(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年2月24日(24.02.2005)

PCT

(10) 国际公布号:
WO 2005/018152 A1

(51) 国际分类号 : H04L 12/26

(21) 国际申请号: PCT/CN2004/000486

(22) 国际申请日: 2004年5月14日(14.05.2004)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
03140202.X 2003年8月15日(15.08.2003) CN

(71) 申请人(对除美国以外的所有指定国): 中兴通讯股份有限公司(ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 傅凯(FU, Kai) [CN/CN]; 袁知贵(YUAN, Zhigui) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司 (BEIJING LEADER PATENT AGENCY CO., LTD.) 中国北京市海淀区花园路13号道隆商务会馆 Beijing 100088 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

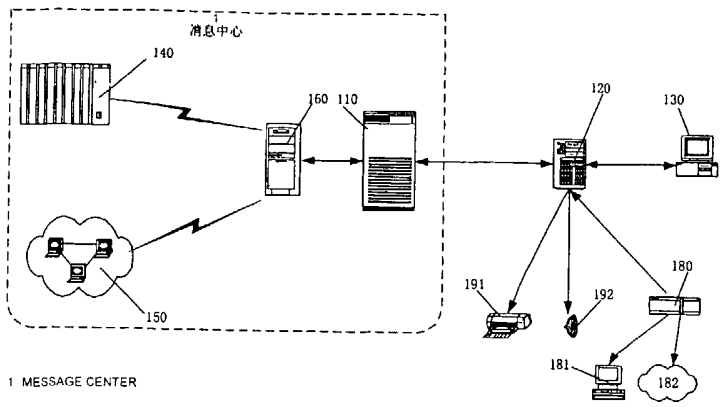
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A SYSTEM AND METHOD OF INTELLIGENTLY MONITORING THE MESSAGE CENTERS

(54) 发明名称: 一种智能监控消息中心的系统和方法



(57) **Abstract:** This invention provides a system of intelligently monitoring message centers, includes a service processor, a monitor server and a monitor administration station, the service processor sends message which need to be monitored, the monitor server processes the message which need to be monitored depends on monitor parameters sent by the monitor administration station, output the user blacklist table produced to the service processor, service processor controls the processing of the message service depends on the user blacklist; this invention can automatically capture the doubtful objects, and set them as blacklist users, the service processor cutoffs all message sources from this user; at the same time delete the users which meet unrestricted condition from the blacklist table, and immediately stop restricting the corresponding message sources . Furthermore, this invention can modify monitor configure paramcters in time, and can be applied to the monitoring of all kinds of short message, multimedia message centers and mail center etc.

[见续页]

WO 2005/018152 A1

(57) 摘要

本发明提出一种智能监控消息中心的系统，包括业务处理机、监控服务器和监控管理台，业务处理机向监控服务器发送待监控消息，监控服务器根据监控管理台输出的监控配置参数处理待监控消息，生成用户黑名单输出到业务处理机，业务处理机根据用户黑名单控制信息业务的处理；本发明可根据监控配置参数自动截获可疑对象，并将其设定为黑名单用户，由业务处理机即时封闭对应该用户的消息源；同时自动将满足解禁条件的用户从黑名单表中删除，即时解禁对应的消息源。此外本发明可实时修改监控配置参数，并可应用于对各类短消息中心、多媒体消息中心和邮件中心等的监控。

一种智能监控消息中心的系统和方法

技术领域

本发明涉及监控通信系统中消息中心的技术领域，尤其涉及对 CDMA 通信系统、GSM 通信系统以及无线市话系统等的短消息中心、多媒体消息中心、邮件中心等进行智能监控的系统和方法。

背景技术

目前，通信系统中消息中心的功能日臻强大，已从短消息中心发展到多媒体消息中心和邮件中心等。使用消息中心的用户数量日益增长，利用消息中心进行宣传的方式层出不穷，各通信网络之间也逐步实现了互连互通，在通信网络间流动的消息量成几何级数增长。在这种市场环境下，不可避免地会出现大量的垃圾消息和恶意消息等。短时间内的垃圾消息攻击可使得通信网络的传输量迅猛增长，容易造成网络瘫痪；而频繁的垃圾消息和恶意消息等也会让使用消息中心的用户不胜其烦；而具有反动性质的、谣言性质的消息更会造成极坏的社会影响。

因此需对各类消息中心进行监控，包括消息流量和消息内容等。目前对消息中心进行监控的方法主要是：消息中心的管理者通过人工方式在消息中心的业务处理机上设置黑名单号码，进行指定过滤，但该方法既不方便又不准确，无法根据网络情况实时修改黑名单号码，时效性很差，无法应付目前消息中心的大消息流量，因此急需有一种可自动监控消息中心的系统和方法，但目前尚未发现有公开的相近的技术方案。

发明内容

本发明所要解决的技术问题在于提供一种智能监控消息中心的系统和方

法，可实现对各类消息中心进行自动监控，并根据通信网络的实际情况修改监控配置参数，避免垃圾消息和恶意消息的传播，保证消息中心的稳定。

本发明所述智能监控消息中心的系统，包括业务处理机、监控服务器和至少一个监控管理台，其中所述业务处理机用于处理收到的信息业务，向所述监控服务器发送待监控消息，并根据所述监控服务器返回的用户黑名单控制信息业务的处理；所述监控服务器，用于根据所述监控管理台输出的监控配置参数处理待监控消息，生成用户黑名单输出到所述业务处理机；所述监控管理台，用于生成监控配置参数，并发送给所述监控服务器。

在所述业务处理机和所述监控服务器中，均设置有一个消息数据库，用于存放消息监控过程中产生的记录，包括被禁发的消息本身以及监控结果。

所述业务处理机还设置有用户黑名单表，用于存放用户黑名单，根据该用户黑名单对用户进行黑名单监控。

所述监控服务器还设置有消息流量监控表，用于存放监控用户的信息。

本发明所述智能监控消息中心的方法，包括以下步骤：业务处理机将待监控消息发送给监控服务器；监控服务器根据监控管理台发送的监控配置参数对待监控消息进行实时监控；监控服务器对满足加禁条件的用户生成用户黑名单，发送给业务处理机；业务处理机根据用户黑名单控制信息业务的处理。

所述监控服务器对待监控消息进行实时监控，包括对消息内容的监控和对消息流量的监控。

本发明所述系统和方法，可根据监控配置参数自动截获可疑对象，并将其设定为黑名单用户，由业务处理机即时封闭对应该用户的消息源；同时也可自动将满足解禁条件的用户从黑名单表中删除，从而即时解禁对应的消息源。本发明可实时修改监控配置参数，监控操作即时生效。另外，本发明可以根据监

控配置进行多渠道的告警；各有权限的远程终端可即时监视监控状态，并可随时查询分析其历史日志。本发明可应用于对各类短消息中心、多媒体消息中心和邮件中心等的监控。

附图说明

图 1 是本发明智能监控消息中心的系统的网络结构示意图；

图 2 是本发明智能监控消息中心的系统的数据流示意图；

图 3 是本发明方法中对用户消息流量进行监控的流程示意图；

图 4 是本发明方法中对消息内容进行监控的流程示意图；

图 5 是本发明方法中业务处理机根据用户黑名单控制信息业务处理的流程示意图。

具体实施方式

下面结合附图和实施例，对本发明的技术方案做进一步的详细介绍。

各类通信系统的消息中心，一般包括业务处理机 110、业务接入服务器 160、交换中心 140 和 WWW 服务器 150，其中业务接入服务器 160 主要用于从交换中心 140、WWW 服务器 150 接入信息业务；业务处理机 110 则用于处理各类信息业务，如短消息、多媒体短消息、多媒体邮件等，并通过业务接入服务器 16 与交换中心 140、WWW 服务器 150 进行各类消息、邮件的交互和收发。

如图 1 所示，本发明提供的智能监控消息中心的系统，包括：位于消息中心的业务处理机 110，监控服务器 120 和监控管理台 130。其中业务处理机 110 与监控服务器 120 进行通讯，业务处理机 110 除了完成一般的信息业务处理之外，还将待监控消息发送给监控服务器 120；监控服务器 120 分别与业务处理机 110、监控管理台 130 连接并实时通信，用于根据监控配置参数对待监控消息进行实时监控，并生成用户黑名单和黑名单解禁名单，发送给业务处理机

110；监控管理台 130 用于设置监控配置参数，并将其发送给监控服务器 120。此外，监控服务器 120 也可将监控结果发给监控管理台 130。

业务处理机 110 发送给监控服务器 120 的待监控消息可以是接收到的信息本身；或者是信息的简化，如话单等。

在监控服务器 120 上还设置有至少一个远端接口 180，为远程用户提供接口。监控服务器 120 通过该远端接口 180 可以连接有远程终端 181 或浏览器 182，为远程用户提供监控配置参数的配置界面或监视界面等。此外，所述监控服务器 120 还可以与日志打印装置 191 或声光告警装置 192 相连，将监控结果输出显示。

在业务处理机 110 和监控服务器 120 中都设置了一个消息数据库，用于存放消息监控过程中产生的记录，包括被禁发的消息本身以及监控结果。上述消息数据库可位于业务处理机 110 和监控服务器 120 的内存中，是采用 HASH 方式组织的数据表。具体实现为：在内存中申请一块结构数组区，数组的每一个成员结构对应一条记录；将成员结构中的某个成员作为索引，如号码。根据索引定位到对应的记录采用 HASH 算法完成，可以高速定位数据。解决 HASH 冲突的方法采用链地址法，即用空闲队列管理内存表的使用情况：每当在内存表中插入一条记录，就从空闲队列头取走一个单元；每当删除一条记录，就将对应的单元置于空闲队列尾。这样，对内存表的操作可以像操作物理数据库一样方便，同时又因为在内存中则更加实时高效。

监控配置参数是用于指导监控服务器 120 进行监控的信息，包括监控方式的配置参数、监控结果处理的参数、黑名单用户解禁条件、超级用户、监控关键字等，其中监控方式是指监控服务器 120 应监控的待监控消息的信息，如消息流量监控、消息内容监控等；超级用户是指不进行消息监控的用户。具体地，

消息流量监控的配置参数包括监控时间、监控计数值、阈值等；消息内容监控的配置参数包括监控关键字；监控结果处理的参数包括“生成用户黑名单”、“监控结果反馈”、“声光报警”、“日志打印”、“通知管理员”等。

监控管理台 130 生成监控配置参数后，发送给监控服务器 120。监控配置参数是存放在监控服务器 120 内存中的全局结构变量，监控服务器 120 根据具体的监控配置参数，对待监控的消息进行实时监控。监控服务器 120 接收到监控管理台 130 的监控配置参数后，即时修改内存中的监控配置参数项，监控服务器 120 遂按照新的监控配置参数进行监控。同时监控服务器 120 将新的配置参数写入监控配置文件中防止配置参数丢失，也可供监控管理台 130 查证。

监控服务器 120 按照监控配置参数对待监控消息进行监控，可以是监控消息的流量和/或消息的内容。在监控服务器 120 中设置了用于存放监控用户的信息的消息流量监控表。消息流量监控表是在内存中采用结构数组区的内存表，如 HASH 方式，同时为防止记录数大于内存表的容量规模，还可进一步采用 LRU 算法确保表的安全和表中记录的实效性。

监控服务器 120 根据监控结果，对满足加禁条件的用户生成用户黑名单，发送给业务处理机 110，由业务处理机 110 根据此黑名单控制信息业务的处理，过滤黑名单用户。为此，在业务处理机 110 中设置了用户黑名单表，用于存放用户黑名单。黑名单表也可以是在内存中采用结构数组区构成的内存表，并且进一步采用 LRU 算法确保表的安全和表中记录的实效性。

本发明所述智能监控消息中心的方法，包括：业务处理机 110 将待监控消息发送给监控服务器 120；监控服务器 120 根据监控管理台 130 发送的监控配置参数对待监控消息进行实时监控；监控服务器 120 根据监控结果，自动筛选出满足加禁条件的用户并生成用户黑名单，发送给业务处理机 110；业务处理

机 110 根据用户黑名单，控制信息业务的处理，封闭黑名单用户的消息源。

在上述过程中，监控配置参数是由管理员通过图形化的配置界面在所述监控管理台 130 上配置的。监控服务器 120 还可以将监控结果发送给监控管理台 130 或其他有权限的远程终端或用户，同时还可以进行全方位告警，包括声光告警等。此外，监控服务器 120 还可以自动生成黑名单解禁名单，发送给业务处理机 110，由业务处理机 110 将解禁黑名单用户从用户黑名单表中删除，从而对该用户解禁。

在本发明所述方法中，消息中心与监控系统之间的数据流向如图 2 所示，其中数据流 A 为业务处理机 110 收到的待处理信息；数据 B 是业务处理机处理后的信息；数据 C 是业务处理机 110 发往监控服务器 120 的待监控消息，待监控消息可以是业务处理机 110 收到的信息本身，也可以是上述信息的简化，如话单等；数据流 D 是监控服务器 120 发往业务处理机 110 的用户黑名单或黑名单解禁名单；数据流 1、2、3 分别是由监控管理台 130 或其他远程用户发往监控服务器 120 的监控配置参数；数据流 4、5、6、7、8、9 则是监控服务器 120 将监控结果发给监控管理台 130 及其它各类终端的消息，供告警、浏览、跟踪分析用。

本发明方法从数据流的角度，具体为：业务处理机 110 收到待处理的信息或邮件即数据流 A 后进行处理，发往后续处理服务器进行正常处理（数据流 B），同时也向监控服务器 120 发送待监控消息即数据流 C 进行监控，发往监控服务器 120 的数据流 C 可以只带监控所需基本信息。监控服务器 120 按照各监控管理台 130 发来的监控配置参数即数据流 1、2、3，对待监控消息进行实时监控，并将监控结果即数据流 4、5、6、7、8、9 发往各监控管理台 130 或分析终端或告警装置或打印装置等。监控服务器 120 将监控得到的用户黑名单数据，即数

据流 D 即时发往业务处理机 110，存放在用户黑名单表中，从而对该用户的信息业务实现封闭。监控服务器 120 同时根据监控管理台 130 配置的解禁条件，定时检查用户黑名单表，筛选出满足解禁条件的黑名单用户，生成黑名单解禁名单，发送给业务处理机 110，由业务处理机 110 将解禁名单中的黑名单用户删除，对这些用户的信息业务解禁。

对待监控消息的监控包括消息流量的监控和消息内容的监控。

消息流量的监控是指监控信息用户在设置的单位时间内发送信息的数量是否超过设置的阈值，如果超过，则生成用户黑名单；然后由监控服务器 120 将用户黑名单发到业务处理机 110 或者输出到告警装置或者进行其他的监控结果处理。

为实现对消息流量的监控，在监控服务器 120 中设置了消息流量监控表，用于存放监控用户的信息，至少包括用户的号码、本次监控时间和本次监控的计数值。消息流量监控表采用了内存数据库的形式。

如图 3 所示，监控服务器 120 进行消息流量监控的具体步骤包括：首先监控服务器 120 收到业务处理机 110 发来的待监控消息（步骤 301），监控服务器 120 检查该待监控消息的用户是否已在消息流量监控表中存在（步骤 302）。

如果该用户不在消息流量监控表中，则监控服务器 120 将该用户的信息记录在消息流量监控表中，其中记录监控的计数值为 1，记录当前时间为监控起始时间（步骤 303）。然后监控服务器 120 检查该用户的计数值是否超过设置的监控计数阈值（步骤 306），如果计数值没有超过监控计数阈值，则表明该用户的消息流量没有超过预设阈值，结束此次监控。如果计数值超过监控计数阈值，则表明该用户的信息流量已超过预设阈值，监控服务器 120 对该监控结果进行处理（步骤 307），可以是：生成该用户的黑名单，发送给业务处理机

110，或者向监控管理台 130 反馈监控结果，或者进行声光告警等或者上述三种处理都进行。然后监控服务器 120 重置该用户的记录，计数值恢复为 0（步骤 308），结束此次监控。

如果该用户已记录在消息流量监控表中，则监控服务器 120 检查该用户的本次监控时间是否到达设置的监控时间间隔（步骤 304），如果超过监控时间间隔，则监控服务器 120 重置该用户的记录，计数值恢复为 0（步骤 308），结束此次监控。如果没有超过监控时间间隔，则监控服务器 120 检查该用户的记录是否刚被重置（步骤 305），如果是，则将该用户的计数值设置为 1，设置当前时间为监控的起始时间，然后执行步骤 306；如果不是刚被重置，则将该用户的计数值加 1，然后执行步骤 306。

对消息内容的监控是指对短消息的内容、多媒体短消息的内容以及多媒体邮件的主题等按照监控管理台 130 配置的监控关键字进行监控。

对消息内容的监控流程如图 4 所示，首先监控服务器 120 收到业务处理机 110 发来的待监控消息（步骤 401），然后检查收到的待监控消息的内容中是否包含设置的监控关键字（步骤 402）。如果含有，则监控服务器 120 对该监控结果进行处理（步骤 403），可以是：生成用户黑名单发送给业务处理机 110，或者进行声光告警，或者将监控结果反馈给监控管理台 130，或者上述三种处理都进行。如果不含有监控关键字，则结束此次监控（步骤 404）。

如果监控管理台 130 设置了超级用户，则在对待监控消息进行监控前，先检查待监控消息用户是否是超级用户，如果是，则对待监控消息不进行监控处理；如果不是，再进行后续的监控处理。

此外，在监控服务器 120 生成用户黑名单之前，还包括：判断监测到的可疑用户是否满足监控管理台 130 设置的黑名单生成条件（如单位时间内被检测

为可疑用户的频度是否达到规定的阈值），将满足黑名单生成条件的可疑用户确定为黑名单用户。

业务处理机 110 收到监控服务器 120 发来的用户黑名单后，存放在用户黑名单表中，该表可以采用内存数据库形式的内存表。业务处理机 110 根据用户黑名单表对黑名单用户进行过滤处理，拦截用户黑名单表中的用户的消息，只对合法用户的消息进行处理。另外，监控服务器 120 根据监控管理台 130 配置的解禁条件，定期检查用户黑名单表，挑选出满足解禁条件的黑名单用户，生成黑名单解禁名单，发送给业务处理机 110。

业务处理机 110 收到黑名单解禁名单后，从用户黑名单表中删除解禁名单中的用户，对其信息业务解禁。

图 5 给出了业务处理机根据用户黑名单控制信息业务处理的过程。首先业务处理机 110 接收到待处理的信息（步骤 501），然后检查该信息用户是否记录在用户黑名单表中（步骤 502）。如果已在用户黑名单表中记录，则业务处理机 110 中止该信息业务的处理，并可根据系统的配置确定是否需保存被截掉的信息（步骤 503）。如果该信息用户不是黑名单用户，则业务处理机 110 对该信息业务进行正常的处理（步骤 504）。

需要指出的是，本发明系统和方法中采用的监控方式并不仅限于上述的消息流量和消息内容的监控，对其他监控方式可以参考上述两类监控方式，而且本发明并未限定必须同时使用对上述两种参数的监控。

最后所应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，其均应涵盖在本发明的权利要求范围当中。

权利要求书

1、 一种智能监控消息中心的系统，其特征在于，包括业务处理机、监控服务器和至少一个监控管理台；其中

所述业务处理机，用于处理收到的信息业务，向所述监控服务器发送待监控消息，并根据所述监控服务器返回的用户黑名单控制信息业务的处理；

所述监控服务器，用于根据所述监控管理台输出的监控配置参数处理待监控消息，生成用户黑名单输出到所述业务处理机；

所述监控管理台，用于生成监控配置参数，并发送给所述监控服务器。

2、 根据权利要求 1 所述的智能监控消息中心的系统，其特征在于，在所述业务处理机和所述监控服务器中，均设置有一个消息数据库，用于存放消息监控过程中产生的记录。

3、 根据权利要求 2 所述的智能监控消息中心的系统，其特征在于，所述记录至少包括被禁发的消息本身及其监控结果。

4、 根据权利要求 1 所述的智能监控消息中心的系统，其特征在于，所述业务处理机设置有至少一个用户黑名单表，用于存放用户黑名单，根据该用户黑名单对用户进行黑名单监控。

5、 根据权利要求 1 所述的智能监控消息中心的系统，其特征在于，所述监控服务器设置有至少一个消息流量监控表，用于存放监控用户的信息。

6、 根据权利要求 2 或 4 或 5 所述的智能监控消息中心的系统，其特征在于，所述消息数据库、所述用户黑名单表和所述消息流量监控表均为在内存中由结构数组区构成的内存表。

7、 根据权利要求 6 所述的智能监控消息中心的系统，其特征在于，所述消息数据库采用 HASH 算法构成内存表。

8、 根据权利要求 7 所述的智能监控消息中心的系统，其特征在于，所述内存表通过空闲队列管理，当记录存入内存表时，从空闲队列头取走单元，当删除记录时将释放的单元置于空闲队列的队尾。

9、 根据权利要求 6 所述的智能监控消息中心的系统，其特征在于，所述消息数据库、所述用户黑名单表和所述消息流量监控表采用 LRU 算法控制记录数。

10、 根据权利要求 1 所述的智能监控消息中心的系统，其特征在于，所述监控配置参数至少包括：监控方式的配置参数、监控结果处理的参数、黑名单用户解禁条件、超级用户和监控关键字，其中监控方式是指监控服务器应监控的待监控消息的信息；超级用户是指不进行消息监控的用户。

11、 根据权利要求 1 所述的智能监控消息中心的系统，其特征在于，所述监控服务器还包括至少一个远端接口，为远程用户提供接入接口。

12、 根据权利要求 11 所述的智能监控消息中心的系统，其特征在于，所述监控服务器还可以与打印装置或声光告警装置相连，输出监控结果。

13、 一种智能监控消息中心的方法，其特征在于，包括以下步骤：业务处理机将待监控消息发送给监控服务器；监控服务器根据监控管理台发送的监控配置参数对待监控消息进行实时监控；监控服务器对满足加禁条件的用户生成用户黑名单，发送给业务处理机；业务处理机根据用户黑名单控制信息业务的处理。

14、 根据权利要求 13 所述的智能监控消息中心的方法，其特征在于，所述监控服务器对待监控消息进行实时监控，包括对消息内容的监控和/或对消息流量的监控。

15、 根据权利要求 13 所述的智能监控消息中心的方法，其特征在于，所

述方法还包括监控服务器定时检查用户黑名单表，查看黑名单用户是否满足解禁条件，如果满足，则将满足条件的黑名单用户生成黑名单解禁名单，发送给业务处理机；业务处理机收到黑名单解禁名单后，删除用户黑名单表中可以解禁的黑名单用户。

16、 根据权利要求 14 所述的智能监控消息中心的方法，其特征在于，如果监控管理台配置了超级用户参数，则在对待监控消息进行监控前，先检查待监控消息用户是否是超级用户，如果是，则对待监控消息不进行监控处理；如果不是，再进行后续的监控处理。

17、 根据权利要求 13 所述的智能监控消息中心的方法，其特征在于，在监控服务器 120 生成用户黑名单之前，还包括：判断监测到的可疑用户是否满足监控管理台 130 设置的黑名单生成条件，将满足黑名单生成条件的可疑用户确定为黑名单用户。

18、 根据权利要求 13 至 17 任一所述的智能监控消息中心的方法，其特征在于，所述方法还包括：监控服务器在发送用户黑名单的同时，将监控结果发给监控管理台或者进行声光告警处理或者打印输出或者发送给有查看监控结果权限的远端用户。

19、 根据权利要求 14 或 16 所述的智能监控消息中心的方法，其特征在于，所述对消息的内容进行监控具体是：监控服务器检查待监控消息的内容中是否含有监控关键字，如果有，则该消息的发送用户成为可疑用户，生成该待监控消息的用户黑名单，发送给业务处理机，结束该条消息的内容监控；如果待监控消息不含有监控关键字，则结束此次监控。

20、 根据权利要求 14 或 16 所述的智能监控消息中心的方法，其特征在于，所述对消息流量的监控具体是：

步骤 1）监控服务器检查待监控消息的用户是否已记录在消息流量监控表中；如果该用户已记录在消息流量监控表中，则转至步骤 2)；如果该用户没有记录在消息流量监控表中，则转至步骤 4)；

步骤 2）检查该用户的监控时间是否到达监控时间间隔，如果到达，则将消息流量监控表中该用户的记录重置，计数值重置为 0；结束此次监控；

步骤 3）如果该用户的监控时间未达到监控时间间隔，则判断该用户是否刚被重置，如果是，则将该用户的计数值置为 1，记录当前时间为监控起始时间，转至步骤 5)；如果该用户不是刚被重置，则将该用户的计数值加 1；转至步骤 5）

步骤 4）将该用户的信息记录在消息流量监控表中，并记录监控的计数值为 1，记录当前时间为监控起始时间；

步骤 5）监控服务器检查该用户的计数值是否超过监控计数阈值，如果计数值超过监控计数阈值，则对该用户生成用户黑名单，发送到业务处理机，结束此次监控；如果计数值未超过监控计数阈值，则结束此次监控。

21、 根据权利要求 13 至 17 任一所述的智能监控消息中心的方法，其特征在于，所述业务处理机控制信息业务的处理的步骤包括：业务处理机收到监控服务器发来的用户黑名单后，将用户黑名单存放在用户黑名单表中；业务处理机接收用户发送的待处理信息后，检查该用户是否属于用户黑名单表中的用户，如果属于，则中止该信息业务的处理；如果不属于，则正常处理该信息业务。

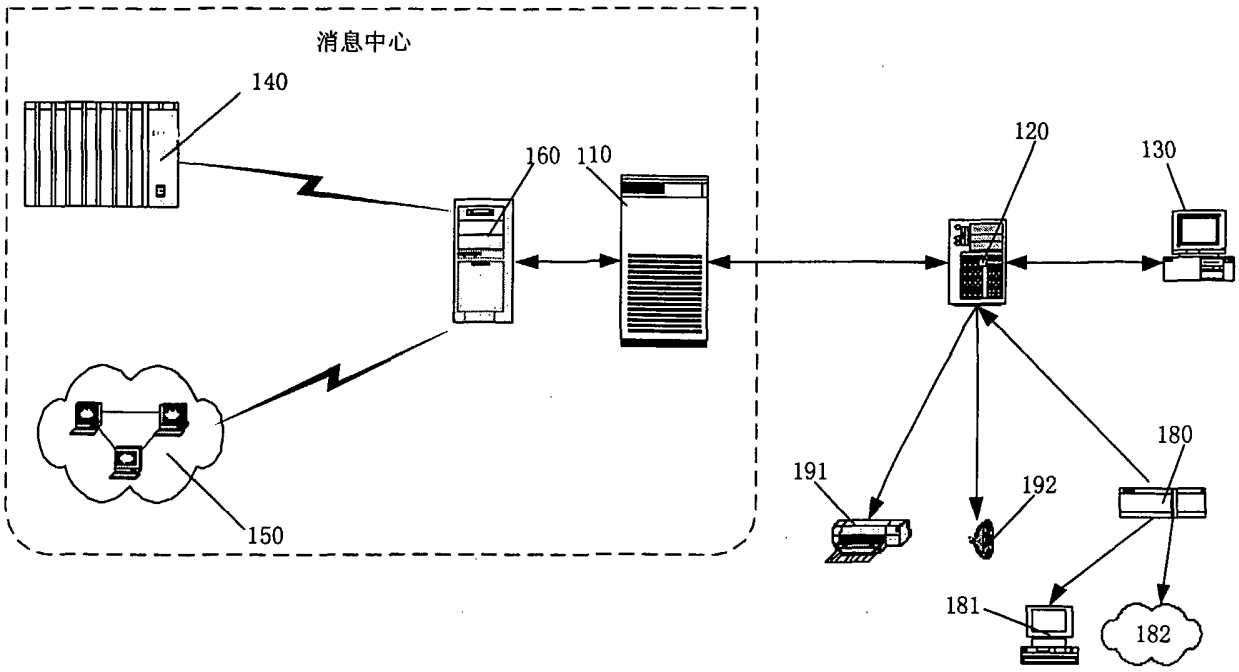

消息中心
140
160
110
120
130
150
180
191
192
181
182

图 1

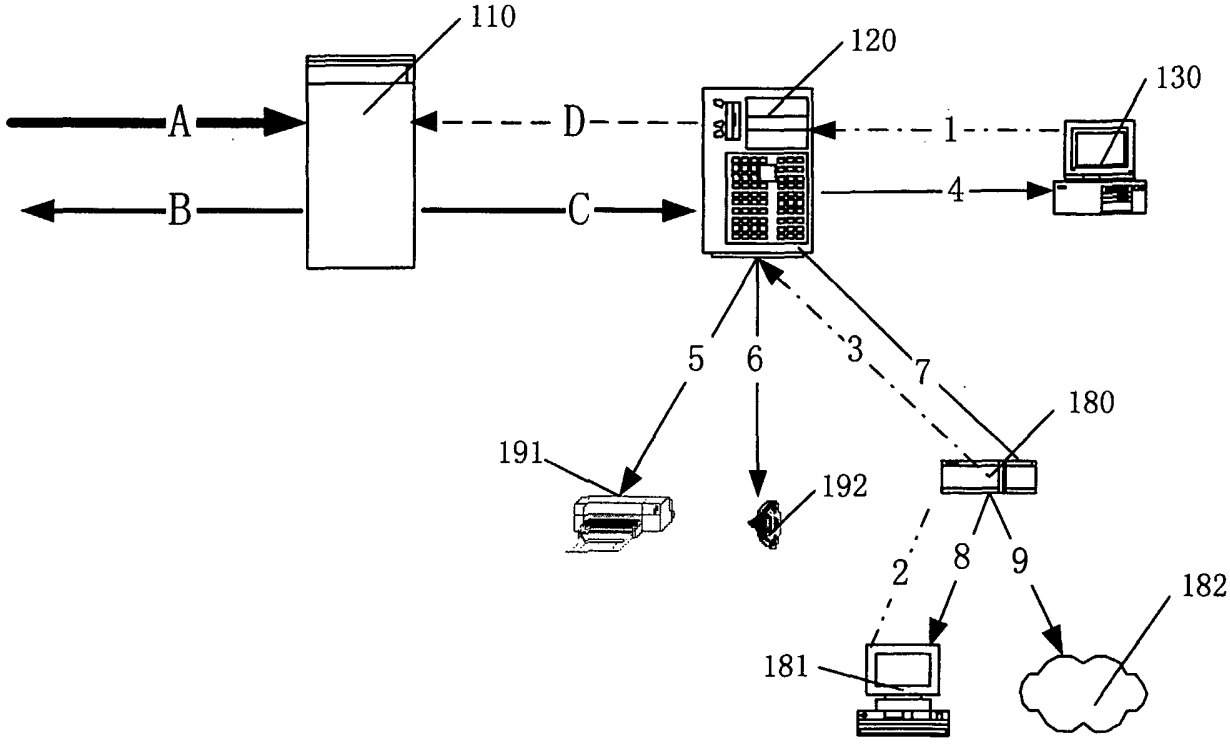

110
120
130
A
B
C
D
1
4
5
6
3
7
180
191
192
2
8
9
182
181

图 2

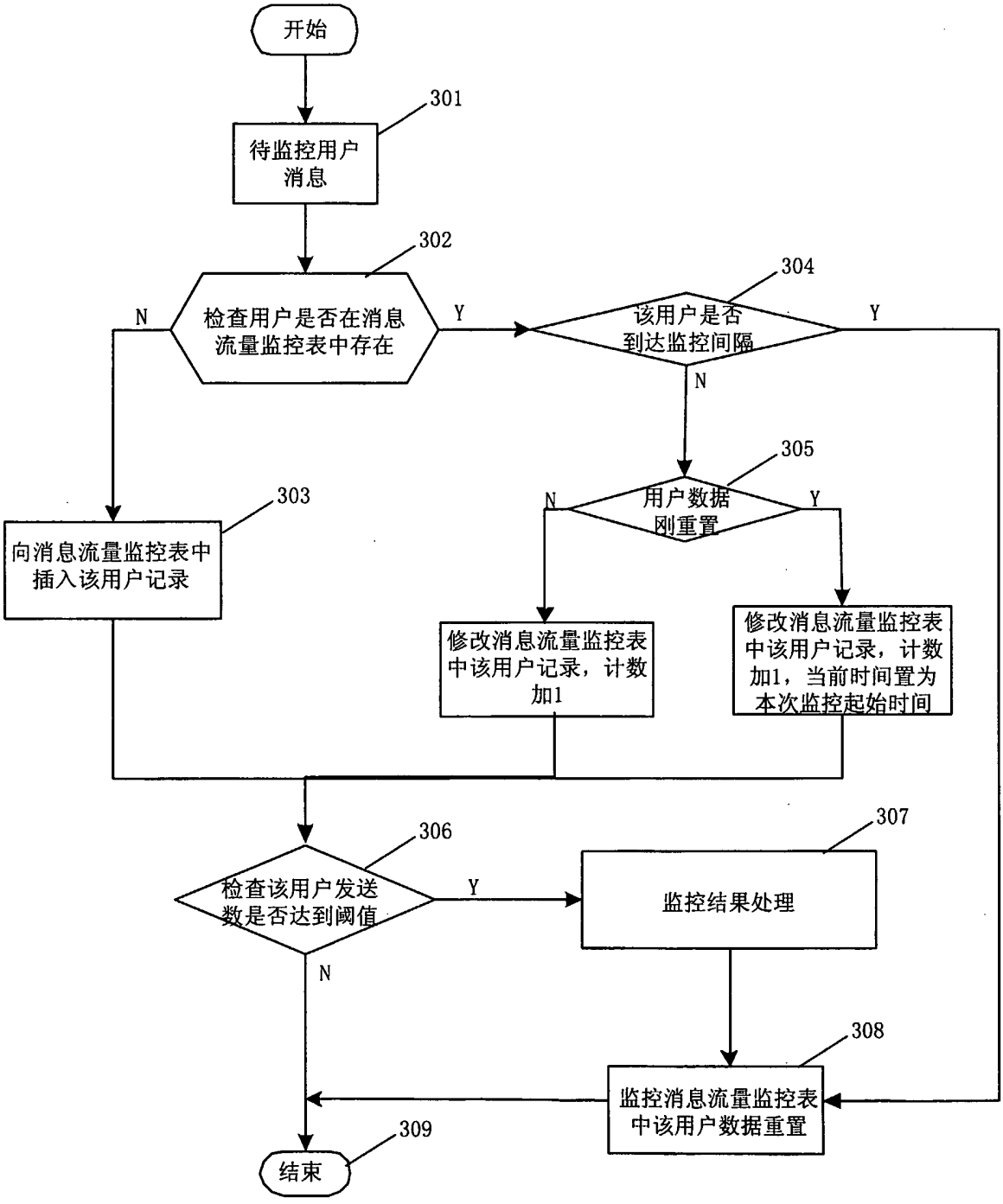

开始
301
待监控用户消息
302
检查用户是否在消息流量监控表中存在
N
Y
304
该用户是否到达监控间隔
Y
N
305
用户数据刚重置
N
Y
303
向消息流量监控表中插入该用户记录
修改消息流量监控表中该用户记录，计数加1
修改消息流量监控表中该用户记录，计数加1，当前时间置为本次监控起始时间
306
检查该用户发送数是否达到阈值
Y
307
监控结果处理
N
308
监控消息流量监控表中该用户数据重置
309
结束

图 3

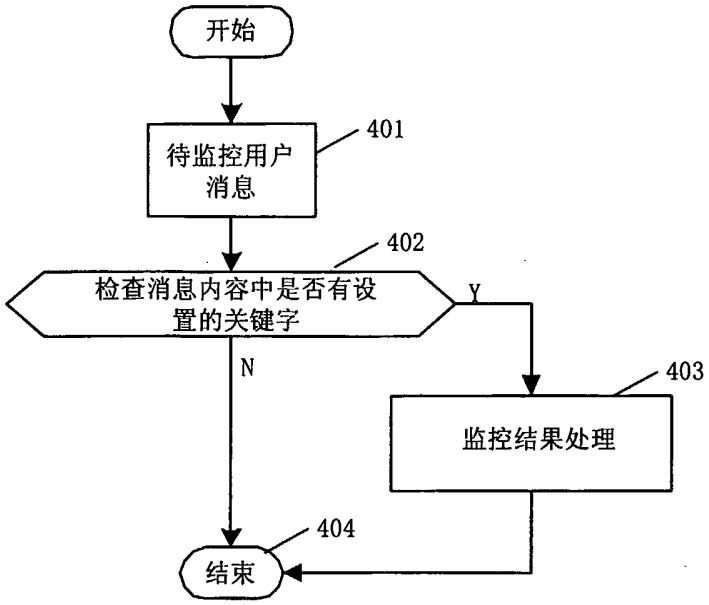

开始
待监控用户消息
401
检查消息内容中是否有设置的关键字
402
Y
N
监控结果处理
403
结束
404

图 4

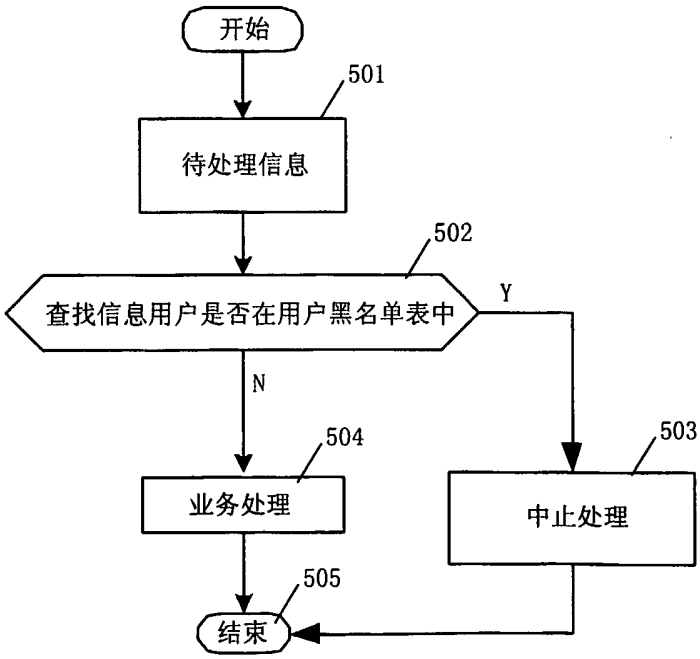

开始
待处理信息
501
查找信息用户是否在用户黑名单表中
502
Y
N
业务处理
504
中止处理
503
结束
505

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/000486

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]: H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: H04L12 H04L12/24 H04L12/28 G06F17/00 H04M3/22 H04Q7/34 H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT,CNKI:（邮件 + 短消息 +短信息 +信息） 过滤 智能

(MAIL OR SHORT MASSAGE OR SHORT INFORMATION OR MASSAGE) AND FILTER AND INTELIGEN+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1426214A (SHANGHAI SECOND INSTITUTE OF ZTE CORPORATION) 25.Jun.2003 see abstact, page9-12,claims, figs	1-21
X	CN1422050A (SHANGHAI SECOND INSTITUTE OF ZTE CORPORATION) 04.Jun.2003 see abstact, page7-9,claims, figs	1-21
A	CN1350246A (SHANGHAI JIAOTONG UNIVERSITY) 22.May 2002 see the whole	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05.Aug.2004	19 · AUG 2004 (19 · 08 · 2004)
Name and mailing address of the ISA/ 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-01-62019451	Authorized officer SUN YUFANG Telephone No. 86-01-62084553

Form PCT/ISA /210 (second sheet) (January 2004)

TERNATIONAL SEARCH REPORT

Information patent family members

Search request No.
PCT/CN2004/000486

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN1426214A	25.Jun.2003	NONE	
CN1422050A	04.Jun.2003	NONE	
CN1350246A	22.May.2002	NONE	

国际检索报告

国际申请号
PCT/CN2004/000486

A. 主题的分类

IPC[7]: H04L12/26

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7]: H04L12 H04L12/24 H04L12/28 G06F17/00 H04M3/22 H04Q7/34 H04L12/66

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI, EPODOC, PAJ, CNPAT,中国期刊全文库：（邮件 + 短消息 +短信息 +信息） 过滤 智能

(MAIL OR SHORT MASSAGE OR SHORT INFORMATION OR MASSAGE) AND FILTER AND INTELIGEN+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN1426214A （深圳市中兴通讯股份有限公司上海第二研究所) 25.6 月 2003 摘要，说明书 9－12 页，权利要求，附图	1－21
X	CN1422050A （深圳市中兴通讯股份有限公司上海第二研究所) 4 .6 月 2003 摘要，说明书 7－9 页，权利要求，附图	1－21
A	CN1350246A （上海交通大学） 22.5 月 2002 全文	1－21

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
5.8 月 2004（5.08.2004）	19 · AUG 2004 (19 · 08 · 2004)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 孙玉芳 电话号码：(86-10)62084553

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2004/000486

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1426214A	25.6 月 2003	无	
CN1422050A	04.6 月 2003	无	
CN1350246A	22.05 月 2002	无	