超星·期刊

第25卷第4期 华东交通大学学报 Vol. 25 No. 4
2008年8月 Journal of East China Jiaotong University Aug. ,2008

文章编号:1005-0523(2008)04-0025-04

P2P网络安全监控系统的设计与实现

刘立月,万仲保,柴亚辉

(华东交通大学 信息工程学院,江西 南昌 330013)

摘要:针对P2P技术带来新的网络安全问题,以国内某一广泛应用的P2P系统为对象,设计并实现了对P2P用户有效监控,对有害信息传播进行封堵过滤,对危害行为进行布控定位,保障了P2P系统健康运行.目前,该系统已经在实际中得到成功应用.

关 键 词:P2P;网络安全;封堵过滤;布控定位

中图分类号:TP393.08 文献标识码:A

当前基于P2P[1](Peer-to-Peer,即对等网络)技术的Internet应用领域越来越多,如BT、eMule、POCO、Vagaa等,由于采用多点共享和传输技术使网络资源传输速度大为提高,从而得到广泛应用.P2P在加强网络上人的交流、文件交换、服务共享、分布式计算等方面已经充分显示出了其强大的技术优势,同时也带来新的网络安全问题,如P2P信息共享与知识产权保护,新型网络病毒和有害信息传播等问题.为了提高网络监察部门对基于P2P技术条件下的信息共享和传播渠道的控制能力,防范各种危害社会稳定的信息在网上的大量传播,及时发现和打击各种网上危害行为,开展P2P监控系统建设势在必行.

针对国内目前用户最多、影响力最大的某一中文P2P软件,我们设计了P2P网络安全监控系统(以下简称监控系统).该系统能对基于P2P技术软件提供的应用服务进行有效监控,如有害信息的传播能及时发现、删除、过滤和封堵,对有害信息的提供者和可疑活动能够快速准确定位,为有效地打击网上违法活动提供技术支持.

1 系统方案设计

P2P系统的应用服务主要表现在文件共享、搜索、下载及聊天等方面,为了实现对网上有害信息的传播进行监控,监控系统应具备以下功能:共享的文件能够根据文件名和内容进行关键字和Hash(哈希)值查找,生成有害信息列表,建立有害信息资源库;能够发现有害信息后定位文件提供者的P2P号及IP地址等信息,对有害信息从源头进行封堵;能对共享文件的P2P用户进行管理,保留对上传下载文件的过程以及点对点的传递信息的日志,对被确定的嫌疑P2P用户进行实时监控和报警等功能.

为了实现对P2P系统应用服务的监控,我们需要在原有P2P系统的基础上架构P2P监控服务器及监控客户端,根据监控系统功能的需要,在不影响原有P2P系统的正常业务的前提下,对P2P用户与服务器端进行必要的修改,增加对P2P用户信息及其操作过程监控.系统主要由P2P用户,P2P业务服务器与P2P(WWW+FTP)服务器、P2P监控服务器、P2P监控客户组成,系统总体结构如图1所示.图中P2P用户通过P2P(WWW)服务器注册,获取P2P号与密码后,向P2P业务服务器登录,登录成功后,P2P用户可进行文件共享、搜索、下载、聊天及上下线等操作,同时需向P2P监控服务器发送操作过程记录数据,以便P2P监控客户并对其行为跟踪,对其传播有害信息进行封堵过滤,必要时可对其进行布控定位与报警.

收稿日期:2008-03-24

作者简介:刘立月(1970-),男,安徽安庆人,讲师,研究方向为网络工程、测控及嵌入式.

超星·期刊

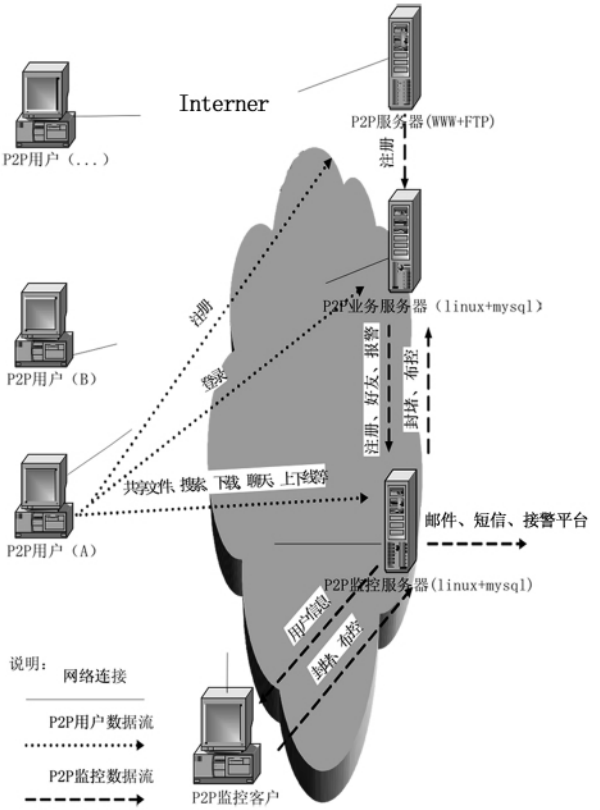

图 1 系统总体结构示意图

2 系统方案实现

2.1 系统功能组成

监控系统主要功能模块: 用户信息查询、封堵过滤与布控定位,功能结构如图 2 所示.

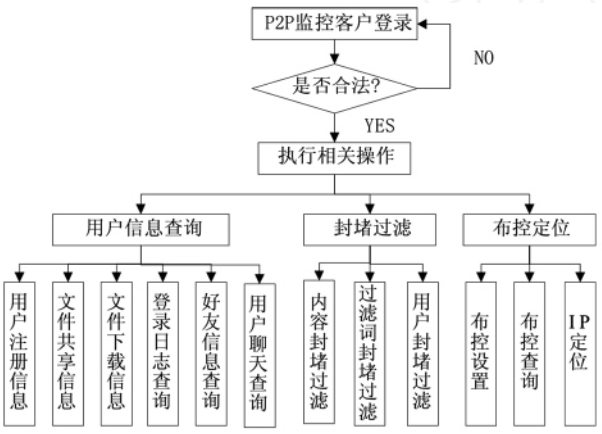

图 2 系统功能集成图

2.2 系统主要功能实现

2.2.1 用户信息查询

用户信息查询模块由用户注册信息、文件共享信息、文件下载信息、登录日志查询、好友信息查询和用户聊天查询 6 个子模块组成.

(1) 用户注册信息: 可根据 P2P 号、昵称要求精确查询用户注册信息(P2P 号、昵称、注册 IP、注册时间) ; 可根据注册用户 IP 地址查询用户注册源.

(2) 文件共享信息: 可根据 P2P 号、关键字或文件 Hash 值要求查询指定时间段共享文件信息; 并可查询提供共享文件最早共享者及其共享时间信息.

(3) 文件下载信息: 可根据 P2P 号、关键字或文件 Hash 值要求查询指定时间段文件下载信息; 并可跟踪下载源.

(4) 登录日志查询: 查询指定时间段用户登录日志信息.

(5) 好友信息查询: 查询指定用户的所有好友以及被加好友.

(6) 用户聊天查询: 查询指定时间段用户聊天消息.

2.2.2 封堵过滤

封堵过滤模块由内容封堵过滤、过滤词封堵过滤与用户封堵过滤 3 个子模块组成.

(1) 内容封堵过滤: 审核文件内容,计算非法文件 Hash 值,对非法文件内容库(含文件 Hash 值) 中所有文件进行自动侦查与封堵(一旦文件加入非法文件内容库,则 P2P 服务器对该文件下载进行自动封堵,P2P 客户无法下载此文件) ; 可增加或删除非法文件内容库类型或内容.

(2) 过滤词封堵过滤: 审核过滤词(即文件名中关键字) ,对文件名中含有此过滤词的文件进行自动侦查与封堵(一旦过滤词加入过滤词库,则 P2P 服务器对含有该库中过滤词的所有文件搜索进行自动封堵,P2P 客户无法搜索此文件) .

(3) 用户封堵过滤: 对指定用户的 P2P 号或 IP 进行封堵管理.

2.2.3 布控定位

布控定位模块由布控设置、布控查询、IP 定位 3 个子模块组成.

(1) 布控设置: 添加与删除布控对象报警设置(布控对象、布控案由、报警手机、报警邮箱、审核人) ; 一旦布控对象设置了报警,当布控对象上线时自动向指定对象报警.

(2) 布控查询: 可根据布控对象 P2P 号,查询布控对象历史报警信息及该布控对象在线状态; 可显示所有在线布控对象信息.

(3) IP 定位: IP 地址库的管理,主要涉及添加、删除与更新; 定位查询主要涉及具体 IP 地址或地区

超星·期刊

位置查询.

3　系统关键问题解决

3.1　数据库查询效率与实时性问题

在系统试运行阶段,P2P 用户共享文件信息每天都有 100 M 多条记录,随着时间增长,数据记录急剧上升,查询速度慢、效率低. 针对此问题,我们从 P2P 用户端与 P2P 监控客户端两方面采取措施,在 P2P 用户端,限制 P2P 用户共享文件上限,且共享文件采取增量发送; 在 P2P 监控客户端,采用多线程查询机制,提高查询效率.

P2P 用户在 P2P 服务器登录成功后,P2P 用户的行为数据,如用户登录或离去、共享文件、搜索下载文件、聊天等信息直接传到 P2P 监控服务器上,从而确保 P2P 监控客户能获取在线 P2P 用户实时数据,实现实时监控.

3.2　文件内容标记与封堵问题

对有危害嫌疑的行为,监控系统的封堵主要有四种形式: 文件内容封堵; 过滤词封堵; 用户 P2P 号与 IP 地址封堵,关键要解决文件内容唯一性标记与封堵策略问题.

SHA(Secure Hash Algorithm) [2,3] 安全 Hash 算法由 Ron Rivest 所设计,当输入长度小于 2^{64} bit 报文时,输出 160 bit 的字符串,该串可以被看作是原输入报文的报文摘要值(Message Digest) 或数字指纹(Digital Fingerprint) . 根据算法的复杂性理论知道,SHA 算法输出具有下列特征:

(1) 由一个给定的报文摘要不可能通过计算导出报文源(即不可逆性的) ;

(2) 要找到两条不同的信息使之产生相同的摘要在计算上是不可行的(即抗冲撞性) .

SHA1 是 SHA 的改进,是一种目前应用广泛的提取数字指纹的算法标准,已获美国标准与技术研究院的认证. 在此系统中,我们采用 SHA1 算法对文件进行加密,生成文件 Hash 值,作为文件存在唯一性标记,为文件内容封堵做好准备.

对于用户 P2P 号与 IP 地址封堵,我们采取的策略是: 当 P2P 用户登录时,与 IP 和 P2P 用户封堵库比较,若其 P2P 号或 IP 地址在库中,则不允许该用户登录,从而实现嫌疑 IP 和 P2P 封堵目的,这种策略对 P2P 用户登录时间有一定影响,但基本可以接受.

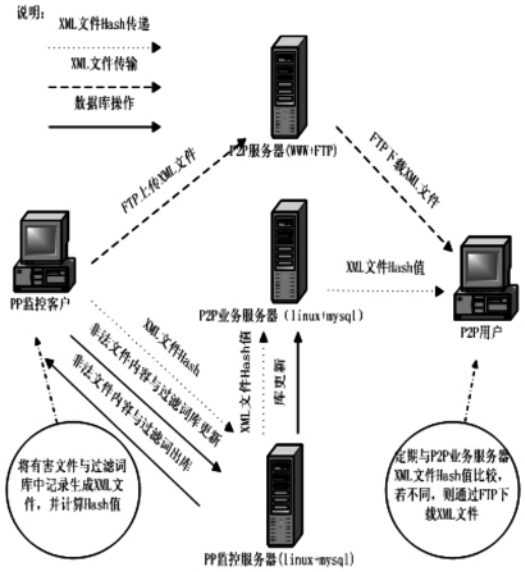

图 3　有害文件内容 Hash 与过滤词传输过程

对文件内容与过滤词封堵,开始设计时采取与上面相同策略. 在试运行阶段发现,大量用户频繁的对共享、搜索、下载操作,需要不断的访问数据库,造成数据库的访问成为瓶颈,严重影响 P2P 用户的运行. 针对此问题,我们将非法文件内容库与过滤词库下载到 P2P 用户端进行封堵过滤,如图 3 所示. 当 P2P 监控客户对非法文件内容库或过滤词库更新时,同时将库中记录以 XML 文件形式存储在本地,并利用 SHA1 算法计算相应 XML 文件 Hash 值; 然后将 XML 文件通过 FTP 上传到 P2P(FTP) 服务器,将文件 Hash 值递交到 P2P 监控服务器,再由 P2P 监控服务器递交到 P2P 业务服务器(P2P 监控客户不直接与 P2P 业务服务器联系) ; 接着由 P2P 业务服务器将文件 Hash 值写入服务器的全局变量中; P2P 用户端程序定期读取服务器的全局变量文件 Hash 值,若与本地的文件 Hash 值不一致,则从 FTP 服务器下载 XML 文件. 当 P2P 用户搜索文件时,若其输入串中含 XML 文件中的过滤词,则报告搜索失败; 当用户下载文件时,若下载文件的 Hash 值(文件共享时提供文件 Hash 值) 在 XML 文件中,则不允许用户下载,从而实现文件内容封堵与文件名封堵过滤.

3.3　报警处置问题

监控系统运行的主要目的是有效地管理 P2P 用户的信息共享行为,为建立一个健康的、有序的信息共享环境奠定基础,对于有危害嫌疑的信息共享行为,必须做出相应的处置. 为此,首先需要对有害信息进行确定,根据有害信息查询 P2P 共享用户历史,确定嫌疑 P2P 用户或嫌疑危害行为,然后进行

超星·期刊

布控,设置报警方式与报警内容,最后接警对象接警.

报警方式有 3 种: 向布控人所指定的对象发送电子邮件、手机短信、或接警中心互动. 对有危害嫌疑的行为,其报警内容主要有三种形式: 嫌疑 P2P 号上线报警; 共享非法文件报警; 下载非法文件报警. 报警处置过程如图 4 所示.

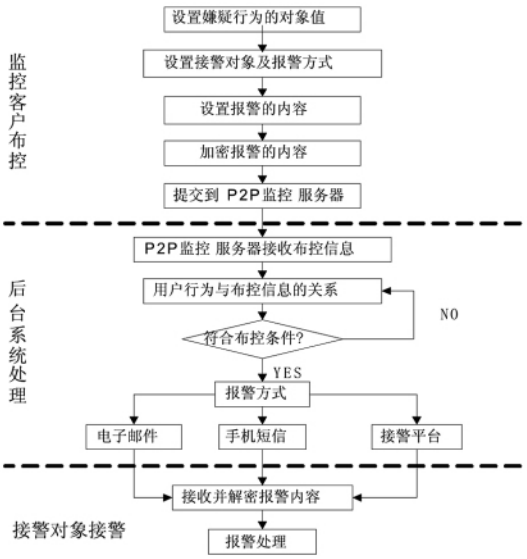

图 4 报警处置过程

3.4 监控日志及数据安全存储问题

为了保障系统数据库的安全和高性能,监控系统前端配置了一台专用的前置应用服务器,从 P2P 网络提交的各种监控信息经过防火墙检查后将数据发送给前置应用服务器,而不是直接提交给数据库服务器,数据库服务器只接收前置应用服务器和授权终端的数据查询和储存请求,这样能进一步保障数据库服务器的安全. 此外,因为系统本身所具有的特殊性,还需要使用数据库备份和容错系统为数据安全提供进一步强有力的保障.

3.4.1 备份工作实现自动化

采用软件与硬件结合的备份方式,配备 SAN 高性能存储阵列[4],数据库服务器上的应用程序可以设置为数据库定时自动转储到 SAN 存储阵列. 还可以根据需要进行数据库恢复或数据库重建.

3.4.2 系统提供的管理功能

利用备份软件可以根据用户的需要制订灵活的管理策略,如可以设置在每周一至周四进行增量或差量备份,以减少备份时间和磁带使用量,每周五进行全备份. 同时备份服务器对备份客户、备份介质、备份策略等进行了有效地管理,一旦出现系统错误会通过电话、传呼、E - mail 等方式通知系统管理员,保证备份工作有效、可靠地运行.

3.4.3 智能灾难恢复功能

备份的目的是为了在故障时进行恢复,系统配有灾难恢复选件,可实现系统的快速恢复,大大减少从发现故障到完全恢复系统的时间.

4 系统运行情况

目前该监控系统已通过相关部门验收,运行良好,但也存在一些有待改进的问题:

(1) IP 定位的精确性问题: IP 定位的精确性完全依赖于 IP 库的数据准确,如何保证 IP 库的数据的更新与准确,需要 IP 服务商或网络运行商的支持; 对于内网用户或外网 IP 动态更新用户,其 IP 定位的精确性仍存在某种不确定性.

(2) 用户 IP 封堵问题: 对于内网用户(实际是其网关,一般为外网 IP) 或外网 IP 动态更新用户,对其 IP 的封堵,可能会对其他用户的使用产生影响. 如对某内网用户 IP 的封堵实际是对其网关(即外网 IP) 的封堵,结果会造成相同网关的其他用户无法登录.

(3) 用户 P2P 号封堵问题: 目前 P2P 号产品用户大多是免费注册,注册信息与其真实身份无太大联系,当嫌疑用户某个 P2P 被封堵了,用户可以再申请一个. 因此如何确保用户 P2P 号封堵有效性,需要对其注册身份进行真实性确认,这需要 P2P 产品运行商的支持.

参考文献:

[1] 蔡 俊,黄兆华,等. 基于 C/S 架构的 eMule 监控系统的设计与实现[J]. 华东交通大学学报,2007,4:93 - 96.

[2] 孙楠楠,韩银河,等. 一种基于循环展开结构的 SHA - 1 算法实现[J]. 信息技术,2007,3:34 - 36.

[3] 张振权,罗新民,等. 数字签名算法 MD5 和 SHA - 1 的比较及其 AVR 优化实现[J]; 网络安全技术与应用,2005,7:65 - 68.

[4] 康春荣,苏武荣. 数据安全项目案例: 存储与备份 SAN 与 NAS 容错与容灾[M]. 北京: 科学出版社. 2004. 135 - 149.

超星·期刊

Design and Implementation of P2P Network Security Monitoring System

LIU Li – yue，WAN Zhong – bao，CHAI Ya – hui

(School of Information Engineering，East China Jiaotong University，Nanchang 330013，China)

Abstract: Aiming at new network security problems brought by P2P technology，with the object of P2P system applied in domestic field，this paper designs and implements a network security monitoring system，which can monitor P2P user actions，jam and filtrate harmful information，control and orientate harmful actions. This system has been applied to P2P security monitoring successfully.

Key words: P2P; network security; jamming and filtrating; controlling and orientating

---

简讯 2:

喜　报
我校两名教授获第五届江西省高等学校教学名师荣誉称号

根据江西省教育厅《关于表彰第五届江西省高等学校教学名师奖获奖者的决定》(赣教高字【2008】43 号) 文件精神，我校基础学院刘二根教授、土木学院郑明新教授喜获第五届江西省高等学校教学名师荣誉称号. 希望我校广大教师以教学名师为模范，重视基础课的教学任务，注重教学改革与实践，不断提高教学水平和人才培养质量，把我校的教学质量和水平提高到一个新的高度.

(来源: 教务处)