(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104572394 B
(45)授权公告日 2018.04.27

(21)申请号 201310522520.4

(22)申请日 2013.10.29

(65)同一申请的已公布的文献号
申请公布号 CN 104572394 A

(43)申请公布日 2015.04.29

(73)专利权人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 梁家辉

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫

(51)Int.Cl.
G06F 11/30(2006.01)

(56)对比文件
CN 102314561 A,2012.01.11,
CN 101290587 A,2008.10.22,

审查员 王晓渊

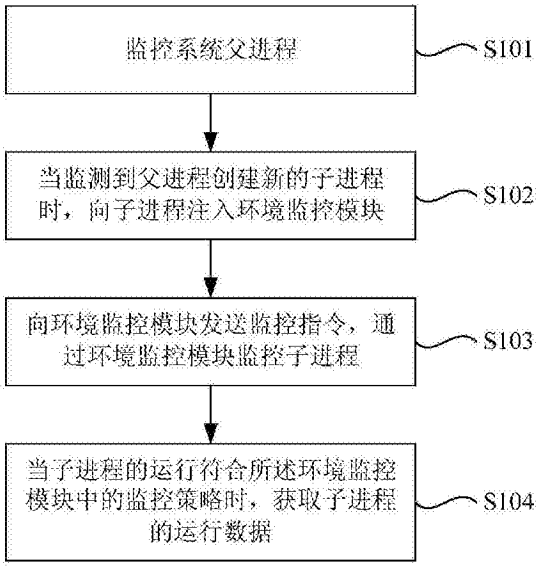
权利要求书1页 说明书5页 附图4页

(54)发明名称

进程监控方法及装置

(57)摘要

本发明实施例提出一种进程监控方法及装置,其方法包括:监控系统父进程;当监测到父进程创建新的子进程时,向新的子进程注入环境监控模块;向环境监控模块发送监控指令,通过环境监控模块监控子进程;以及当子进程的运行符合所述环境监控模块中的监控策略时,获取子进程的运行数据。本发明通过在父进程建立子进程时,动态地对子进程注入监控程序,无需对源码作任何改变,不影响正常运作的情况下,实现对系统进程的监控,具有较低的技术风险,开发成本低。而且在需要更新或修复bug时,也不会牵扯到大量的源码,技术门槛低,修改和使用时更加方便。



CN 104572394 B

1.一种进程监控方法,其特征在于,包括:

监控系统父进程;具体包括:监测是否有创建新进程的函数被调用,以获知是否有新的子进程被创建;

当监测到父进程创建新的子进程时,即监测到父进程调用创建新进程的函数时,动态地向新的子进程注入环境监控模块;向环境监控模块发送监控指令,通过环境监控模块监控子进程的运行状况或监控子进程是否调用文件操作函数;其中,所述环境监控模块中设置有监控策略,监控策略为预先设置在环境监控模块中或通过监控指令传输给环境监控模块;

当子进程的运行符合所述环境监控模块中的监控策略时,获取所述环境监控模块监控到的所有数据或当子进程调用文件操作函数时,核对文件操作事件是否符合环境监控模块中的监控策略,并在文件操作事件符合监控策略时,获取文件操作事件的上下文数据;

对获取的数据进行过滤,以提高收集到的数据的有效性,降低后续对这些数据分析时的运算量和错误率;

对子进程运行状况进行管理与分析,通过对数据的分析获知对某个文件的操作情况,或者根据子进程的运行数据查找是否存在病毒动态行为数据。

2.如权利要求1所述的进程监控方法,其特征在于,所述环境监控模块中设置有监控配置表,所述监控配置表用于存放所述监控信息,所述监控信息包括用户标识符和文件路径;

所述核对文件操作事件是否符合环境监控模块中的监控策略的步骤包括:核对文件操作事件的用户标识符和文件路径是否与所述监控配置表中存放的监控信息一致。

3.一种进程监控装置,其特征在于,包括:

父进程监控单元,用于监控系统父进程;具体包括:监测是否有创建新进程的函数被调用,以获知是否有新的子进程被创建;

逻辑加载单元,用于当所述父进程监控单元监测到父进程创建新的子进程时,即监测到父进程调用创建新进程的函数时,动态地向新的子进程注入环境监控模块;

控制中心单元,向环境监控模块发送监控指令,并通过环境监控模块监控子进程的运行状况或监控子进程是否调用文件操作函数;其中,所述环境监控模块中设置有监控策略,监控策略为预先设置在环境监控模块中或通过监控指令传输给环境监控模块;

数据获取单元,用于在子进程的运行符合所述环境监控模块中的监控策略时,获取所述环境监控模块监控到的所有数据或在子进程调用文件操作函数且文件操作事件符合监控策略时,获取文件操作事件的上下文数据;还用于对子进程运行状况进行管理与分析,通过对数据的分析获知对某个文件的操作情况,或者根据子进程的运行数据查找是否存在病毒动态行为数据;

过滤单元,用于对获取的数据进行过滤,以提高收集到的数据的有效性,降低后续对这些数据分析时的运算量和错误率。

4.如权利要求3所述的进程监控装置,其特征在于,所述环境监控模块中设置有监控配置表,所述监控配置表用于存放所述监控信息,所述监控信息包括用户标识符和文件路径;

所述数据获取单元在子进程调用文件操作函数,且文件操作事件的用户标识符和文件路径与所述监控配置表中存放的监控信息一致时,获取文件操作事件的上下文数据。

进程监控方法及装置

技术领域

[0001] 本发明涉及一种监控技术，特别涉及一种进程监控方法及装置。

背景技术

[0002] 随着移动通信电子技术的发展，如今以手机为典型代表的移动终端已经不单具有远程通话的功能，许多个人电脑上的应用程序功能都可以通过移动终端来实现，如用户可以通过手机的浏览器浏览网页内容、通过手机上播放器播放视频和音乐、通过手机上的摄像头进行拍照等。因此为了全方位地掌握智能手机的运行状况，对系统中应用程序的进程管理也变得尤为重要。

[0003] 目前，对移动终端系统进程的监控，需要修改操作系统的底层源码。以安卓系统的手机为例，现有技术是通过修改系统zygote源码(zygote是安卓系统上所有应用程序的父进程，通过修改zygote的逻辑，会直接影响到其所有子进程)的方式，实现对应用进程的监控。

[0004] 但是，由于需要修改操作系统源码，因此不同的厂商会有不同的定制化要求，开发成本高；其次，因为代码是写死在系统中的，如果需要版本更新或者存在bug需要修复，对于普通用户来说，技术门槛非常高，造成使用上的不便。另外，由于厂商修改了操作系统的底层源码，需要承担更多的技术风险。

发明内容

[0005] 本发明实施例的目的是提供一种进程监控方法及装置，以解决现有的对移动终端进程监控，需要修改系统源码，而造成的开发成本高、更新修改不便、技术风险大的问题。

[0006] 本发明实施例提出一种进程监控方法，包括：

[0007] 监控系统父进程；

[0008] 当监测到父进程创建新的子进程时，向新的子进程注入环境监控模块；

[0009] 向环境监控模块发送监控指令，通过环境监控模块监控子进程；以及

[0010] 当子进程的运行符合所述环境监控模块中的监控策略时，获取子进程的运行数据。

[0011] 本发明实施例还提出一种进程监控装置，包括：

[0012] 父进程监控单元，用于监控系统父进程；

[0013] 逻辑加载单元，用于当所述父进程监控单元监测到父进程创建新的子进程时，向新的子进程注入环境监控模块；

[0014] 控制中心单元，用于向环境监控模块发送监控指令，并通过环境监控模块监控子进程；以及

[0015] 数据获取单元，用于在子进程的运行符合所述环境监控模块中的监控策略时，获取子进程的运行数据。

[0016] 相对于现有技术，本发明的有益效果是：本发明实施例的方法和装置，通过在父进

程建立子进程时，动态地对子进程注入监控程序，无需对源码作任何改变，不影响正常运作的情况下，实现对系统进程的监控，因而可以把整个逻辑实现在一个应用程序上。因此，在不牵扯到源码的情况下，只需要单纯对监控程序进行设计，具有较低的技术风险，开发成本低。而且在需要更新或修复bug时，也不会牵扯到大量的源码，技术门槛低，修改和使用时更加方便。

附图说明

[0017] 图1为本发明实施例的第一种进程监控方法的流程图；

[0018] 图2为本发明实施例的第二种进程监控方法的流程图；

[0019] 图3为本发明实施例的第三种进程监控方法的流程图；

[0020] 图4为本发明实施例的第一种进程监控装置的结构图；

[0021] 图5为本发明实施例的第二种进程监控装置的结构图。

具体实施方式

[0022] 有关本发明的前述及其他技术内容、特点及功效，在以下配合参考图式的较佳实施例详细说明中将可清楚的呈现。通过具体实施方式的说明，当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解，然而所附图式仅是提供参考与说明之用，并非用来对本发明加以限制。

[0023] 请参见图1，其为本发明实施例的第一种进程监控方法的流程图，其包括以下步骤：

[0024] S101，监控系统父进程。

[0025] S102，当监测到父进程创建新的子进程时，向新的子进程注入环境监控模块。

[0026] 监控父进程时，可以监测是否有创建新进程的函数被调用，例如安卓系统如的父进程zygote，每产生一个子进程，其都会调用fork这个函数，因而只需监测fork是否被调用便可知道是否有新的子进程创被建。

[0027] S103，向环境监控模块发送监控指令，通过环境监控模块监控子进程。

[0028] 当接受到监控指令，环境监控模块便会开始工作，对子进程进行监控，以获取需要的数据。所述环境监控模块中设置有监控策略，例如监测某一个函数是否被调用，或者监测某个文件是否被操作等。监控策略可以是预先设置在环境监控模块中的，也可以是通过监控指令传输给环境监控模块的。

[0029] S104，当子进程的运行符合所述环境监控模块中的监控策略时，获取子进程的运行数据。

[0030] 获取的数据是用来后续对子进程运行状况的管理与分析，例如通过对数据的分析获知对某个文件的操作情况，或者根据子进程的运行数据查找是否存在病毒动态行为数据等。

[0031] 所述获取的运行数据的范围可以在监控策略中进行相应的设定。例如对某个文件的操作进行监控时，设定获取对这个对文件整个操作事件的上下文数据。又如，监控病毒时可以获取环境监控模块监测到的所有数据。

[0032] 本实施例的方法，通过在父进程建立子进程时，动态地对子进程注入监控程序，无

需对源码作任何改变，不影响正常运作的情况下，实现对系统进程的监控，因而可以把整个逻辑实现在一个应用程序上，如APK(APK是应用程序安卓文件格式)的形式或开发包jar(Java Archive，归档文件)的形式。因此，在不牵扯到源码的情况下，只需要单纯对监控程序进行设计，具有较低的技术风险，开发成本低。而且在需要更新或修复bug时，也不会牵扯到大量的源码，技术门槛低，修改和使用时更加方便。

[0033] 请参见图2，其为本发明实施例的第二种进程监控方法的流程图，其包括以下步骤：

[0034] S201，监控系统父进程。

[0035] S202，判断父进程是否调用创建新进程的函数，若是则进入步骤S203，若否则返回步骤S201。

[0036] S203，向新的子进程注入环境监控模块。本实施例的环境监控模块中设置有监控配置表，所述监控配置表用于存放用户标识符(uid)、文件路径及监控规则等监控信息。

[0037] S204，向环境监控模块发送监控指令，通过环境监控模块监测子进程是否调用文件操作函数。文件操作函数如open，unlink，rename，read，write等函数。

[0038] S205，当子进程调用文件操作函数时，核对文件操作事件的用户标识符和文件路径是否与所述监控配置表中存放的监控信息一致，若一致则进入步骤S206，若不一致则返回S204。

[0039] 监控配置表中存放的监控信息可以通过发送给环境监控模块的监控指令来配置。例如用户要对某个文件的操作行为进行监控时，可以将用户标识符、要监控的文件路径及要监控的操作函数等监控信息中的一种或多种添加到监控指令中发送给环境监控模块，并由环境监控模块配置在监控配置表中。假设监控配置表中的一组监控信息包括：用户A、文件路径B、操作函数open，则当子程序调用open函数时，会核对操作事件中的用户标识符和文件路径是否分别为A和B，若是则一致，反之则不一致。

[0040] S206，获取文件操作事件的上下文数据。获取的数据包括但不仅限于文件操作ID(open，unlink，rename函数的编号)，文件路径，操作事件，用户标识符uid和进程标识符pid等。

[0041] 本实施例的方法可以实现对进程中的文件操作行为进行的监控，基于不用修改源码的特点，具有技术风险低、开发成本低、技术门槛低、修改和使用方便的优点。而且，由于采用动态注入技术，所以不需要预先指定要监控的文件路径，而是可以由用户在需要的时候动态指定，具有很强的互动性。

[0042] 请参见图3，其为本发明实施例的第三种进程监控方法的流程图，其包括以下步骤：

[0043] S301，监控系统父进程。

[0044] S302，当监测到父进程创建新的子进程时，向新的子进程注入环境监控模块。

[0045] S303，向环境监控模块发送监控指令，通过环境监控模块监控子进程。本实施中，环境监控模块中的监控策略是监测子进程的一切运行状况。

[0046] S304，获取所述环境监控模块监控到的所有数据。

[0047] S305，对获取的数据进行过滤。过滤的目的是为了提高收集到的数据的有效性，以降低后续对这些数据分析时的运算量和错误率。比如对单位时间内重复的日志数据进行去

重。

[0048] 本实施例的方法特别适用于大数据量的收集和测试，例如利用对日志数据的分析，查找是否存在病毒动态行为数据。由于采用动态注入技术进行监控，无需修改系统源码，降低了开发成本和技术风险，也方便了对监控程序的更新和修改。

[0049] 本发明实施例还提出一种进程监控装置，请参见图4，其包括：父进程监控单元41、逻辑加载单元42、控制中心单元43以及数据获取单元44。

[0050] 父进程监控单元41用于监控系统父进程。具体来说，父进程监控单元41会对父进程是否创建新的子进程进行监控，例如监测父进程是否调用创建子进程的函数。

[0051] 逻辑加载单元42用于当父进程监控单元41监测到父进程创建新的子进程时，向新的子进程注入环境监控模块。所述环境监控模块中设置有监控策略，其用来对子进程的运行进行监控并对需要的数据进行采集。

[0052] 控制中心单元43用于向环境监控模块发送监控指令，并通过环境监控模块监控子进程。控制中心单元43可以为用户提供一个交互界面，并让用户设定监控策略，如要监控的对象、函数等，并通过监控指令一同发送给环境监控模块。

[0053] 数据获取单元44用于在子进程的运行符合所述环境监控模块中的监控策略时，获取子进程的运行数据。获取的数据是用来后续对子进程运行状况的管理与分析，例如通过对数据的分析获知对某个文件的操作情况，或者根据子进程的运行数据查找是否存在病毒动态行为数据等。所述获取的运行数据的范围可以在监控策略中进行相应的设定。

[0054] 以对文件操作的监控为例，当父进程监控单元41监测到父进程创建了新的子进程时，逻辑加载单元42会将环境监控模块加载到新建的子进程中。然后，控制中心单元43可以向用户提供交互界面，以供用户输入要监控的文件、路径、操作等监控信息，然后将这些监控信息添加到监控指令中，并发送给环境监控模块。环境监控模块接收到监控指令后开始工作，监测子进程是否调用预设的open,unlink,rename,read,write等文件操作函数。当文件操作函数被调用时，会与环境监控模块中设置的监控配置表进行比对，核对操作事件的用户标识符和文件路径与所述监控配置表中存放的监控信息是否一致。若一致则数据获取单元44会获取该文件操作事件的上下文数据，以供用户分析或使用。

[0055] 又如以监控病毒动态行为数据为例，当父进程监控单元41监测到父进程创建了新的子进程时，逻辑加载单元42会将环境监控模块加载到新建的子进程中。控制中心单元43向环境监控模块发出监控指令后，会通过环境监控模块监测子进程的动态行为数据。并由数据获取单元44获取环境监控模块监测到的这些动态行为数据，以供用户分析其中是否存在病毒动态行为数据。

[0056] 本实施例的装置，通过在父进程建立子进程时，动态地对子进程注入监控程序，无需对源码作任何改变，不影响正常运作的情况下，实现对系统进程的监控，因而可以把整个逻辑实现在一个应用程序上，如APK(APK是应用程序安卓文件格式)的形式或开发包jar(Java Archive，归档文件)的形式。因此，在不牵扯到源码的情况下，只需要单纯对监控程序进行设计，具有较低的技术风险，开发成本低。而且在需要更新或修复bug时，也不会牵扯到大量的源码，技术门槛低，修改和使用时更加方便。

[0057] 请参见图5，其为本发明实施例的第二种进程监控装置的结构图，与图4的实施例相比，本实施例的装置还包括过滤单元45，过滤单元45用于对数据获取单元44获取的数据

进行过滤。过滤的目的是为了提高收集到的数据的有效性，以降低后续对这些数据分析时的运算量和错误率。比如对单位时间内重复的日志数据进行去重。本实施例装置的其它结构与功能均与图4的实施例相同，在此不再赘述。

[0058] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明实施例可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明实施例的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM，U盘，移动硬盘等)中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或网络设备等)执行本发明实施例各个实施场景所述的方法。

[0059] 以上所述，仅是本发明的较佳实施例而已，并非对本发明作任何形式上的限制，虽然本发明已以较佳实施例揭露如上，然而并非用以限定本发明，任何熟悉本专业的技术人员，在不脱离本申请技术方案范围内，当可利用上述揭示的技术内容作出些许更动或修饰为等同变化的等效实施例，但凡是未脱离本申请技术方案内容，依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

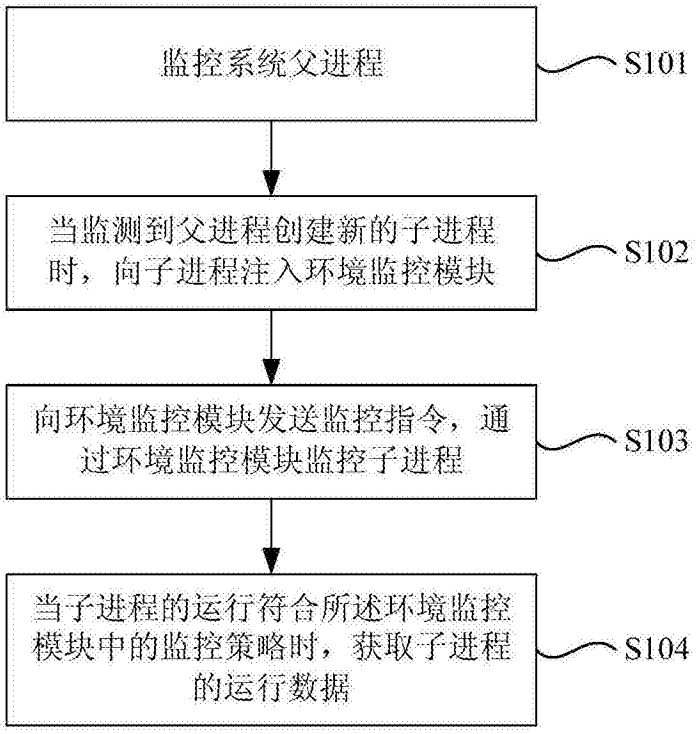

监控系统父进程
S101
当监测到父进程创建新的子进程时，向子进程注入环境监控模块
S102
向环境监控模块发送监控指令，通过环境监控模块监控子进程
S103
当子进程的运行符合所述环境监控模块中的监控策略时，获取子进程的运行数据
S104

图1

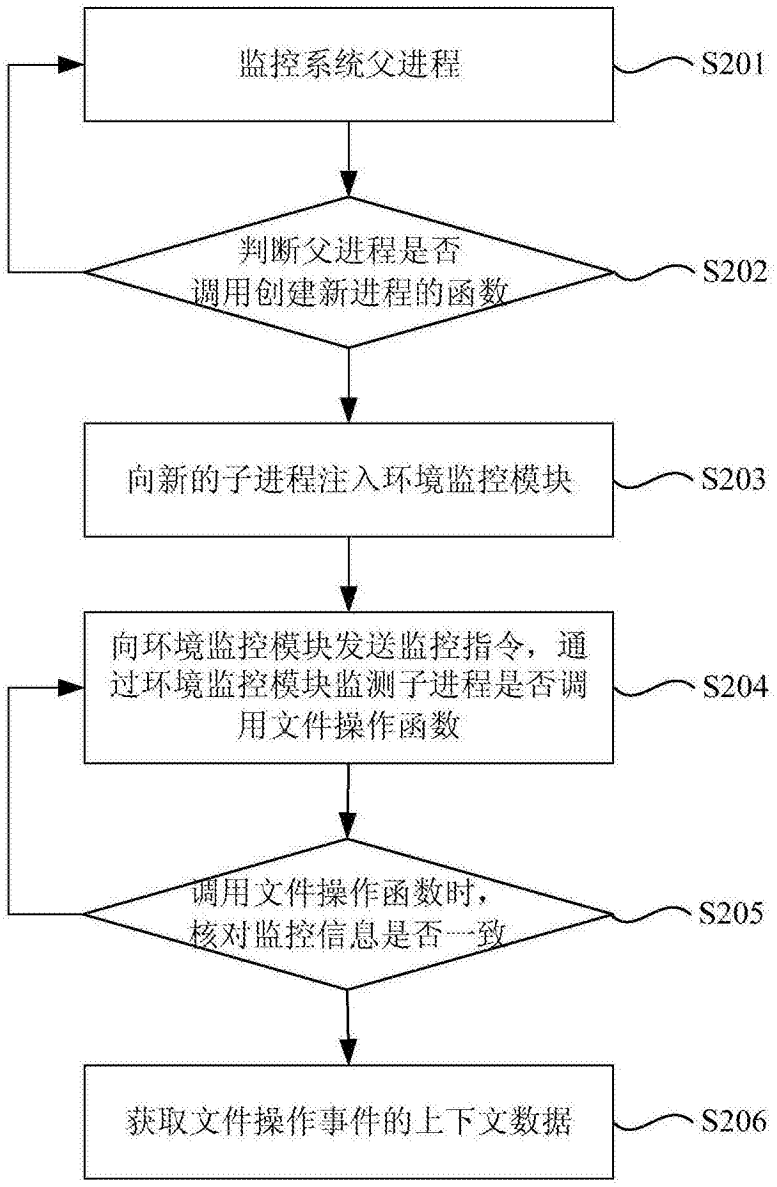

监控系统父进程
S201
判断父进程是否
调用创建新进程的函数
S202
向新的子进程注入环境监控模块
S203
向环境监控模块发送监控指令，通
过环境监控模块监测子进程是否调
用文件操作函数
S204
调用文件操作函数时，
核对监控信息是否一致
S205
获取文件操作事件的上下文数据
S206

图2

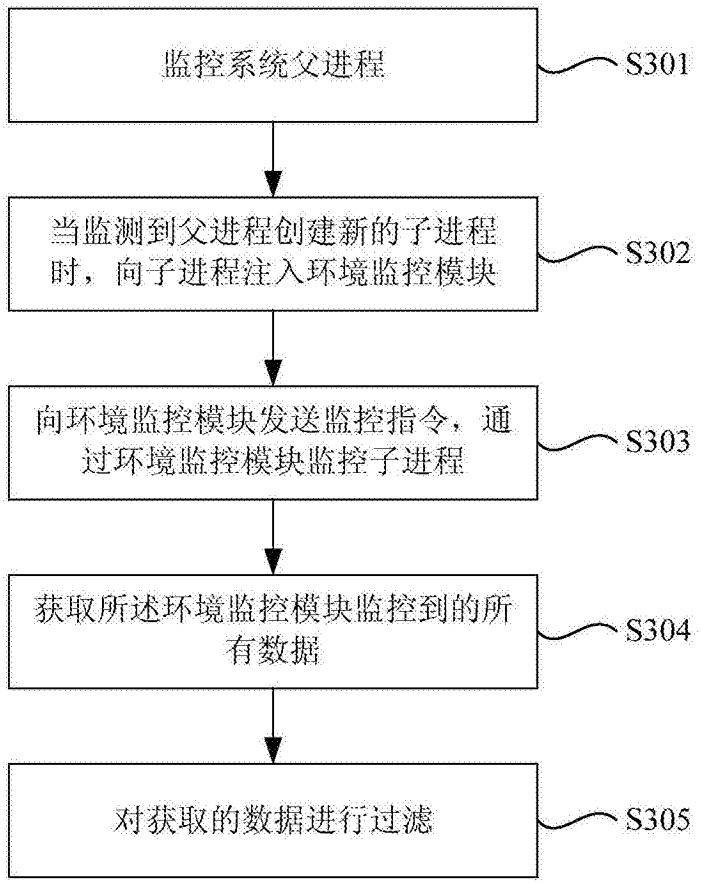

监控系统父进程
S301
当监测到父进程创建新的子进程时，向子进程注入环境监控模块
S302
向环境监控模块发送监控指令，通过环境监控模块监控子进程
S303
获取所述环境监控模块监控到的所有数据
S304
对获取的数据进行过滤
S305

图3

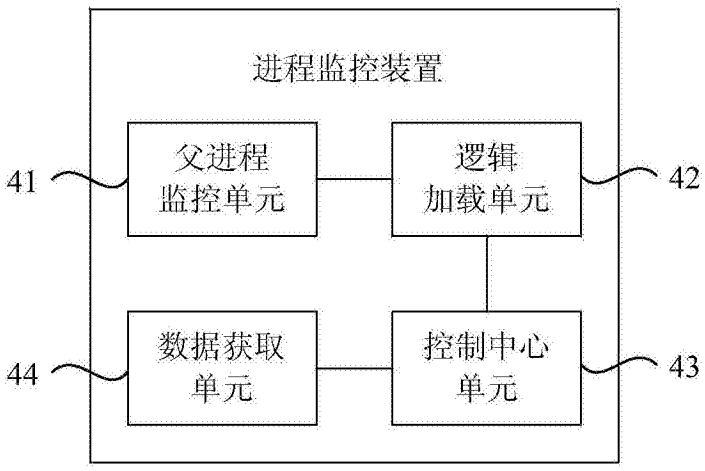

进程监控装置
父进程监控单元
逻辑加载单元
数据获取单元
控制中心单元
41
42
43
44

图4

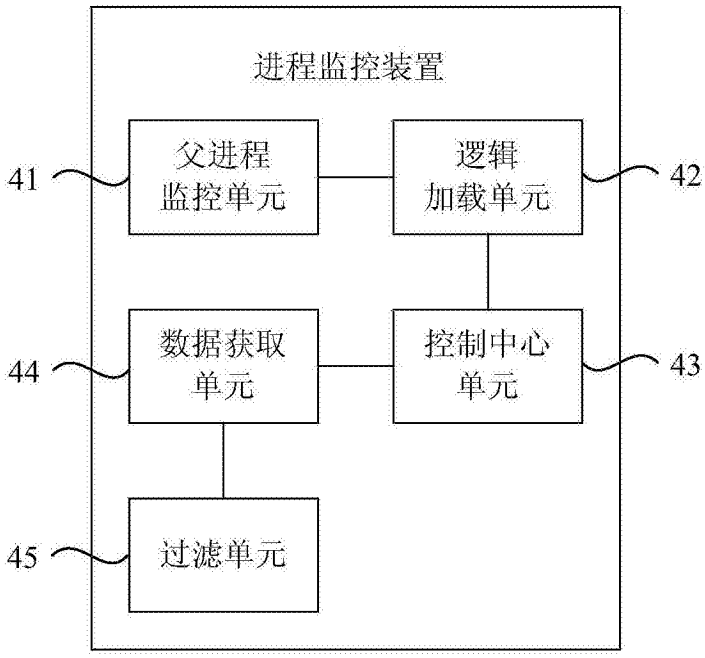


图5