(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
2012 年 5 月 24 日 (24.05.2012)

WIPO | PCT

(10) 国际公布号
WO 2012/065381 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01)

(21) 国际申请号: PCT/CN2011/071428

(22) 国际申请日: 2011 年 3 月 1 日 (01.03.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010546405.7 2010 年 11 月 15 日 (15.11.2010) CN

(71) 申请人 (对除美国外的所有指定国): **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): **马震宇 (MA, Zhenyu)** [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)。 **王冲 (WANG, Chong)** [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: **北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区知春路 113 号 0717 室, Beijing 100086 (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: METHOD AND APPARATUS FOR PREVENTING MALICIOUS SOFTWARES FROM TRANSMITTING DATA

(54) **发明名称** : 一种防止恶意软件发送数据的方法及装置

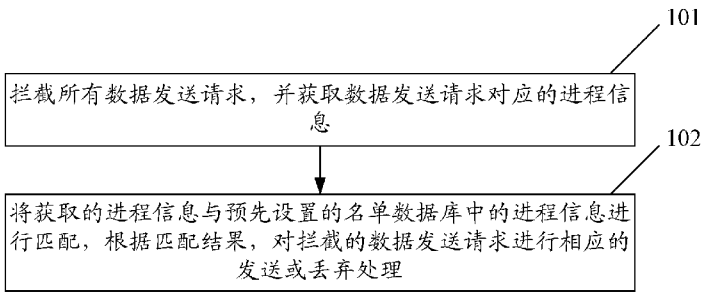

图 1 /Fig.1

101 INTERCEPTING ALL DATA TRANSMISSION REQUESTS AND OBTAINING THE PROCESS INFORMATION CORRESPONDING TO THE DATA TRANSMISSION REQUESTS

102 MATCHING THE OBTAINED PROCESS INFORMATION WITH THE PROCESS INFORMATION PRESET IN A LIST DATABASE, AND CORRESPONDINGLY TRANSMITTING OR DISCARDING THE INTERCEPTED DATA TRANSMISSION REQUESTS ACCORDING TO THE MATCHED RESULT

(57) **Abstract**: A method for preventing malicious softwares from transmitting data is disclosed. The method includes: intercepting a data transmission request and obtaining the process information corresponding to the data transmission request; matching the obtained process information with the process information preset in a list database; according to the matched result, correspondingly transmitting or discarding the intercepted data transmission request. An apparatus for preventing malicious softwares from transmitting data is also disclosed. With the method and the apparatus in the present invention, the malicious softwares are prevented from transmitting data in the background, and thereby the expense loss is reduced and the user experience is satisfied.

(57) **摘要**: 本发明公开了一种防止恶意软件发送数据的方法，包括：拦截数据发送请求，并获取数据发送请求对应的进程信息；将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。本发明同时公开了一种防止恶意软件发送数据的装置，采用本发明的方法及装置，能阻止恶意软件在后台发送数据，进而能减少费用损失，满足用户体验。

WO 2012/065381 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种防止恶意软件发送数据的方法及装置

技术领域

本发明涉及移动终端技术，特别是指一种防止恶意软件发送数据的方法及装置。

背景技术

随着科学技术的发展，智能移动终端比如智能手机的使用人群逐渐平民化，智能手机已不再是商务人士的专爱，其用户群规模迅猛扩展。智能手机的一个显著特点是能灵活安装应用软件，随着用户群的不断扩大，这一特点也引起了一些恶意软件的关注，以前只在计算机上才出现的恶意软件已经开始在智能手机上出现。由于手机牵涉到话费问题，即：存在经济利益，所以智能手机上的恶意软件与计算机上的相比危害更大。一般，恶意软件会捆绑在某些比较热门的正常软件中，利用正常软件诱导用户去下载，当用户下载了那些捆绑了恶意软件的软件包并安装后，恶意软件就会在后台偷偷运行。

恶意软件的行为有很多种类型，其中一种就是在后台发送短信，比如：利用智能手机提供的短信接口，订购一些消费业务等，或者，不停地外发短信，这些操作都会造成用户话费的大量损失，而且还不易被发觉，只有事后到运营商处仔细查询清单才能发现一些端倪，经济损失一般比较难以挽回。因此，如何及时发现、最好能提前防范这类恶意软件的行为，进而防止话费损失，就显得尤其重要，已成为用户的迫切需求。

目前，还没有防止恶意软件发送短信的技术方案。

发明内容

有鉴于此，本发明的主要目的在于提供一种防止恶意软件发送数据的方法及装置，能阻止恶意软件在后台发送数据，减少费用损失。

为达到上述目的，本发明的技术方案是这样实现的：

本发明提供了一种防止恶意软件发送数据的方法，该方法包括：

拦截数据发送请求，并获取所述数据发送请求对应的进程信息；

将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。

上述方案中，所述根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理，为：

当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求；

当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求；

当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户。

上述方案中，该方法进一步包括：

将包含数据内容及所述获取的进程信息的相关信息展示给用户后，根据收到的用户的命令作出相应的处理。

上述方案中，所述根据收到的用户的命令作出相应的处理，为：

收到的用户的命令为同意发送的命令时，则发送所述拦截的数据发送请求，并将所述获取的进程信息添加到白名单的进程信息中；

收到的用户的命令为不同意发送的命令时，则丢弃所述拦截的数据发送请求，并将所述获取的进程信息添加到黑名单的进程信息中。

上述方案中，该方法进一步包括：将发送记录保存到记录数据库中。

上述方案中，该方法进一步包括：将已丢弃的数据发送请求保存到记录数据库中。

本发明还提供了一种防止恶意软件发送数据的装置，该装置包括：数据拦截模块、名单判断模块、及处理模块；其中，

数据拦截模块，用于拦截数据发送请求，获取所述数据发送请求对应的进程信息，并将获取的进程信息发送给名单判断模块；

名单判断模块，用于收到数据拦截模块发送的获取的进程信息后，将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，并将匹配结果发送给处理模块；

处理模块，用于收到名单判断模块发送的匹配结果后，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。

上述方案中，所述处理模块，具体用于：当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求，当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求，当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户。

上述方案中，所述处理模块，还用于收到用户的同意发送的命令后，发送所述拦截的数据发送请求，并将所述获取的进程信息添加到白名单的进程信息中；或者，收到用户的不同意发送的命令后，丢弃所述拦截的数据发送请求，并将所述获取的进程信息添加到黑名单的进程信息中。

上述方案中，该装置进一步包括：记录模块，用于收到处理模块发送的发送记录后，将发送记录保存到记录数据库中，或者，收到处理模块发送的已丢弃的数据发送请求后，将已丢弃的数据发送请求也保存到记录数据库中，并标记成被拦截；

所述处理模块，还用于发送所述拦截的数据发送请求后，将发送记录

发送给记录模块，或者，丢弃所述拦截的数据发送请求后，将已丢弃的数据发送请求发送给记录模块。

本发明提供的防止恶意软件发送数据的方案，拦截数据发送请求，并获取对应的进程信息，将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理，如此，能阻止恶意软件在后台发送数据，进而能减少费用损失，满足用户体验。

另外，可以将发送记录保存到记录数据库中，如此，能方便用户查询发送历史记录，进一步提升用户体验。

附图说明

图 1 为本发明防止恶意软件发送数据的方法流程示意图；

图 2 为实施例防止恶意软件发送短信的方法流程示意图；

图 3 为本发明防止恶意软件发送数据的装置结构示意图。

具体实施方式

下面结合附图及具体实施例对本发明再作进一步详细的说明。

本发明防止恶意软件发送数据的方法，如图 1 所示，包括以下步骤：

步骤 101：拦截数据发送请求，并获取数据发送请求对应的进程信息；

这里，所述数据发送请求可以是短信发送请求、彩信发送请求或其它数据包发送请求；

如果拦截的数据发送请求为短信发送请求时，拦截的短信发送请求包含短信内容、短信的目的地址、及发送时间等；

在实际使用时，需要将智能移动终端的数据拦截模块设置于智能移动终端的短信接口的下面，拦截每个短信发送请求；

应用软件如恶意软件或正常的短信软件发送短信时，需要调用智能移

动终端如智能手机的短信接口，此时，在智能手机的进程中会保存有调用手机的短信接口的进程信息，因此，在拦截短信发送请求后，可以从智能手机的进程中保存的进程信息中获得短信发送请求对应的进程信息;

如果拦截的数据发送请求为彩信发送请求时，拦截的彩信发送请求包含彩信内容、彩信的目的地址、及发送时间等;

如果拦截的数据发送请求为数据包发送请求时，拦截的数据发送请求包含数据包的目的网址、数据包内容、及发送时间等;

同样的，在发送彩信或数据包时，需要调用智能手机相应的接口，此时，在智能手机的进程中会保存有调用手机相应的接口的进程信息，因此，在拦截数据发送请求后，可以从智能手机的进程中保存的进程信息中获得数据发送请求对应的进程信息。

步骤 102: 将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理;

这里，所述名单数据库包含白名单的进程信息及黑名单的进程信息;其中，白名单的进程信息为：能向外发送数据的进程信息，黑名单的进程信息为：不能向外发送数据的进程信息;

所述根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理，具体为:

当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求，当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求，当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户;

其中，所述数据内容可以是短信内容、彩信内容或数据包内容；所述

相关信息还可以包括短信或彩信的目的地址、发送时间或数据包的目的网址、发送时间等；将包含数据内容及所述获取的进程信息的相关信息展示给用户后，根据收到的用户的命令作出相应的处理，具体地，如果收到的用户的命令为同意发送的命令时，则发送所述拦截的数据发送请求，如果收到的用户的命令为不同意发送的命令时，则丢弃所述拦截的数据发送请求；此时，进一步地，可以将所述获取的进程信息添加到名单数据库中，具体地，如果发送了所述数据发送请求，则将所述获取的进程信息添加到白名单的进程信息中，如果丢弃了所述拦截的数据发送请求，则将所述获取的进程信息添加到黑名单的进程信息中；

当所述拦截的数据发送请求为短信发送请求时，所述发送所述拦截的数据发送请求，具体为：

调用移动终端的短信模块，由短信模块发送短信；其中，短信模块发送短信的具体处理流程与现有的处理流程完全相同；

在发送所述拦截的数据发送请求后，该方法可以进一步包括：

将发送记录保存到记录数据库中，以便事后用户可以查询发送历史记录；进一步地，还可以将已丢弃的数据发送请求也保存到记录数据库中，并标记成被拦截；所述发送历史记录包含数据内容、对应的进程信息等内容。

下面以短信为例，本实施例防止恶意软件发送短信的方法，如图 2 所示，包括以下步骤：

步骤 201：拦截短信发送请求，并获取短信发送请求对应的进程信息；

这里，所述拦截的短信发送请求包含短信内容、短信的目的地址、及发送时间等。

步骤 202：判断获取的进程信息与预先设置的名单数据库中的进程信息是否能匹配，所述名单数据库包含白名单的进程信息及黑名单的进程信息，

如果所述获取的进程信息与白名单中的进程信息相匹配时，则执行步骤203a，如果所述获取的进程信息与黑名单中的进程信息相匹配时，则执行步骤 203b，如果所述获取的进程信息与名单数据库中的进程信息不能匹配时，则执行步骤 204。

步骤 203a：发送所述拦截的短信发送请求，之后执行步骤 207。

步骤 203b：丢弃所述拦截的短信发送请求，之后执行步骤 208。

步骤 204：将包含短信内容及所述获取的进程信息的相关信息展示给用户，并在收到同意发送的命令后，执行步骤 205，在收到不同意发送的命令后，执行步骤 206；

这里，所述相关信息包括：短信内容、所述获取的进程信息、短信的目的地址、发送时间等。

步骤 205：发送所述拦截的短信发送请求，并将所述获取的进程信息添加到白名单的进程信息中，之后执行步骤 207。

步骤 206：丢弃所述拦截的短信发送请求，并将所述获取的进程信息添加到黑名单的进程信息中，之后执行步骤 208。

步骤 207：将发送记录保存到记录数据库中，之后执行步骤 209。

步骤 208：将已丢弃的所述拦截的短信发送请求保存到记录数据库中，并标记成被拦截，之后执行步骤 209。

步骤 209：结束当前处理流程。

为实现上述方法，本发明还提供了一种防止恶意软件发送数据的装置，如图 3 所述，该装置包括：数据拦截模块 31、名单判断模块 32、及处理模块 33；其中，

数据拦截模块 31，用于拦截数据发送请求，获取数据发送请求对应的进程信息，并将获取的进程信息发送给名单判断模块 32；

名单判断模块 32，用于收到数据拦截模块 31 发送的获取的进程信息后，

将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，并将匹配结果发送给处理模块 33;

处理模块 33，用于收到名单判断模块 32 发送的匹配结果后，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。

其中，如果用于拦截短信时，数据拦截模块 31 设置于智能移动终端的短信接口的下面，拦截每个短信发送请求。

所述处理模块 33，具体用于:

当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求，当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求，当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户。

该装置还可以进一步包括: 记录模块，用于收到处理模块 33 发送的发送记录后，将发送记录保存到记录数据库中;

所述处理模块 33，还用于发送所述拦截的数据发送请求后，将发送记录发送给记录模块。

所述处理模块 33，还用于丢弃所述拦截的数据发送请求后，将已丢弃的数据发送请求发送给记录模块;

记录模块，还用于收到处理模块 33 发送的已丢弃的数据发送请求后，将已丢弃的数据发送请求也保存到记录数据库中，并标记成被拦截。

所述处理模块 33，还用于收到用户的同意发送的命令后，发送所述拦截的数据发送请求，并将所述获取的进程信息添加到白名单的进程信息中;收到用户的不同意发送的命令后，丢弃所述拦截的数据发送请求，并将所述获取的进程信息添加到黑名单的进程信息中。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保

护范围，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种防止恶意软件发送数据的方法，其特征在于，该方法包括:

拦截数据发送请求，并获取所述数据发送请求对应的进程信息;

将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。

2、根据权利要求 1 所述的方法，其特征在于，所述根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理，为:

当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求;

当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求;

当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户。

3、根据权利要求 2 所述的方法，其特征在于，该方法进一步包括:

将包含数据内容及所述获取的进程信息的相关信息展示给用户后，根据收到的用户的命令作出相应的处理。

4、根据权利要求 3 所述的方法，其特征在于，所述根据收到的用户的命令作出相应的处理，为:

收到的用户的命令为同意发送的命令时，则发送所述拦截的数据发送请求，并将所述获取的进程信息添加到白名单的进程信息中;

收到的用户的命令为不同意发送的命令时，则丢弃所述拦截的数据发送请求，并将所述获取的进程信息添加到黑名单的进程信息中。

5、根据权利要求 1 至 4 任一项所述的方法，其特征在于，该方法进一步包括:

将发送记录保存到记录数据库中。

6、根据权利要求 1 至 4 任一项所述的方法，其特征在于，该方法进一步包括:

将已丢弃的数据发送请求保存到记录数据库中。

7、一种防止恶意软件发送数据的装置，其特征在于，该装置包括：数据拦截模块、名单判断模块、及处理模块；其中，

数据拦截模块，用于拦截数据发送请求，获取所述数据发送请求对应的进程信息，并将获取的进程信息发送给名单判断模块;

名单判断模块，用于收到数据拦截模块发送的获取的进程信息后，将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，并将匹配结果发送给处理模块;

处理模块，用于收到名单判断模块发送的匹配结果后，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理。

8、根据权利要求 7 所述的装置，其特征在于，所述处理模块，具体用于:

当所述获取的进程信息与白名单中的进程信息相匹配时，则发送所述拦截的数据发送请求，当所述获取的进程信息与黑名单中的进程信息相匹配时，则丢弃所述拦截的数据发送请求，当所述获取的进程信息与名单数据库中的进程信息不能匹配时，将包含数据内容及所述获取的进程信息的相关信息展示给用户。

9、根据权利要求 8 所述的装置，其特征在于，所述处理模块，还用于收到用户的同意发送的命令后，发送所述拦截的数据发送请求，并将所述获取的进程信息添加到白名单的进程信息中；或者，收到用户的不同意发送的命令后，丢弃所述拦截的数据发送请求，并将所述获取的进程信息添加到黑名单的进程信息中。

10、根据权利要求 7 至 9 任一项所述的装置，其特征在于，该装置进

一步包括：记录模块，用于收到处理模块发送的发送记录后，将发送记录保存到记录数据库中，或者，收到处理模块发送的已丢弃的数据发送请求后，将已丢弃的数据发送请求也保存到记录数据库中，并标记成被拦截；

所述处理模块，还用于发送所述拦截的数据发送请求后，将发送记录发送给记录模块，或者，丢弃所述拦截的数据发送请求后，将已丢弃的数据发送请求发送给记录模块。

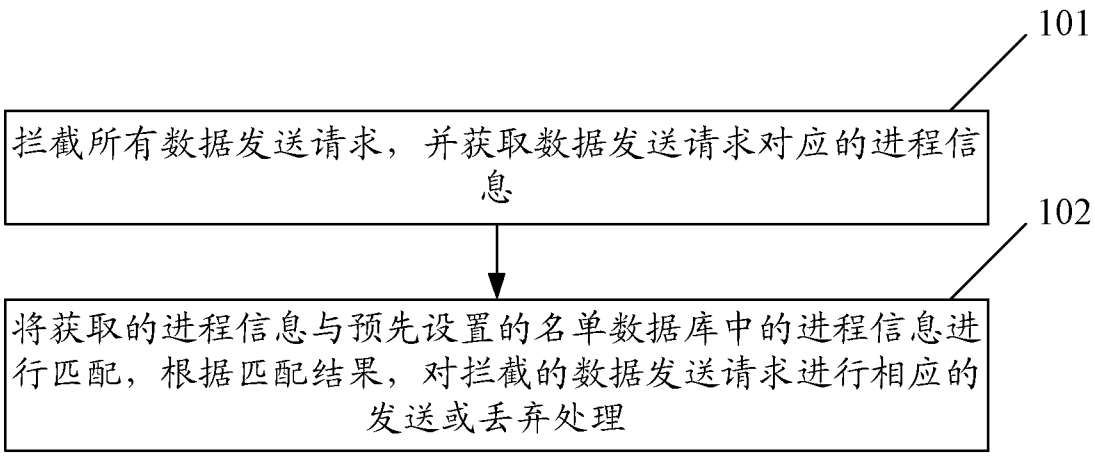
101
拦截所有数据发送请求，并获取数据发送请求对应的进程信息
102
将获取的进程信息与预先设置的名单数据库中的进程信息进行匹配，根据匹配结果，对拦截的数据发送请求进行相应的发送或丢弃处理

图 1

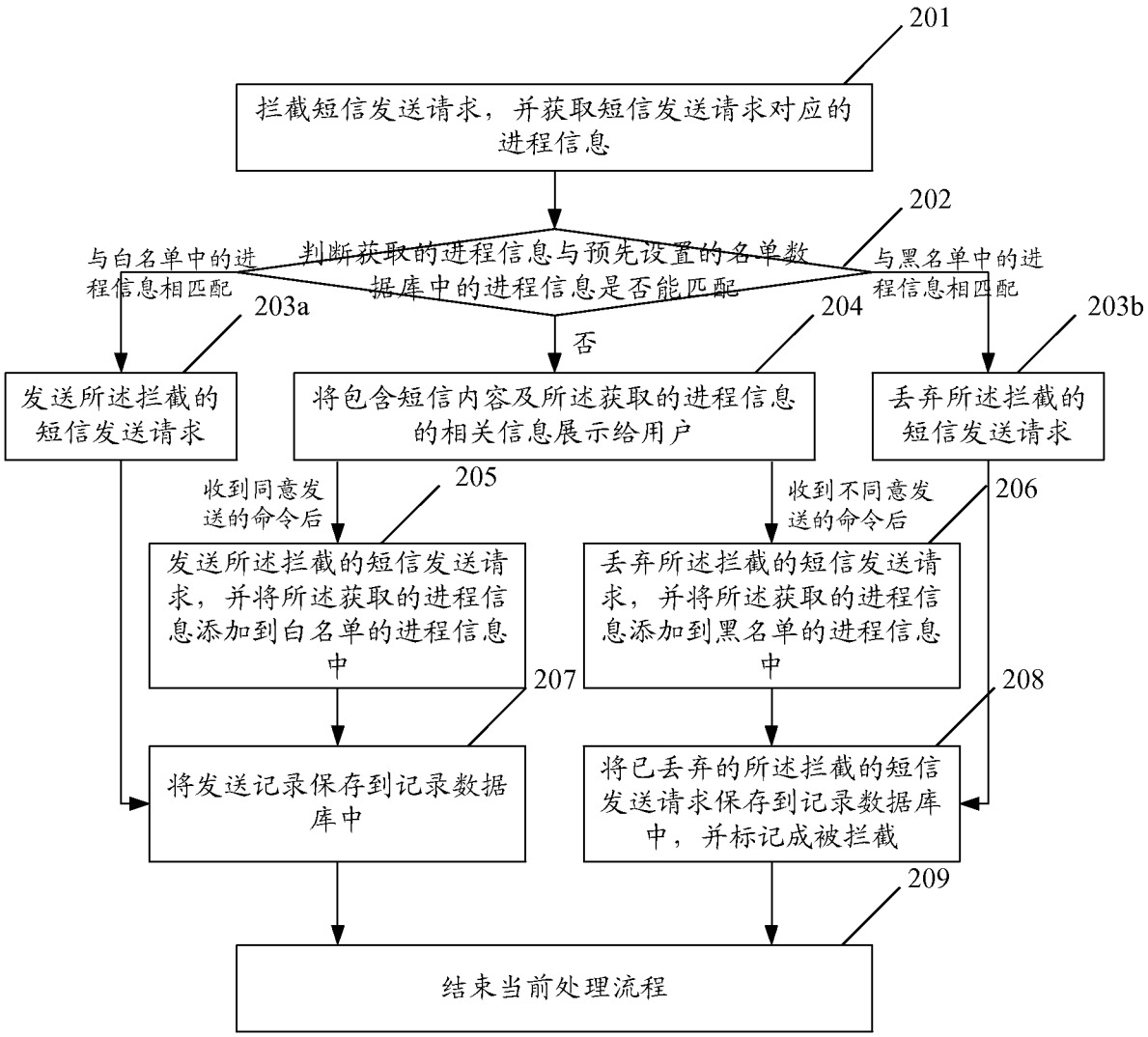
201
拦截短信发送请求，并获取短信发送请求对应的进程信息
202
判断获取的进程信息与预先设置的名单数据库中的进程信息是否能匹配
与白名单中的进程信息相匹配
与黑名单中的进程信息相匹配
否
203a
发送所述拦截的短信发送请求
204
将包含短信内容及所述获取的进程信息的相关信息展示给用户
203b
丢弃所述拦截的短信发送请求
收到同意发送的命令后
205
收到不同意发送的命令后
206
发送所述拦截的短信发送请求，并将所述获取的进程信息添加到白名单的进程信息中
丢弃所述拦截的短信发送请求，并将所述获取的进程信息添加到黑名单的进程信息中
207
208
将发送记录保存到记录数据库中
将已丢弃的所述拦截的短信发送请求保存到记录数据库中，并标记成被拦截
209
结束当前处理流程

图 2

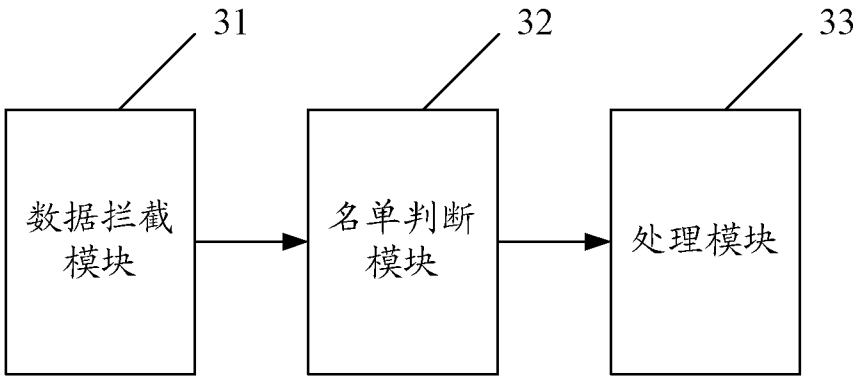

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/071428

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i

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: H04L; H04W; H04Q

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)

CPRSABS, CNTXT, CNKI, VEN: transmi+, sen+, outgoing, outbound, blacklist, whitelist, process??, software?, program?, application?, short 1w message?, SMS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LI Xiaoli. Anylasis of Mobile Virus and Research of Countermeasures. Chinese Doctoral Dissertations & Master's Theses Full-text Database (Master) Information Science and Technology. 15 May 2006, No.5 2006, ISSN 1671-6779 the straight matter pages 44-61 chapter 5	1-10
X	WO2010010060A2 (F-SECURE OYJ) 28 Jan. 2010(28.01.2010) the description page 6 line 3-page 10 line 13	1-10
X	CN101771686A (ASPIRE DIGITAL TECHNOLOGIES SHENZHEN CO LTD) 07 Jul. 2010(07.07.2010) claims 1-10	1-10
E	CN102088679A (BEIJING WANGQIN TIANXIA SCI & TECHNOLOGY CO LTD) 08 Jun. 2011(08.06.2011) the description page 3 paragraph 2-page 6 the last paragraph 2	1, 7
A	CN1889423A (HUAWEI TECHNOLOGIES CO LTD) 03 Jan. 2007(03.01.2007) the whole document	1-10

☐ 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
06 Jul. 2011(06.07.2011)	**11 Aug. 2011 (11.08.2011)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LI, Meili Telephone No. (86-10)62411247

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/071428

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO2010010060A2	28.01.2010	WO2010010060A3	06.05.2010
		AU2009273280A1	28.01.2010
		GB2474203A	06.04.2011
CN101771686A	07.07.2010	None	
CN102088679A	08.06.2011	None	
CN1889423A	03.01.2007	None	

国际检索报告

国际申请号
PCT/CN2011/071428

A. 主题的分类

H04W 12/00(2009.01)i

按照国际专利分类(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: H04L; H04W; H04Q

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）)

CPRSABS, CNTXT, CNKI, VEN: 发送,发出,名单,进程,软件,程序,短信,短消息,短信息, transmi+, sen+, outgoing, outbound, blacklist, whitelist, process??, software?, program?, application?, short 1w message?, SMS

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	李晓丽，手机病毒的分析及对策研究，中国优秀硕士学位论文全文数据库信息科技辑，15.5 月 2006，2006 年第 05 期，ISSN 1671-6779 正文第 44-61 页第 5 章	1-10
X	WO2010010060A2（F-SECURE OYJ） 28.1 月 2010(28.01.2010) 说明书第 6 页第 3 行-第 10 页第 13 行	1-10
X	CN101771686A（卓望数码技术(深圳)有限公司） 07.7 月 2010(07.07.2010) 权利要求 1-10	1-10
E	CN102088679A（北京网秦天下科技有限公司） 08.6 月 2011(08.06.2011) 说明书第 3 页第 2 段-第 6 页倒数第 2 段	1, 7
A	CN1889423A（华为技术有限公司） 03.1 月 2007(03.01.2007) 全文	1-10

☐ 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，或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（如具体说明的）

"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
06.7 月 2011(06.07.2011)	**11.8 月 2011 (11.08.2011)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 李美丽 电话号码：(86-10) **62411247**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/071428

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO2010010060A2	28.01.2010	WO2010010060A3	06.05.2010
		AU2009273280A1	28.01.2010
		GB2474203A	06.04.2011
CN101771686A	07.07.2010	无	
CN102088679A	08.06.2011	无	
CN1889423A	03.01.2007	无	