

# (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  
2019 年 1 月 3 日 (03.01.2019)



(10) 国际公布号  
**WO 2019/001334 A1**

- (51) 国际专利分类号:  
**G06F 11/07** (2006.01)
- (21) 国际申请号: PCT/CN2018/092153
- (22) 国际申请日: 2018 年 6 月 21 日 (21.06.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201710502695.7 2017年6月27日 (27.06.2017) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 刘自龙 (**LIU, Zilong**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。朱亮亮 (**ZHU, Liangliang**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。曾旭 (**ZENG, Xu**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。陈凌君 (**CHEN, Lingjun**); 中国浙江省杭州市余杭区文一西路 969

号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。王斌 (**WANG, Bin**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。蔡俊杰 (**CAI, Junjie**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (**BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.**); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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。

(54) Title: STACK OVERFLOW PROCESSING METHOD AND DEVICE

(54) 发明名称: 一种栈溢出处理的方法及装置

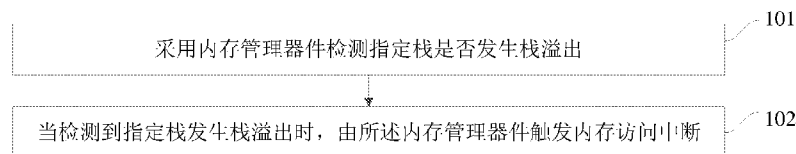


图 1

- 101 A memory management device is used to detect whether a specified stack overflows or not
- 102 When stack overflow of the specified stack is detected, the memory management device triggers a memory access interruption

(57) Abstract: Provided in the embodiments of the present application are a stack overflow processing method and device. The method comprises: a memory management device is used to detect whether a specified stack overflows or not; and when stack overflow of the specified stack is detected, the memory management device triggers memory access interruption. with the present invention, a memory management device is used to detect stack overflow, so that the timeliness of stack overflow detection may be effectively improved, occasional problems such as stack overflow may be discovered in time, and the time for inspecting stack overflow problems may be shortened.

(57) 摘要: 本申请实施例提供了一种栈溢出处理的方法及装置, 其中所述方法包括: 采用内存管理器件检测指定栈是否发生栈溢出; 当检测到所述指定栈发生栈溢出时, 由所述内存管理器件触发内存访问中断。通过内存管理器件来检测栈溢出, 可以有效提高栈溢出检测的时效性, 及时发现栈溢出等偶现性问题, 缩短栈溢出问题排查时间。

(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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

## 一种栈溢出处理的方法及装置

本申请要求 2017 年 06 月 27 日递交的申请号为 201710502695.7、发明名称为“一种栈溢出处理的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

### 技术领域

本申请涉及内存处理技术领域，特别是涉及一种栈溢出处理的方法以及一种栈溢出处理的装置。

### 10 背景技术

在操作系统的运行过程中，栈溢出是导致操作系统不稳定的重要原因，由于栈溢出具有偶现的特点，往往很难找到导致问题的原因，导致产品研发周期的不确定性。

在现有技术中，通常采用如下方式进行栈溢出检测：

在进程的栈初始化的时候，按预设的字节对齐方式，用特定魔数（比如 0x9527）将  
15 栈元素依次完成初始化；在系统运行的时候，通过守护进程，依次遍历各个进程的栈，检测栈元素的值是否等于初始化的魔数，求得被污染的元素个数所占栈大小的比例，即为栈使用量，根据栈使用量来判定是否发生栈溢出。

通过这种方法，虽然能检测到是否出现栈溢出，但由于需要在系统运行的时候通过检测魔数有没有改变来判定是否出现溢出，此时距离栈溢出已经有一段时间，因此，现  
20 有方案不能及时的检测出栈溢出，导致栈溢出的排查时间较长。

### 发明内容

鉴于上述问题，提出了本申请实施例以便提供一种克服上述问题或者至少部分地解决上述问题的一种栈溢出处理的方法和相应的一种栈溢出处理的装置。

25 为了解决上述问题，本申请实施例公开了一种栈溢出处理的方法，所述方法包括：  
采用内存管理器件检测指定栈是否发生栈溢出；

当检测到所述指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

优选地，在所述采用所述内存管理器件检测指定栈是否发生栈溢出的步骤之前，还包括：

30 获取所述指定栈的栈信息，所述栈信息包括所述指定栈的起始地址以及栈大小；

基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

采用所述内存管理器件，设置所述栈底地址的访问权限。

优选地，所述指定栈包括任务栈，所述获取所述指定栈的栈信息的步骤包括：

当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

5 优选地，所述指定栈包括中断栈，所述获取所述指定栈的栈信息的步骤包括：

从编译链接脚本程序中获取所述中断栈的栈信息。

优选地，所述采用所述内存管理器件检测指定栈是否发生栈溢出的步骤包括：

当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出。

优选地，所述方法还包括：

10 获取所述栈溢出对应的上下文信息；

基于所述上下文信息，进行栈溢出问题排查。

优选地，所述内存管理器件包括内存保护单元 MPU 或内存管理单元 MMU。

本申请实施例还公开了一种栈溢出处理的装置，所述装置包括：

栈溢出检测模块，用于采用内存管理器件检测指定栈是否发生栈溢出；

15 中断处理模块，用于当检测到所述指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

优选地，所述装置还包括：

栈信息获取模块，用于获取所述指定栈的栈信息，所述栈信息包括所述指定栈的起始地址以及栈大小；

20 栈底地址确定模块，用于基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

访问权限设置模块，用于采用所述内存管理器件，设置所述栈底地址的访问权限。

优选地，所述指定栈包括任务栈，所述栈信息获取模块还用于：

当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

25 优选地，所述指定栈包括中断栈，所述栈信息获取模块还用于：

从编译链接脚本程序中获取所述中断栈的栈信息。

优选地，所述栈溢出检测模块还用于：

当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出。

优选地，所述装置还包括：

30 上下文信息获取模块，用于获取所述栈溢出对应的上下文信息；

问题排查模块，用于基于所述上下文信息，进行栈溢出问题排查。

优选地，所述内存管理器件包括内存保护单元 MPU 或内存管理单元 MMU。

本申请实施例还公开了一种装置，包括：

一个或多个处理器；和

- 5        其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述装置执行上述的方法。

本申请实施例还公开了一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得装置执行上述的方法。

- 10       本申请实施例包括以下优点：

本申请实施例可以通过内存管理器件来检测任务栈或中断栈是否发生溢出。当内存管理器件检测到任务栈或中断栈发生溢出时，内存管理器件立刻触发内存访问中断，通过内存管理器件这种硬件的方式来检测栈溢出，可以有效提高栈溢出检测的时效性，及时发现栈溢出等偶现性问题，缩短栈溢出问题排查时间。

15

#### 附图说明

图 1 是本申请的一种栈溢出处理的方法实施例一的步骤流程图；

图 2 是本申请的一种栈溢出处理的方法实施例二的步骤流程图；

图 3 是本申请的一种栈溢出处理的装置实施例的结构框图；

- 20       图 4 本申请一种智能终端实施例的结构框图。

#### 具体实施方式

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

- 25       本申请实施例可以应用于安装有操作系统的计算设备中，该计算设备可以包括终端或服务器，该计算设备中可以包括内存管理器件。具体的，该内存管理器件可以用于对计算设备的内存进行管理，例如设置内存的访问权限、检测内存是否溢出、触发内存访问异常中断、进行内存异常处理等。

在本申请实施例中，该内存管理器件可以包括硬件器件和/或软件程序。

- 30       例如，该内存管理器件可以包括 MPU（Memory Protection Unit，内存保护单元），

MPU 中一个域就是一些属性值以及其对应的一片内存，这些属性包括：起始地址、长度、读写权限以及缓存等。

又如，该内存管理器件可以包括 MMU (Memory Management Unit, 内存管理单元)，MMU 是中央处理器 CPU 中用来管理虚拟存储器、物理存储器的控制线路，同时也负责  
5 虚拟地址映射为物理地址、以及提供硬件机制的内存访问授权、多用户多进程操作系统。

在一种实施方式中，该内存管理可以包括栈的管理，其中，栈是操作系统中抽象出来的一种先进后出的内存区域，主要用于局部变量和接口调用参数的自动存取。作为一种示例，栈可以包括任务栈和中断栈。

任务栈可以用于在任务切换时保存上下文信息。

10 中断栈可以用于产生中断时保存上下文信息。

本申请实施例可以应用于互联网中的内存管理，也可以应用于物联网 (Internet of Things, 简称 IoT) 中的内存管理。

以下以物联网的内存管理为例，对本申请实施例进行详细说明：

参照图 1，示出了本申请的一种栈溢出处理的方法实施例一的步骤流程图，本申请  
15 实施例具体可以包括如下步骤：

步骤 101，采用内存管理器件检测指定栈是否发生栈溢出；

在本申请实施例中，计算设备所使用的操作系统可以包括 RTOS (Real Time Operating System, 实时操作系统)。

在一种实施方式中，本申请实施例所说的指定栈可以包括 RTOS 系统中任务栈或中  
20 断栈。

步骤 102，当检测到指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

本申请实施例可以通过内存管理器件来检测任务栈或中断栈是否发生溢出。当内存管理器件检测到任务栈或中断栈发生溢出时，内存管理器件立刻触发内存访问中断，通过内存管理器件这种硬件的方式来检测栈溢出，可以有效提高栈溢出检测的时效性，及  
25 时发现栈溢出等偶现性问题，缩短栈溢出问题排查时间。

参照图 2，示出了本申请的一种栈溢出处理的方法实施例二的步骤流程图，本申请实施例具体可以包括如下步骤：

步骤 201，获取指定栈的栈信息；

30 在具体实现中，RTOS 系统可以获取指定栈的栈信息，作为一种示例，该栈信息可

以包括但不限于：指定栈的起始地址、栈大小、栈名称、任务名称等。

在本申请实施例的一种优选实施例中，若指定栈为任务栈，则步骤 201 进一步可以包括如下子步骤：当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

5 具体的，由于任务栈随着任务的切换而切换，因此，可以在检测到任务栈进行切换时，获得任务栈的栈信息。在具体实现中，若检测到系统调度的任务的指针发生变化时，则可以判定此时任务栈发生切换，此时，可以根据切换后的任务的指针所指向的地址，获得切换后的任务的数据结构，从该数据结构中获得栈信息。

在本申请实施例的另一种优选实施例中，若指定栈为中断栈，则步骤 201 进一步可以包括如下子步骤：从编译链接脚本程序中获取所述中断栈的栈信息。

10 具体的，物联网系统中共用一个中断栈，栈信息在系统编译链接脚本中声明，因此可以在系统编译前从编译链接脚本程序中获取中断栈的栈信息。

步骤 202，基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

在具体实现中，可以从栈信息中获得对应的栈的起始地址以及栈大小，并根据“栈的起始地址+栈大小”得到该栈的栈底地址。

15 在实际中，该栈底地址可以为栈增长方向的边缘。

步骤 203，采用内存管理器件，设置所述栈底地址的访问权限；

在本申请实施例中，得到栈底地址以后，可以采用内存管理器件，设置栈底地址的访问权限，以对栈增长方向的边缘进行保护。

20 在具体实现中，可以对栈底地址对应的内存空间设置 MPU 保护，在 MPU 中设定该栈底地址的访问权限，作为一种示例，该访问权限可以包括：禁止读和/或禁止写和/或禁止执行代码等。或者，该访问权限也可以设定为禁止一切访问操作。

步骤 204，当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出；

25 具体的，当检测到针对栈底地址的访问操作时，则可以判定该任务栈或中断栈发生栈溢出。在实现中，因为已经限制了栈底的访问权限，当对栈底进行读或写或执行等操作时，则可以判定栈溢出。

步骤 205，由所述内存管理器件触发内存访问中断；

在本申请实施例中，当检测到针对任务栈或中断栈的栈底的访问操作时，可以立刻触发内存访问异常的中断。

30 步骤 206，获取所述栈溢出对应的上下文信息，并基于所述上下文信息，进行栈溢出问题排查。

当内存管理器件触发内存访问中断以后，操作系统执行中断异常处理函数以进行内存访问异常处理。

在内存访问异常处理的过程中，可以打印上下文信息，并根据该上下文信息进行异常分析，以进行问题排查。

5       作为一种示例，该上下文信息可以包括但不限于触发中断的任务标识、中断执行状态、函数调用栈信息等。

在本申请实施例中，可以通过 MPU 对栈增长方向的边缘进行保护，禁止读和/或写和/或执行等操作，在系统代码出现栈溢出时立刻触发内存访问中断，通过硬件中断的方式有效提高栈溢出检测的时效性，及时发现栈溢出等偶现性问题，缩短栈溢出问题排查  
10   时间。

需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员  
15   也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请实施例所必须的。

参照图 3，示出了本申请的一种栈溢出处理的装置实施例的结构框图，所述装置具体可以包括如下模块：

20       栈溢出检测模块 301，用于采用内存管理器件检测指定栈是否发生栈溢出；

中断处理模块 302，用于当检测到所述指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

在本申请实施例的一种优选实施例中，所述装置还可以包括如下模块：

25       栈信息获取模块，用于获取所述指定栈的栈信息，所述栈信息包括所述指定栈的起始地址以及栈大小；

栈底地址确定模块，用于基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

访问权限设置模块，用于采用所述内存管理器件，设置所述栈底地址的访问权限。

30       在本申请实施例的一种优选实施例中，所述指定栈包括任务栈，所述栈信息获取模块还用于：

当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

在本申请实施例的一种优选实施例中，所述指定栈包括中断栈，所述栈信息获取模块还用于：

从编译链接脚本程序中获取所述中断栈的栈信息。

5       在本申请实施例的一种优选实施例中，所述栈溢出检测模块 301 还用于：

当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出。

在本申请实施例的一种优选实施例中，所述装置还可以包括如下模块：

上下文信息获取模块，用于获取所述栈溢出对应的上下文信息；

问题排查模块，用于基于所述上下文信息，进行栈溢出问题排查。

10       在本申请实施例的一种优选实施例中，所述内存管理器件包括内存保护单元 MPU 或内存管理单元 MMU。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

15       本公开的实施例可被实现为使用任意适当的硬件，固件，软件，或及其任意组合进行想要的配置的系统。图 4 示意性地示出了可被用于实现本公开中所述的各个实施例的示例性系统（或装置）400。

20       对于一个实施例，图 4 示出了示例性系统 400，该系统具有一个或多个处理器 402、被耦合到(一个或多个)处理器 402 中的至少一个的系统控制模块（芯片组）404、被耦合到系统控制模块 404 的系统存储器 406、被耦合到系统控制模块 404 的非易失性存储器 (NVM)/存储设备 408、被耦合到系统控制模块 404 的一个或多个输入/输出设备 410，以及被耦合到系统控制模块 406 的网络接口 412。

25       处理器 402 可包括一个或多个单核或多核处理器，处理器 402 可包括通用处理器或专用处理器（例如图形处理器、应用处理器、基频处理器等）的任意组合。在一些实施例中，系统 400 能够作为本申请实施例中所述的浏览器。

在一些实施例中，系统 400 可包括具有指令的一个或多个计算机可读介质(例如，系统存储器 406 或 NVM/ 存储设备 408) 以及与该一个或多个计算机可读介质相合并被配置为执行指令以实现模块从而执行本公开中所述的动作的一个或多个处理器 402。

30       对于一个实施例，系统控制模块 404 可包括任意适当的接口控制器，以向(一个或多个)处理器 402 中的至少一个和/或与系统控制模块 404 通信的任意适当的设备或组件提供

任意适当的接口。

系统控制模块 404 可包括存储器控制器模块，以向系统存储器 406 提供接口。存储器控制器模块可以是硬件模块、软件模块和/或固件模块。

5 系统存储器 406 可被用于例如为系统 400 加载和存储数据和/或指令。对于一个实施例，系统存储器 406 可包括任意适当的易失性存储器，例如，适当的 DRAM。在一些实施例中，系统存储器 406 可包括双倍数据速率类型四同步动态随机存取存储器 (DDR4SDRAM)。

对于一个实施例，系统控制模块 404 可包括一个或多个输入/输出控制器，以向 NVM/存储设备 408 及(一个或多个)输入/输出设备 410 提供接口。

10 例如，NVM/存储设备 408 可被用于存储数据和/或指令。NVM/存储设备 408 可包括任意适当的非易失性存储器(例如，闪存)和/或可包括任意适当的(一个或多个)非易失性存储设备(例如，一个或多个硬盘驱动器(HDD)、一个或多个光盘(CD)驱动器和/或一个或多个数字通用光盘(DVD)驱动器)。

15 NVM/存储设备 408 可包括在物理上作为系统 400 被安装在其上的设备的一部分的存储资源，或者其可被该设备访问而不必作为该设备的一部分。例如，NVM/存储设备 408 可通过网络经由(一个或多个)输入/输出设备 410 进行访问。

NVM/存储设备 408 还可以包括内存管理器件，该内存管理器件可以包括 MPU 或 MMU 等，用于对终端的内存进行管理，例如设置内存的访问权限、检测内存是否溢出、触发内存访问异常中断、进行内存异常处理等。

20 (一个或多个)输入/输出设备 410 可为系统 400 提供接口以与任意其他适当的设备通信，输入/输出设备 410 可以包括通信组件、音频组件、传感器组件等。网络接口 412 可为系统 400 提供接口以通过一个或多个网络通信，系统 400 可根据一个或多个无线网络标准和/或协议中的任意标准和/或协议来与无线网络的一个或多个组件进行无线通信，例如接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合进行无线通信。

25 对于一个实施例，(一个或多个)处理器 402 中的至少一个可与系统控制模块 404 的一个或多个控制器(例如，存储器控制器模块)的逻辑封装在一起。对于一个实施例，(一个或多个)处理器 402 中的至少一个可与系统控制模块 404 的一个或多个控制器的逻辑封装在一起以形成系统级封装(SiP)。对于一个实施例，(一个或多个)处理器 402 中的至少一个可与系统控制模块 404 的一个或多个控制器的逻辑集成在同一模具上。对于一个实施例，(一个或多个)处理器 402 中的至少一个可与系统控制模块 404 的一个或多个控制

30

器的逻辑集成在同一模具上以形成片上系统(SoC)。

在各个实施例中，系统 400 可以但不限于是：浏览器、工作站、台式计算设备或移动计算设备(例如，膝上型计算设备、手持计算设备、平板电脑、上网本等)。在各个实施例中，系统 400 可具有更多或更少的组件和/或不同的架构。例如，在一些实施例中，

5 系统 400 包括一个或多个摄像机、键盘、液晶显示器(LCD) 屏幕(包括触屏显示器)、非易失性存储器端口、多个天线、图形芯片、专用集成电路(ASIC)和扬声器。

其中，如果显示器包括触摸面板，显示屏可以被实现为触屏显示器，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或

10 滑动操作相关的持续时间和压力。

本申请实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块 (programs)，该一个或多个模块被应用在终端设备时，可以使得该终端设备执行本申请实施例中各方法步骤的指令 (instructions)。

15 在一个示例中提供了一种装置，包括：一个或多个处理器；和，其上存储的有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述装置执行如本申请实施例中的方法。

在一个示例中还提供了一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得装置执行如本申请实施例中的方法。

20 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

25

本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可

30

提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

- 5        这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

- 10       这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

- 15       尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

- 20       最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

- 25       以上对本申请所提供的栈溢出的处理方法及装置进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

## 权 利 要 求 书

1.一种栈溢出处理的方法，其特征在于，所述方法包括：

采用内存管理器件检测指定栈是否发生栈溢出；

当检测到所述指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

5        2.根据权利要求1所述的方法，其特征在于，在所述采用所述内存管理器件检测指定栈是否发生栈溢出的步骤之前，还包括：

获取所述指定栈的栈信息，所述栈信息包括所述指定栈的起始地址以及栈大小；

基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

采用所述内存管理器件，设置所述栈底地址的访问权限。

10       3.根据权利要求2所述的方法，其特征在于，所述指定栈包括任务栈，所述获取所述指定栈的栈信息的步骤包括：

当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

4.根据权利要求2所述的方法，其特征在于，所述指定栈包括中断栈，所述获取所述指定栈的栈信息的步骤包括：

15       从编译链接脚本程序中获取所述中断栈的栈信息。

5.根据权利要求2-4任一项所述的方法，其特征在于，所述采用所述内存管理器件检测指定栈是否发生栈溢出的步骤包括：

当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出。

6.根据权利要求1-4任一项所述的方法，其特征在于，还包括：

20       获取所述栈溢出对应的上下文信息；

基于所述上下文信息，进行栈溢出问题排查。

7.根据权利要求1所述的方法，其特征在于，所述内存管理器件包括内存保护单元MPU或内存管理单元MMU。

8.一种栈溢出处理的装置，其特征在于，所述装置包括：

25       栈溢出检测模块，用于采用内存管理器件检测指定栈是否发生栈溢出；

中断处理模块，用于当检测到所述指定栈发生栈溢出时，由所述内存管理器件触发内存访问中断。

9.根据权利要求8所述的装置，其特征在于，还包括：

30       栈信息获取模块，用于获取所述指定栈的栈信息，所述栈信息包括所述指定栈的起始地址以及栈大小；

栈底地址确定模块，用于基于所述指定栈的起始地址以及栈大小，确定所述指定栈的栈底地址；

访问权限设置模块，用于采用所述内存管理器件，设置所述栈底地址的访问权限。

10.根据权利要求 9 所述的装置，其特征在于，所述指定栈包括任务栈，所述栈信息  
5 获取模块还用于：

当检测到所述任务栈进行任务切换时，获取所述任务栈的栈信息。

11.根据权利要求 9 所述的装置，其特征在于，所述指定栈包括中断栈，所述栈信息  
获取模块还用于：

从编译链接脚本程序中获取所述中断栈的栈信息。

10 12.根据权利要求 9-11 任一项所述的装置，其特征在于，所述栈溢出检测模块还用于：

当检测到对栈底的访问操作时，判定所述指定栈发生栈溢出。

13.根据权利要求 8-11 任一项所述的装置，其特征在于，还包括：

上下文信息获取模块，用于获取所述栈溢出对应的上下文信息；

15 问题排查模块，用于基于所述上下文信息，进行栈溢出问题排查。

14.根据权利要求 8 所述的装置，其特征在于，所述内存管理器件包括内存保护单元  
MPU 或内存管理单元 MMU。

15.一种装置，其特征在于，包括：

一个或多个处理器；和

20 其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，  
使得所述装置执行如权利要求 1-7 一个或多个的方法。

16.一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使  
得装置执行如权利要求 1-7 一个或多个的方法。

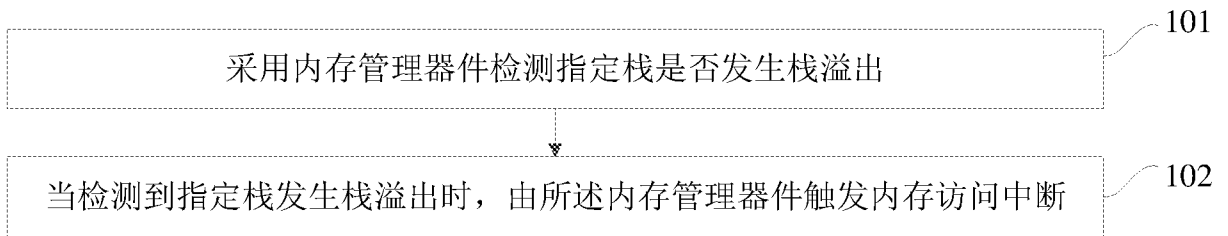


图 1

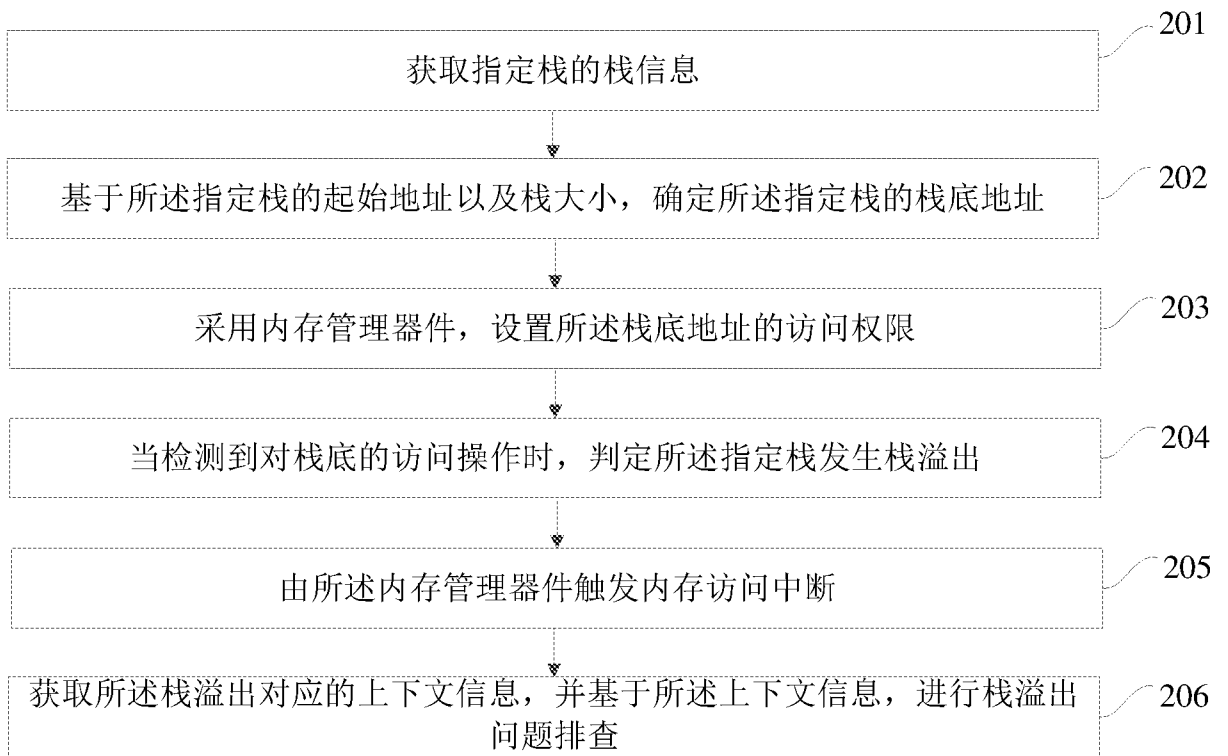


图 2

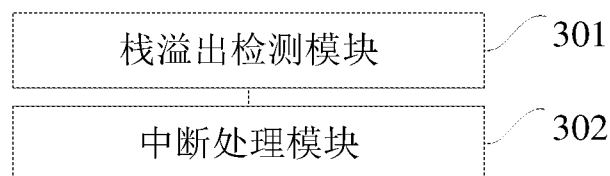


图 3

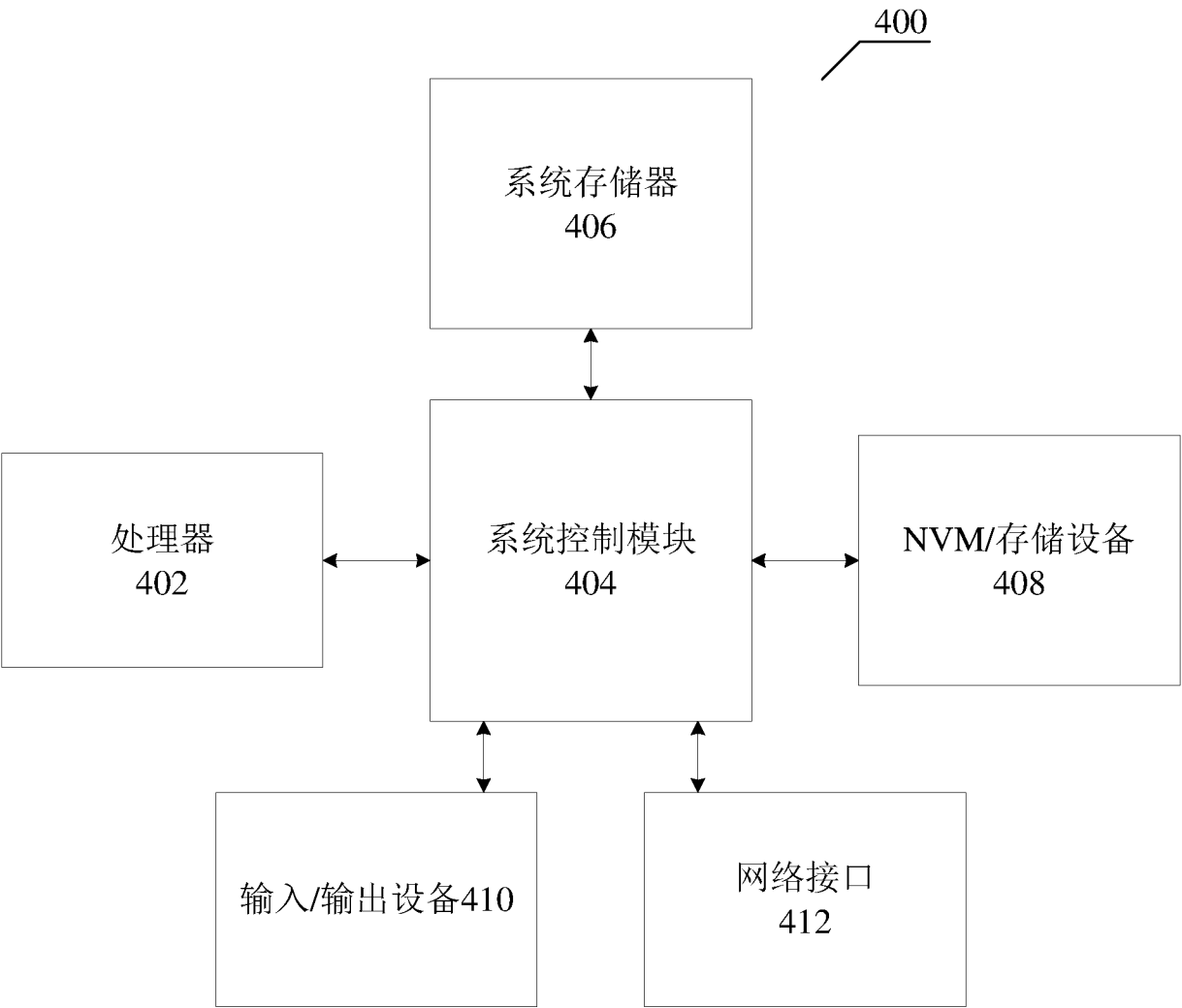


图 4

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/092153

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 11/07(2006.01)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)

G06F

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)

CNABS, CNTXT, CNKI, SIPOABS, DWPI, USTXT: 栈, 溢出, 内存管理, MMU, 中断, 访问, 写, 读, stack, overflow, memory management, interrupt, access, write, read

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                      | Relevant to claim No. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 101290596 A (ZTE CORPORATION) 22 October 2008 (2008-10-22)<br>description, page 4, paragraphs 3-6, and figures 1-3                                   | 1-16                  |
| X         | CN 101154180 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 02 April 2008 (2008-04-02)<br>description, page 4, paragraph 3 to page 6, paragraph 7 | 1-16                  |
| A         | CN 104714834 A (AERONAUTICAL COMPUTING TECHNIQUE RESEARCH INSTITUTE) 17 June 2015 (2015-06-17)<br>entire document                                       | 1-16                  |
| A         | CN 104679645 A (AVIC AEROENGINE CONTROL RESEARCH INSTITUTE) 03 June 2015 (2015-06-03)<br>entire document                                                | 1-16                  |



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

17 September 2018

Date of mailing of the international search report

30 September 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China  
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing  
100088  
China

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2018/092153**

| Patent document<br>cited in search report |           |   | Publication date<br>(day/month/year) | Patent family member(s) |           |   | Publication date<br>(day/month/year) |
|-------------------------------------------|-----------|---|--------------------------------------|-------------------------|-----------|---|--------------------------------------|
| CN                                        | 101290596 | A | 22 October 2008                      | None                    |           |   |                                      |
| CN                                        | 101154180 | A | 02 April 2008                        | CN                      | 101154180 | B | 12 May 2010                          |
| CN                                        | 104714834 | A | 17 June 2015                         | CN                      | 104714834 | B | 12 January 2018                      |
| CN                                        | 104679645 | A | 03 June 2015                         | None                    |           |   |                                      |

## 国际检索报告

国际申请号

PCT/CN2018/092153

## A. 主题的分类

G06F 11/07(2006.01)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)

G06F

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))

CNABS, CNTXT, CNKI, SIPOABS, DWPI, USTXT: 栈, 溢出, 内存管理, MMU, 中断, 访问, 写, 读, stack, overflow, memory management, interrupt, access, write, read

## 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    | CN 101290596 A (中兴通讯股份有限公司) 2008年 10月 22日 (2008 - 10 - 22)<br>说明书第4页第3-6段、图1-3 | 1-16    |
| X    | CN 101154180 A (大唐移动通信设备有限公司) 2008年 4月 2日 (2008 - 04 - 02)<br>说明书第4页第3段-第6页第7段 | 1-16    |
| A    | CN 104714834 A (中国航空工业集团公司第六三一研究所) 2015年 6月 17日 (2015 - 06 - 17)<br>全文         | 1-16    |
| A    | CN 104679645 A (中国航空工业集团公司航空动力控制系统研究所) 2015年 6月 3日 (2015 - 06 - 03)<br>全文      | 1-16    |

☐ 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

“&amp;” 同族专利的文件

国际检索实际完成的日期

2018年 9月 17日

国际检索报告邮寄日期

2018年 9月 30日

ISA/CN的名称和邮寄地址

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

冯慧萍

电话号码 62411838

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2018/092153

| 检索报告引用的专利文件 |           |   | 公布日<br>(年/月/日) | 同族专利 |           |   | 公布日<br>(年/月/日) |
|-------------|-----------|---|----------------|------|-----------|---|----------------|
| CN          | 101290596 | A | 2008年 10月 22日  | 无    |           |   |                |
| CN          | 101154180 | A | 2008年 4月 2日    | CN   | 101154180 | B | 2010年 5月 12日   |
| CN          | 104714834 | A | 2015年 6月 17日   | CN   | 104714834 | B | 2018年 1月 12日   |
| CN          | 104679645 | A | 2015年 6月 3日    | 无    |           |   |                |

表 PCT/ISA/210 (同族专利附件) (2015年1月)