用开发中继或开放代理发送

  - ✓发展——智能化发送技术

    发件人地址随机变化、邮件主题随机变化、伪造邮件头干扰信息、信体内容随机变化、正文以图片方式显示、使用垃圾邮件群发工具

  - ✓恶化——对抗反垃圾邮件技术，多层次，更加智能化

    信体加入干扰内容识别算法的文字，利用人的视觉反差干扰内容分析，结合动态IP技术低速群发垃圾邮件

传统的反垃圾邮件技术

小结

- ✓预防
  - 增强邮件服务器安全性
  - 提高邮件系统防病毒能力
  - 提供邮件服务安全身份认证
- ✓检测
  - 电子邮票
  - Challenge-Response
  - DomainKeys
  - SPF、DMP、RMX
  - RBL
  - 黑/白/灰名单
  - 连接频度
  - 反向域名验证
  - 关键词过滤
  - 贝叶斯过滤
  - 基于规则评分的过滤

垃圾邮件综合举报

- 传统松散的、“烟囱林立”式的反垃圾邮件方式越来越不能满足日益增长的网络与信息安全管理需求
- 通过构建垃圾邮件综合举报系统模型与功能框架，开展关键技术研究，进而实现具有自主知识产权的垃圾邮件综合举报系统是一项重要任务
- 国家242信息安全计划资助

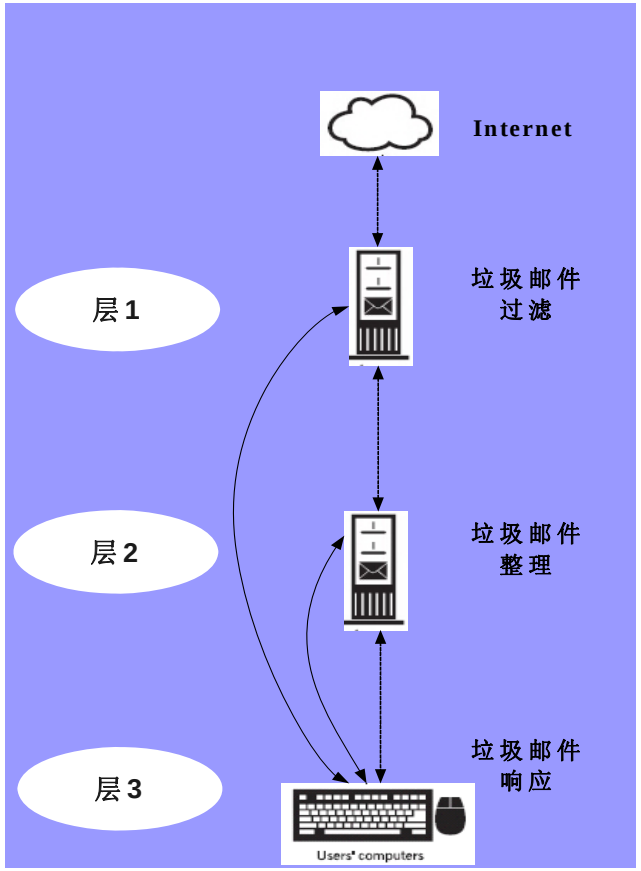
垃圾邮件综合举报

- 建立垃圾邮件综合举报系统三层模型

  层1：负责垃圾邮件过滤工作

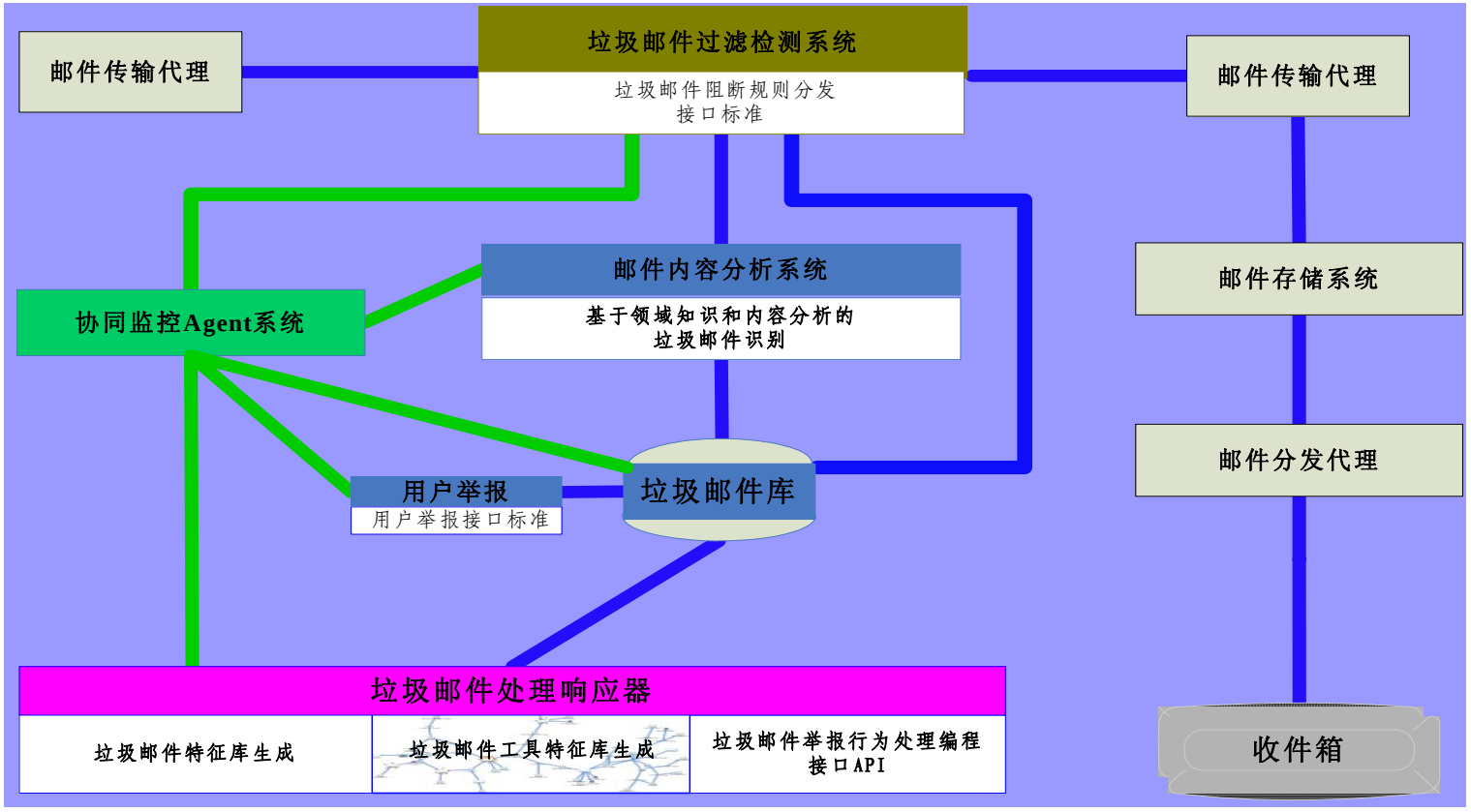
  层2：负责垃圾邮件整理工作

  层3：负责垃圾邮件处理响应工作



垃圾邮件综合举报

- “初审-复审-学习反馈”一体化协作式垃圾邮件综合举报系统架构



关键技术

- 协同监控Agent技术
  - 主要解决“初审、复审、学习反馈”三者之间的相互协同问题
- 基于内容分析的垃圾邮件识别技术
  - 对邮件正文进行内容分析
  - 基于最大熵模型统计过滤

关键技术

- 垃圾邮件属性特征和特征串自动发现技术
  - 引入N-gram串特征和领域特征识别技术，从不同层次上表示邮件内容
  - 通过统计模型融合不同层次的特征，采用基于AdaBoost的特征发现技术
- 基于快速扫描算法的垃圾邮件过滤技术
  - 采用Wu-Manber算法来实现

关键技术

- 基于反馈学习的自适应技术
  - 采用基于反馈学习的boosting自适应技术
- 基于垃圾邮件分类子集路径跟踪的热区发现技术
  - 通过分析垃圾邮件分类子集，进行路径跟踪，确定垃圾邮件发生热区
  - 实施网络层阻断，乃至进行反制

关键技术

- 客户端垃圾邮件过滤技术
- 垃圾邮件特征库与垃圾邮件发生工具特征库建立技术

关键技术

- 垃圾邮件样本分析技术
- 样本收集与存储技术
  - 大规模样本收集
  - 样本库消重技术
    - 基于内容分析的深层消重

关键技术

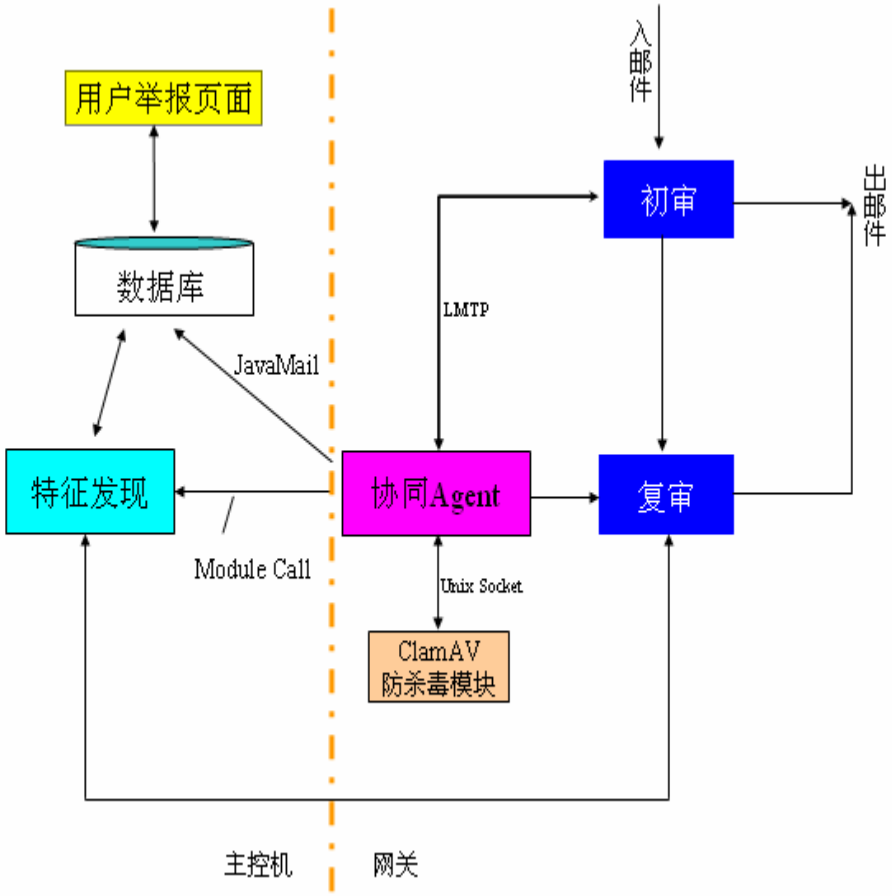
- 垃圾邮件样本分析技术
- 样本语料库建立技术
  - 适用于训练改进分类器
  - 提供统一的评测语料平台
  - 提高反垃圾邮件产品的效率
  - 促进反垃圾邮件产品的规范化
- 垃圾邮件举报接口标准和垃圾邮件阻断规则分发接口标准建议草案

系统实现

- 对上述关键技术进行实现与性能评价，并进行适当改进
- 集成上述关键技术，实现垃圾邮件综合举报软件系统

系统实现

➢系统结构



基于如下目标

- ➢初审快速
- ➢复审精确
- ➢支持学习反馈

系统包括

- ➢主控机
- ➢邮件网关服务器

系统实现

- 主要子系统
  - ✓通用模块子系统
  - ✓邮件入库子系统
  - ✓特征发现子系统
  - ✓邮件初审子系统
  - ✓邮件复审子系统
  - ✓协同监控Agent子系统
  - ✓用户举报接口
  - ✓主流群发工具特征库建立子系统
  - ✓垃圾邮件分析子系统

系统实现

- 通用模块子系统
  - ✓邮件解析

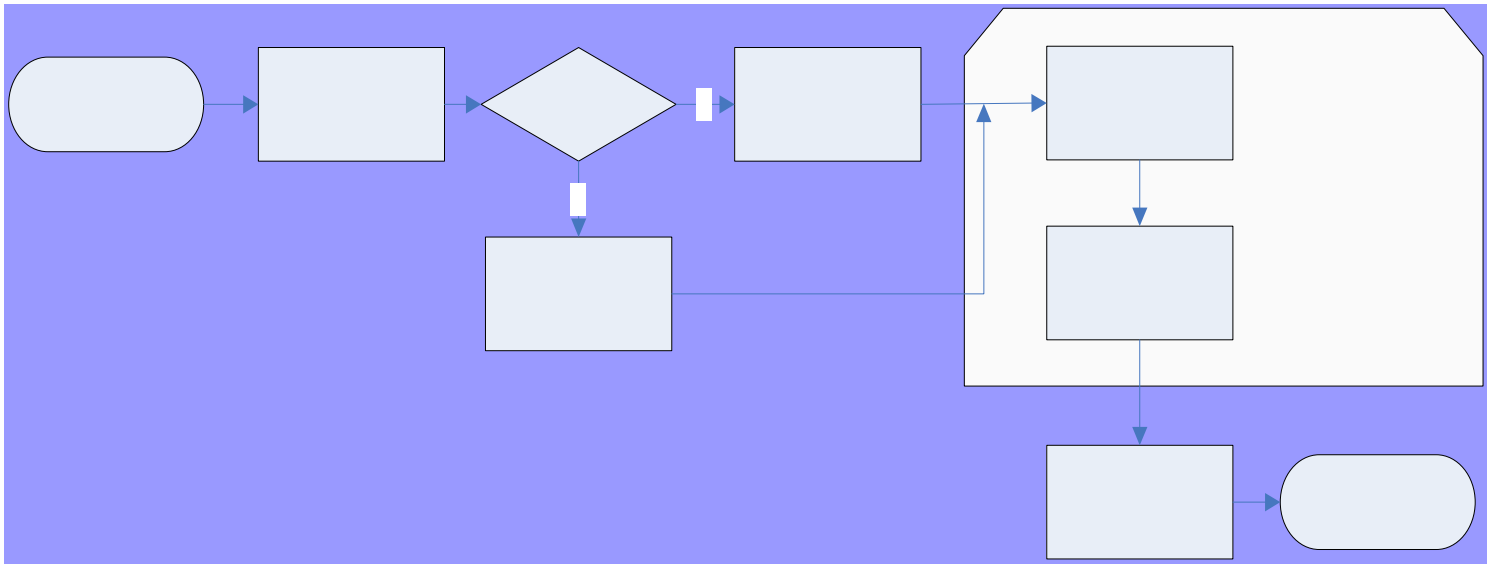
    解析RFC822邮件格式，提取正文、主题等信息
  - ✓邮件预处理

    主要是处理邮件文本，得到字元串和分段信息

系统实现

- 邮件入库子系统

将邮件样本按照特征发现、复审分类器的训练需求收集到主控机数据库中去，流程如下：



系统实现

- 特征发现子系统
  - ✓由样本库消重、样本读取、**Ngram**统计、**Ngram**过滤、特征选择等组成
  - ✓处理流程

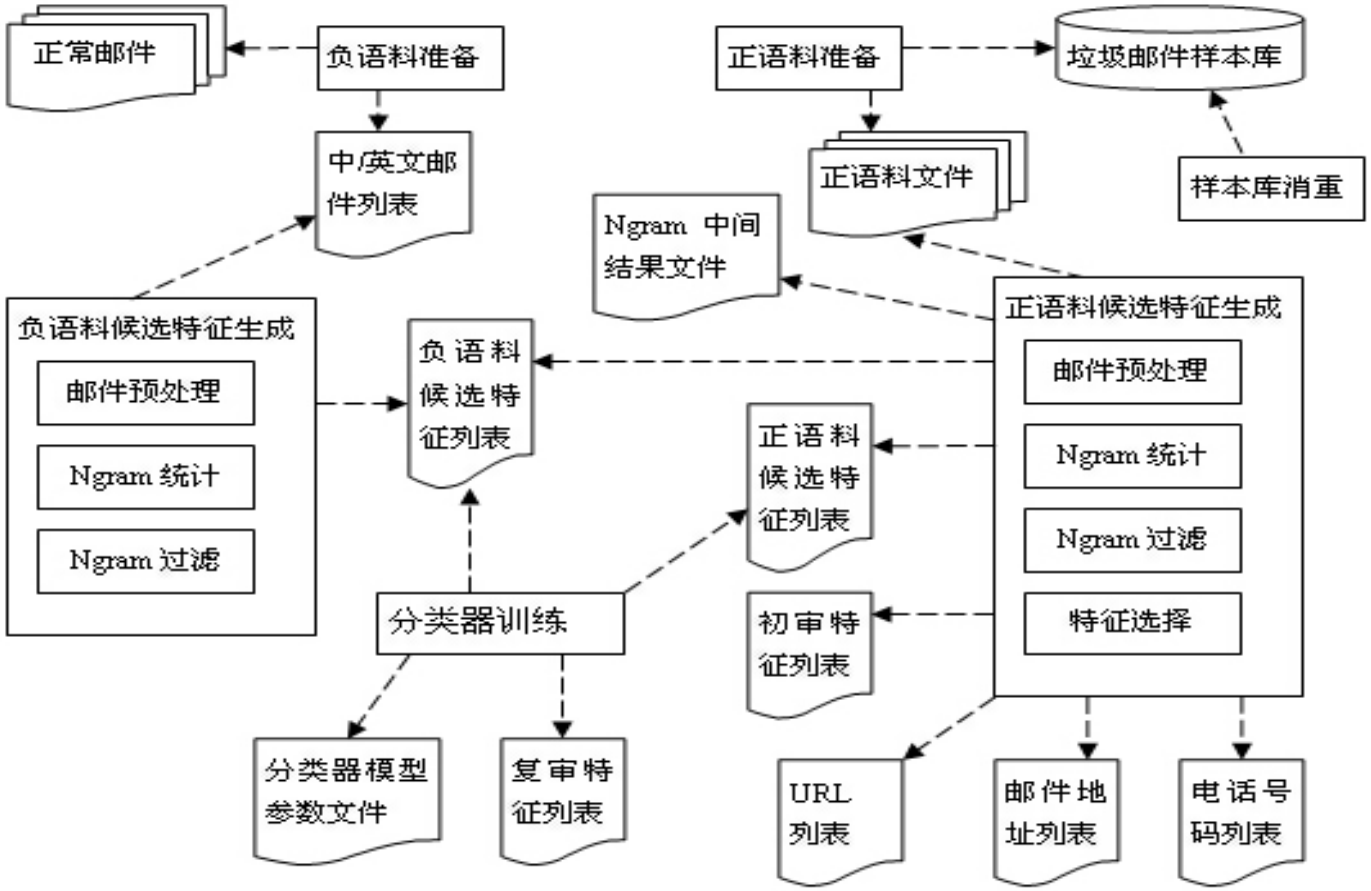
    调用消重模块对样本库中的垃圾邮件进行消重处理

    调用正语料准备模块更新正语料（垃圾邮件）

    调用负语料准备模块更新负语料（正常邮件）

系统实现

- 特征发现子系统示意图



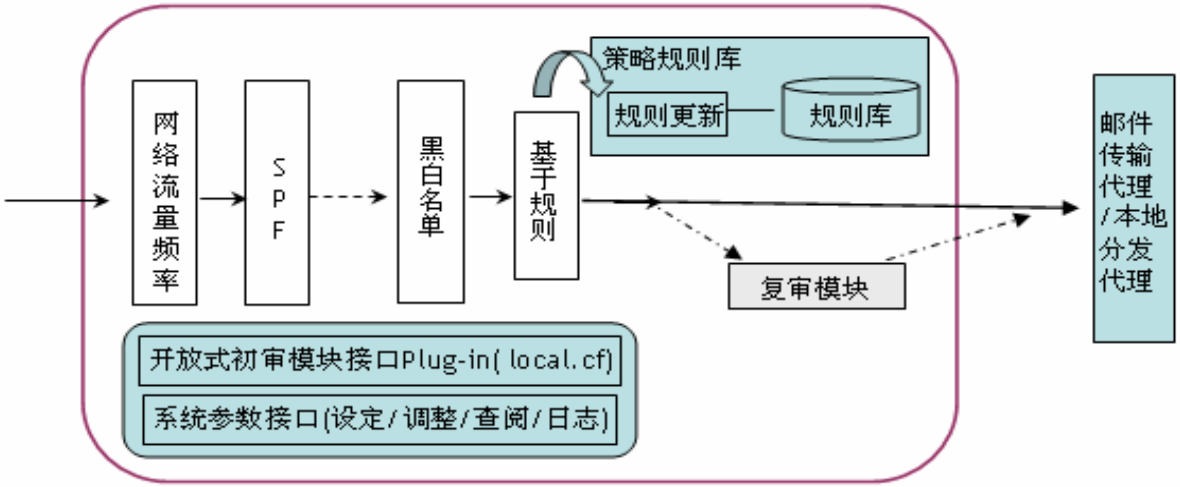
系统实现

- 垃圾邮件属性特征和特征串发现技术
  - 基于**Ngram**的特征选择方法
  - 应用领域知识改善特征表示
  - 邮件特征区域识别
  - 垃圾邮件隐藏特征的发现与使用
  - 增量式学习与特征自动发现的结合

系统实现

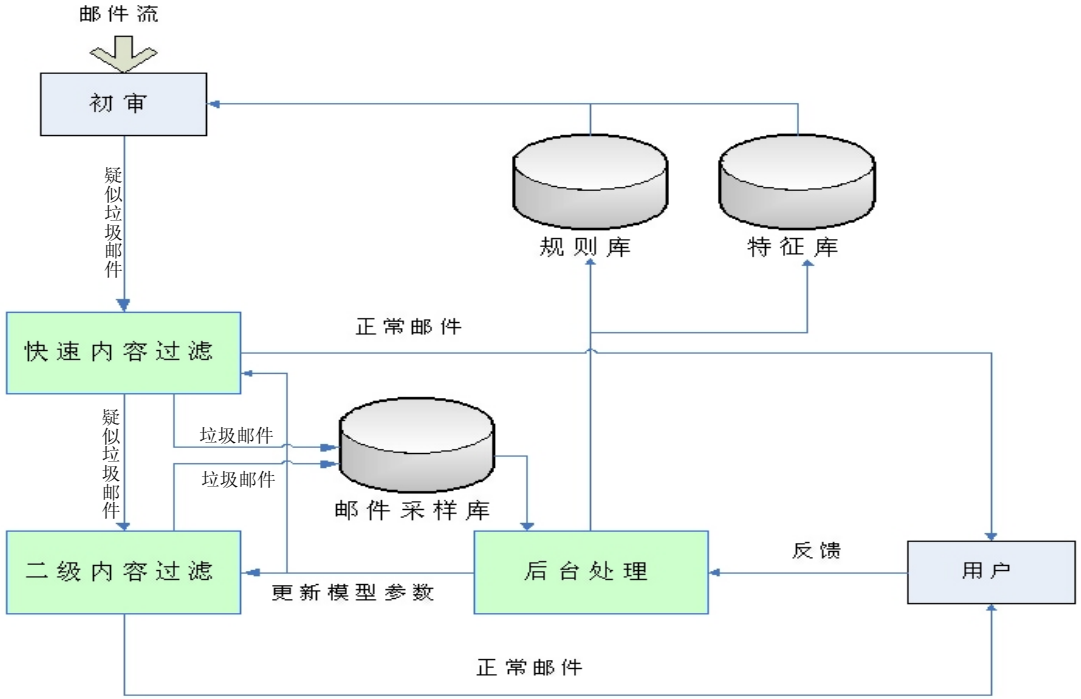
邮件初审子系统

- **SMTP特征检测—邮件传输阶段行为特征检测**
- 基于规则判分，目前系统使用规则近**1700**条
- 具备开放式模块接口



系统实现

- 邮件复审子系统
  - 分层过滤“疑似”垃圾邮件：快速 / 二级内容过滤
  - 特征匹配
  - 分类器判定
  - 建立与更新垃圾邮件特征库和规则库



系统实现

- 邮件复审分类器

  K最临近（KNN）分类器

  - ✓自适应性能好，对训练实例敏感
  - ✓对二类分类问题，不需要负语料（正常邮件）
  - ✓主要用于二级内容过滤
  - ✓改进并实现了一种**1NN**算法，用于复审模块对用户举报邮件的自适应过滤

系统实现

- 邮件复审分类器

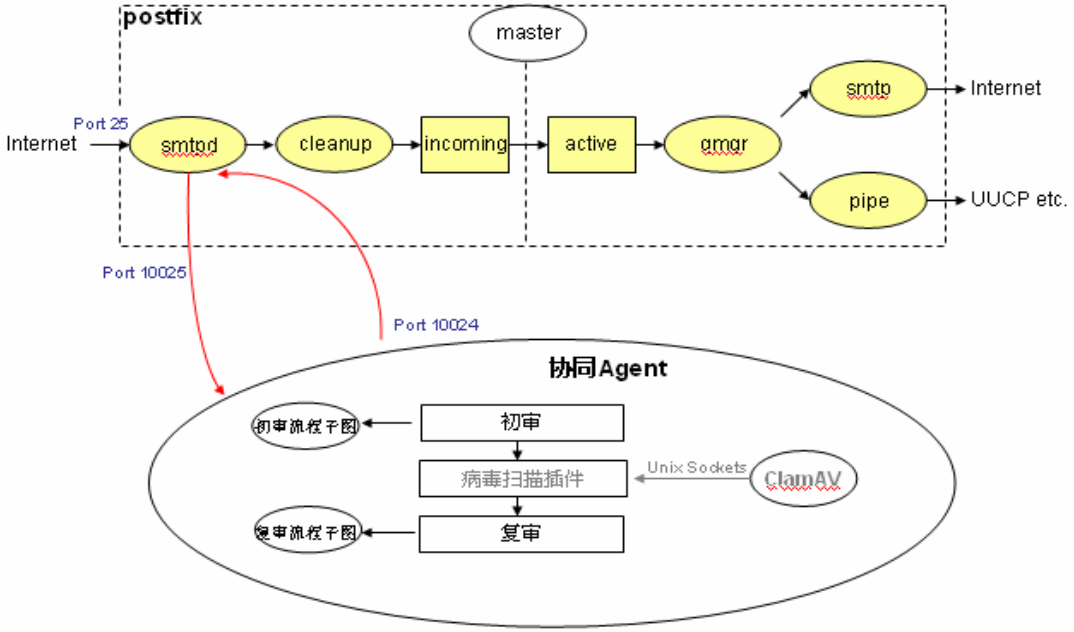
  最大熵模型

  - ✓具有融合不同层次特征的能力
  - ✓Boosting学习框架与最大熵模型相结合来弱化“训练语料和测试语料服从相同分布”的假设，因为在实际应用中，相对于需要检验的邮件，训练语料总是不充分的
  - ✓取得了优于贝叶斯分类器的性能

系统实现

➢协同监控Agent子系统

主要解决“初审－复审－学习反馈”三者之间的协同，协调垃圾邮件过滤、内容分析识别和举报等功能，达到低误报率和低漏报率，实现快速响应

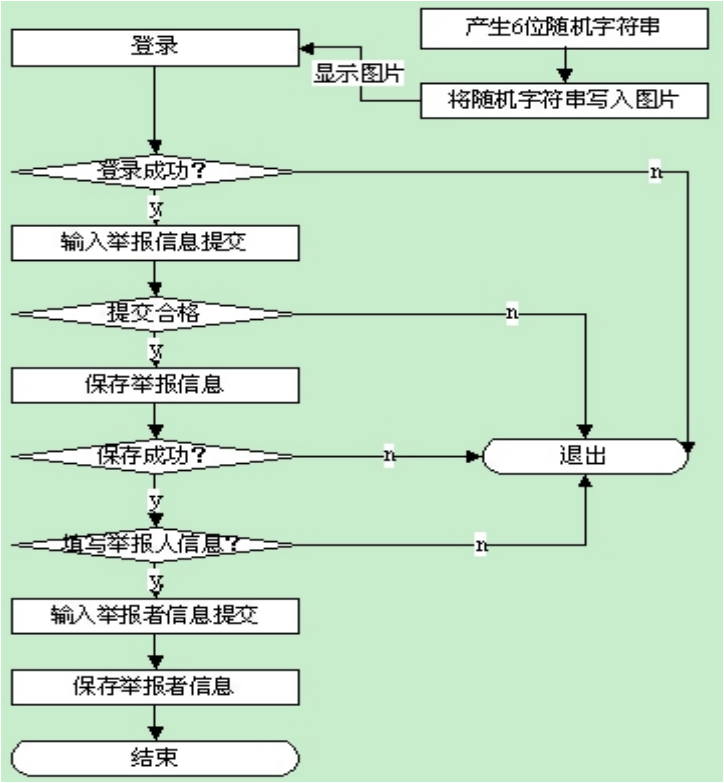


- **MTA采用Postfix**
- **病毒扫描模块集成ClamAV**

系统实现

➢用户举报接口

用户举报是一种获得垃圾邮件样本的好方式，流程如下：



系统实现

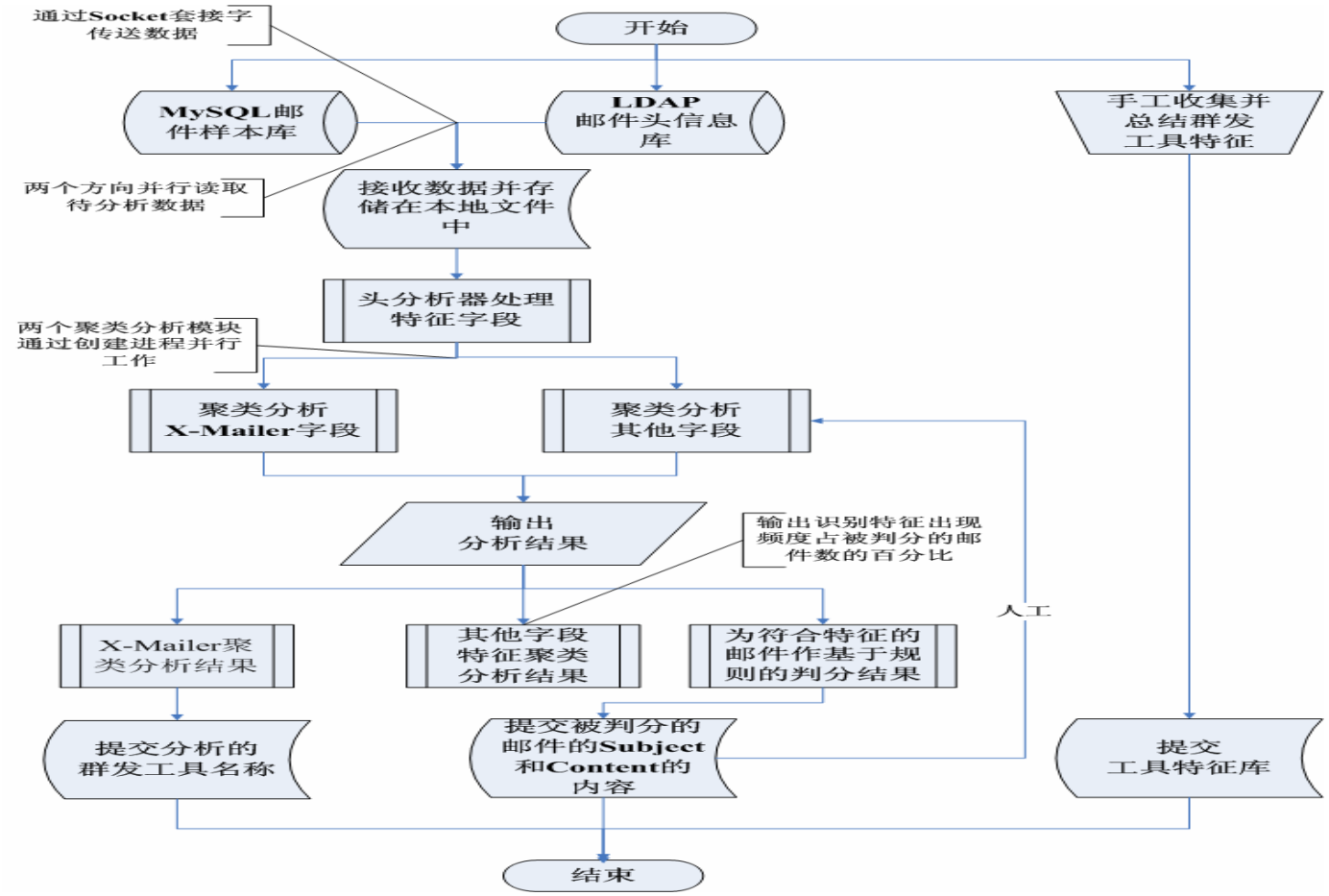
- 主流群发工具特征库建立子系统

群发工具泛滥，比如使用谷歌（**Google**）或百度以关键字“邮件群发软件”或者“邮件群发工具”搜索，可以找到数千种这类软件。如果愿意付费，则可得到的垃圾邮件群发工具更多。

立足发现垃圾邮件携带的群发工具特征，通过归纳，建立主流群发工具特征库。

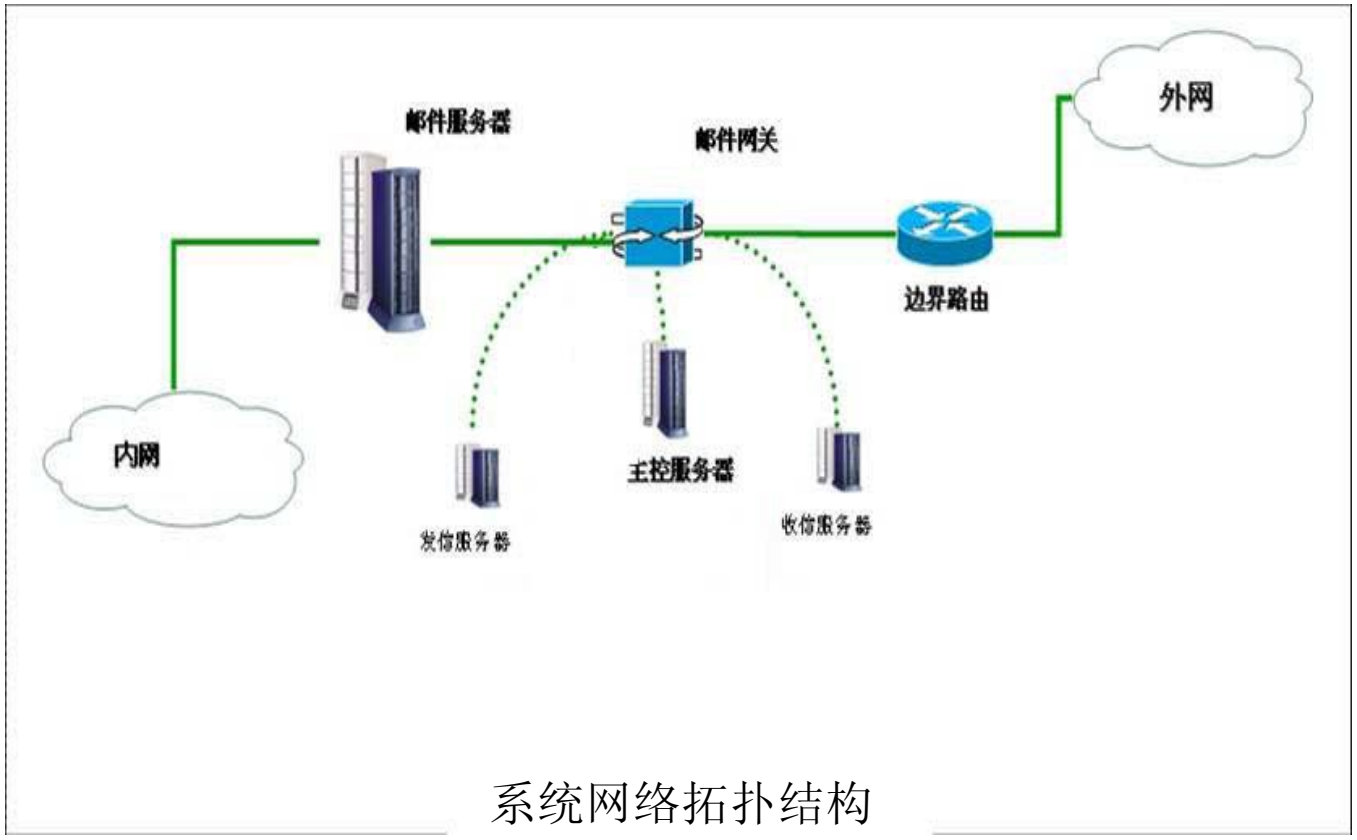
系统实现

- 主流群发工具特征库建立子系统



系统实现

- 垃圾邮件综合举报系统



系统网络拓扑结构

试用情况

目前系统已经在东北大学网络中心和中国教育和科研计算机网CERNET东北地区网络中心试用。结果表明：该系统处理速度快，可以有效拦截垃圾邮件，平均处理邮件的速度为307Mb/秒（Xeon MP 3.0G *4 / 8G / SCSI Ultra320 / Raid 5)，漏报率低于5%，误报率低于2%，效果良好。

谢谢！