# (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
2016 年 8 月 18 日 (18.08.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/127555 A1



(51) 国际专利分类号:
*G06F 21/56* (2013.01)

(21) 国际申请号: PCT/CN2015/083522

(22) 国际申请日: 2015 年 7 月 8 日 (08.07.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510064799.5 2015 年 2 月 9 日 (09.02.2015) CN



(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **李金明 (LI, Jinming)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **陈焰 (CHEN, Yan)**; 中国浙江省杭州市西湖区浙大路 38 号则通楼 503 室, Zhejiang 310027 (CN)。 **胡成臣 (HU, Chengchen)**; 中国陕西省西安市咸宁西路 28 号西安交通大学, Shaanxi 710049 (CN)。

(74) 代理人: **北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.)**; 中国北京市海淀区丹棱街 16 号海兴大厦 C 座 1108, Beijing 100080 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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。

(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)。


[见续页]

(54) **Title**: METHOD AND CONTROLLER FOR CONTROLLING APPLICATION PERMISSIONS

(54) **发明名称** : 控制应用程序权限的方法及控制器

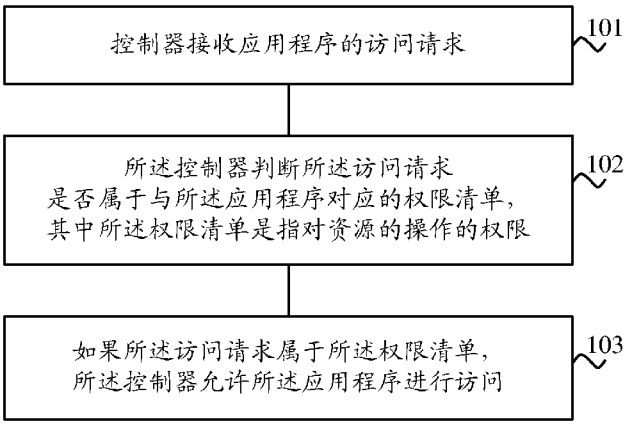


图1

101 CONTROLLER RECEIVES ACCESS REQUEST OF APPLICATION
102 CONTROLLER DETERMINES WHETHER ACCESS REQUEST BELONGS TO PERMISSIONS LIST CORRESPONDING TO APPLICATION, PERMISSIONS LIST REFERRING TO PERMISSIONS FOR OPERATION OF RESOURCE
103 IF ACCESS REQUEST BELONGS TO PERMISSIONS LIST, CONTROLLER ALLOWS APPLICATION TO CARRY OUT ACCESS


(57) **Abstract**: Provided is a method for controlling application permissions; the present method is used in the field of SDN and comprises: a controller receiving an access request of an application (101); said controller determining whether said access request belongs to a permissions list corresponding to said application, said permissions list referring to permissions for operation of a resource (102); if said access request belongs to the permissions list, said controller allowing said application to carry out access (103). In the present method for controlling application permissions, the controller determines whether the access request of the application belongs to a permissions list corresponding to the application; thus the access permissions of the application are restricted according to the permissions list, and in turn, malicious attacks by the application are prevented and the security of the network is safeguarded.

(57) **摘要**: 一种控制应用程序权限的方法，本方法应用于 SDN 领域，包括：控制器接收应用程序的访问请求(101)，所述控制器判断所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限(102)；如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问(103)。本控制应用程序权限的方法中，控制器判断应用程序的访问请求是否属于与该应用程序对应的权限清单，这样根据权限清单限制该应用程序的访问权限，进而能够避免应用程序的恶意攻击，保障网络安全。


WO 2016/127555 A1

**本国际公布**:

— 包括国际检索报告(条约第 21 条(3))。

# 控制应用程序权限的方法及控制器

## 技术领域

本发明实施例涉及通信领域，并且更具体地，涉及一种控制应用程序权限的方法及控制器。

## 背景技术

软件定义网络（Software Define Network，SDN）是一种控制和转发相分离的网络架构，将网络的控制功能集中在控制器上，并在控制器的上层部署应用程序（Application，APP）。这样，上层的应用程序可以通过控制器实现对网络的访问。

但是，由于应用程序的来源众多，且控制器无法获知应用程序的来源是否可靠，这样容易导致非安全的应用程序对控制器的攻击，并造成对网络的恶意的破坏，从而可能会带来网络安全威胁。

## 发明内容

本发明实施例提供一种控制应用程序权限的方法，能够避免应用程序的恶意攻击，保障网络安全。

第一方面，提供了一种控制应用程序权限的方法，包括：控制器接收应用程序的访问请求；所述控制器判断所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限；如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问。

结合第一方面，在第一方面的第一种可能的实现方式中，在所述控制器接收应用程序的访问请求之前，还包括：

所述控制器接收所述应用程序发送的权限请求；

所述控制器根据所述权限请求，生成与所述应用程序对应的所述权限清单。

结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述根据所述权限请求，生成与所述应用程序对应的所述权限清单，包括：

根据所述权限请求，采用权限过滤器，生成所述权限清单；

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的应用程序接口 API 调用的一个属性维度的过滤表达式。

结合上述第一方面的任一种可能的实现方式，在第一方面的第三种可能的实现方式中，所述根据所述权限请求，生成与所述应用程序对应的所述权限清单，包括：根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围；当确定所述权限请求合法时，生成所述权限清单。

结合第一方面或者上述第一方面的任一种可能的实现方式，在第一方面的第四种可能的实现方式中，

所述判断所述访问请求是否属于与所述应用程序对应的权限清单，包括：

将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；

判断所述析取范式是否属于所述合取范式；

所述如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问，包括：

如果所述析取范式属于所述合取范式，所述控制器允许所述应用程序进行访问。

第二方面，提供了一种控制器，包括：

接收单元，用于接收应用程序的访问请求；

判断单元，用于判断所述接收单元接收的所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限；

执行单元，用于在所述判断单元确定所述访问请求属于所述权限清单时，允许所述应用程序进行访问。

结合第二方面，在第二方面的第一种可能的实现方式中，所述接收单元，还用于接收所述应用程序发送的权限请求；所述执行单元，还用于根据所述权限请求，生成与所述应用程序对应的所述权限清单。

结合第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述执行单元，具体用于：根据所述权限请求，采用权限过滤器，生成所述权限清单；

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过

滤器中的一个原子过滤器用于表示对所述控制器的应用程序接口 API 调用的一个属性维度的过滤表达式。

结合第二方面的任意一种可能的实现方式，在第二方面的第三种可能的实现方式中，所述执行单元，具体用于：

根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围；当确定所述权限请求合法时，生成所述权限清单。

结合第二方面或者上述第二方面的任意一种可能的实现方式，在第二方面的第四种可能的实现方式中，

所述判断单元，具体用于：将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；判断所述析取范式是否属于所述合取范式；

所述执行单元，具体用于：在所述判断单元确定所述析取范式属于所述合取范式时，允许所述应用程序进行访问。

本发明实施例中，控制器判断应用程序的访问请求是否属于与该应用程序对应的权限清单，这样根据权限清单限制该应用程序的访问权限，进而能够避免应用程序的恶意攻击，保障网络安全。

## 附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明一个实施例的控制应用程序权限的方法的流程图。

图 2 是本发明另一个实施例的控制应用程序权限的方法的流程图。

图 3 是本发明一个实施例的控制器的结构框图。

图 4 是本发明另一个实施例的控制器的结构框图。

## 具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创

造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

图 1 是本发明一个实施例的控制应用程序权限的方法的流程图。图 1 所示的方法包括:

101，控制器接收应用程序的访问请求。

102，所述控制器判断所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限。

103，如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问。

本发明实施例中，控制器判断应用程序的访问请求是否属于与该应用程序对应的权限清单，这样根据权限清单限制该应用程序的访问权限，进而能够避免应用程序的恶意攻击，保障网络安全。

可理解，本发明实施例所示的方法应用于 SDN 领域，相应地，本发明实施例所示的控制器是指 SDN 中的控制器。

可选地，控制器中存储有与所述应用程序对应的权限清单。该权限清单可以是由管理员进行预配置的，或者是由控制器根据自身所开放的权限范围进行预配置的。

应注意，本发明对权限清单的形式不作限定。例如，权限清单可以是清单的形式，或者可以是列表的形式，或者也可以是集合的形式，等等。本发明实施例不应该将权限清单的名称作为对其形式的限定。

或者，可选地，在 101 之前，还可以包括：控制器生成与所述应用程序对应的权限清单。作为一例，控制器可以接收所述应用程序发送的权限请求；根据所述权限请求，生成与所述应用程序对应的所述权限清单。

本发明实施例中，应用程序对控制器的访问包括对资源的访问，其中，所述资源包括以下中的至少一种：流表、拓扑、统计信息和错误、组表、流量整形、操作系统、入包（Packet_in）和出包（Packet_out）。如表一所示。对资源的操作可以是读或写或事件回调。

本发明实施例中，权限清单可以用于表示对资源的操作的权限。如表一所示的第三列包括本发明实施例所定义的权限。

表一

| 资源 | 操作 | 权限 |
|---|---|---|
| 流表 | 读 | read flow table |
| | 写 | insert flow |
| | | delete flow |
| | 事件回调 | flow event |
| 拓扑 | 读 | visible topology |
| | 写 | modify topology |
| | 事件回调 | topology event |
| 统计信息和错误 | 读 | read statistics |
| | 事件回调 | error event |
| Packet_in 和 Packet_out | 读 | read pkt in payload |
| | 写 | send pkt out |
| | 事件回调 | pkt in event |
| 组表 | 读 | read group table entry |
| | 写 | insert group table entry |
| | | delete group table entry |
| | 事件回调 | flow event |
| 流量整形 | 读 | read meter table |
| | 写 | Insert meter table entry |
| | | delete meter table entry |
| | 事件回调 | flow event |
| 操作系统 | | file system access |
| | | process runtime access |
| | | network access |

为了对表一所示的权限的范围进行限定，本发明实施例定义了权限语言，具体地，权限语言及其含义如下所述:

PERM: 声明权限的名称;

LIMITING: 声明开始限定权限;

AND: 与操作，二元操作符，两个均为真时才为真;

OR：或操作，二元操作符，只要有一个为真时即为真；

NOT：否定操作，一元操作符，表示当前的否定；

IP_SRC（V6 或 V4）：IP 源地址，其值可以是一个整型变量，也可以是一个 IP 格式的字符串；

IP_DST（V6 或 V4）：IP 目的地址，其值可以是一个整型变量，也可以是一个 IP 格式的字符串；

TCP_SRC：TCP 源地址，其值可以是一个整型变量，也可以是一个 IP 格式的字符串；

TCP_DST：TCP 目的地址，其值可以是一个整型变量，也可以是一个 IP 格式的字符串；

MASK：子网掩码，其值可以是一个整型变量，也可以是一个 IP 格式的字符串；

WILDCARD：通配符匹配；

DROP：丢弃当前包；

FORWARD：转发当前包；

MODIFY：修改当前包，具体使用时需要限定可以修改的域；

OWN_FLOWS：所有权权限，只允许查看和修改 APP 自身创建的流表规则；

ALL_FLOWS：所有权权限，允许查看和修改所有的流表规则；

GROUP_FLOW：所有权权限，只允许查看和修改 APP 自身创建的组表规则；

ALL_GROUP_FLOWS：所有权权限，允许查看和修改所有的组表规则；

METER_FLOW：所有权权限，只允许查看和修改 APP 自身创建的 meter_table 规则；

ALL_METER_FLOWS：所有权权限，允许查看和修改所有的 meter_table 规则；

MAX_PRIORITY：限制可以创建或修改的规则的最大优先级；

MIN_PRIORITY：限制可以创建或修改的规则的最小优先级；

MAX_RULE_COUNT：限制在一个交换机上的规则的数目；

FROM_PKT_IN：只允许在回复 packet-in 消息时对外发送数据包；

ARBITRARY：允许在任何情况下对外发送数据包；

SWITCH: 限定可以操作的交换机，具体使用时可以是一个或者一组交换机，同时与 LINK 合用，限定可以操作的链路;

LINK: 限定可以操作的链路，具体使用时可以是一条或一组链路;

ALL_SWITCHES: 允许操作所有的交换机;

BORDER_SWITCHES: 允许操作边界交换机;

VIRTUAL: 限定可以操作的虚拟交换机;

SINGLE_BIG_SWITCH: 限定为单个虚拟的交换机;

ALL_ADJACENT_LINKS: 限定为所有与该交换机直接相邻的链路;

PATHS_AS_LINKS: 限定为该交换机直接或间接相邻的链路;

EVENT_INTERCEPTION: 允许监听截获回调事件;

MODIFY_EVENT_ORDER: 允许修改回调事件被 APP 处理的顺序;

FLOW_LEVEL: 允许查看流级别的统计信息;

PORT_LEVEL: 允许查看端口级别的统计信息;

SWITCH_LEVEL: 允许查看交换机级别的统计信息;

这样，可以利用上述权限语言，来描述和定义应用程序的访问权限。

具体地，本发明实施例中，控制器在生成权限清单时，可以先根据安全约束判断权限请求是否合法; 当确定所述权限请求合法时，生成所述权限清单。其中，所述安全约束用于表示所述控制器所开放的权限的范围。这里，控制器所开放的权限的范围可以是由管理员预先定义并配置在该控制器上的。

可理解，若控制器确定所述权限请求不合法时，不生成权限清单，进而不允许该应用程序进行访问。

本发明实施例中，应用程序的权限请求可以理解为一种粗略的权限清单，是一种全有或全无的授权方式，即全部通过或者全部不通过，粒度较粗。那么，相应地，控制器所生成的权限清单可以理解为一种细化后的权限清单，用于限制权限的范围。

进一步地，控制器生成权限清单可以包括: 根据所述权限请求，采用预定义的权限语法规则，生成所述权限清单。

具体地，控制器可以根据权限请求以及所述安全约束，采用预定义的权限语法规则，生成所述权限清单。

这里，所述预定义的权限语法规则可以表示为权限过滤器。那么，可理

解，控制器生成权限清单可以包括：控制器根据所述权限请求，采用权限过滤器，生成所述权限清单。或者，控制器可以根据权限请求以及所述安全约束，采用权限过滤器，生成所述权限清单。

本发明实施例中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的应用程序接口（Application Interface，API）调用的一个属性维度的过滤表达式。

原子过滤器可以为过滤表达式的构建块。应用程序对控制器的 API 调用通常与一定数量的参数和运行时的属性相关联，例如流表项的匹配字段和目标交换机。原子过滤器可以根据 API 调用的特定属性维度划分 API 调用。不同的原子过滤器检查不同的属性维度，因此不同的原子过滤器是相互独立的。通常情况下，一个原子过滤器是一个包含特定属性的权限的子集。

应注意，本发明实施例对属性维度的划分方式不作限定，举例来说，可以按照如表一所示的资源确定属性维度。例如，属性维度可以包括：流、拓扑、事件回调、统计、组表和流量整形。

原子过滤器可以进一步包括：流过滤器、拓扑过滤器、事件回调过滤器、统计过滤器、组表过滤器和流量整形过滤器。具体地，这些过滤器的含义可以如下所述。

（a）、流过滤器：流过滤器作用于特定流参数的 API 调用。因此，流过滤器可以与权限管理中流表的资源相关联。流过滤器检查几种类型的输入。

具体地，可以将 API 调用时的参数与过滤器参数进行比较。过滤器参数值可为一个特定值或者一个范围，范围可以使用逐位掩码来表示。

例如：

PERM read_flow_table LIMITING

IP_DST 10.13.0.0 MASK 255.255.0.0

那么这个应用程序只能看到在特定子网的流表项。

此外，还可以提供对通配字段的检查。当与 read_flow_table 权限相关联时，应用程序可以看到的流表项的匹配字段的位数。当与 insert_flow 或 delete_flow 权限相关联时，可以确保应用程序产生恰当的通配位。例如，一个只处理数据包低 8 位 IP 目的地址的负载平衡 APP 应具有以下权限：

PERM insert_flow LIMITING

WILDCARD IP_DST 255.255.255.0

表示任何新插入的规则的IP目的地址的高24位必须是通配符，只有该IP目的地址的低8位的可以被指定。因此任何数据包的IP目的地址的高24为都不能被该APP修改，而只有该IP目的地址的低8位可以被该APP进行修改。

本发明实施例中，流过滤器可以进一步包括：动作过滤器、所有权过滤器、优先级过滤器、表大小过滤器和包流出过滤器。

其中，动作过滤器标识的是在一个特定域丢弃、转发和修改流的行为。所有权过滤器识别和跟踪所有现有流的发行人。优先级过滤器限制了一个应用程序可以设置其流规则的最大/最小优先级值。表大小过滤器限制应用程序可以放到一个交换机的规则的最大数量。包流出过滤器，如果设置为FROM_PKT_IN，可以防止应用程序发行任意的数据层的数据包（即不是回应packet_in的数据包）。

可理解，属性维度也可以包括动作、所有权、优先级、表大小和包流出。

可见，本发明实施例中，流过滤器可以限制流表的可见性或操作性。

（b）、拓扑过滤器：拓扑过滤器检查一个应用程序看到并操作的交换机和链接。拓扑过滤器可以工作在物理拓扑结构，或者也可以工作在所创建的一个虚拟拓扑结构。

本发明实施例中，拓扑过滤器可以进一步包括：物理拓扑过滤器和虚拟拓扑过滤器。

其中，物理拓扑过滤器可以将物理交换机和链路的子集暴露给一个应用程序。

例如：

PERM visible_topology LIMITING

SWITCH BORDER_SWITCHES LINK PATHS_AS_LINKS

允许应用程序查看包括拓扑结构中所有的边界交换机和他们之间的每对路径。

虚拟拓扑过滤器可以将整个网络看成一个大型交换机，或者将整个网络分割成多个虚拟网络。

例如：

PERM visible_topology LIMITING

VIRTUAL SINGLE_BIG_SWITCH LINK ALL_ADJACENT_LINKS

允许应用程序将网络拓扑结构看作一个单一的大型交换机。

可理解，属性维度也可以包括物理拓扑和虚拟拓扑。

（c）、事件回调过滤器：事件回调过滤器可以用于检查在事件回调的过程中两个特定的应用程序行为，分别为 1）拦截回调事件，2）修改回调事件被应用程序处理的顺序。

本发明实施例中，事件回调过滤器可以进一步包括：事件侦听过滤器和事件顺序过滤器。

其中，事件侦听过滤器可以检查一个应用程序是否可以拦截回调事件，即防止事件被其他应用程序处理。事件顺序过滤器可以检查 API 调用是否尝试修改回调事件被应用程序处理的顺序。

可理解，属性维度也可以包括事件侦听和事件顺序。

（d）、统计过滤器：可以限制一个应用程序的可见数据到三个级别中的一个或几个，其中，三个级别包括：流级（FLOW_LEVEL）、端口级（PORT_LEVEL）和交换机级（SWITCH_LEVEL）。可见，统计过滤器是唯一有效地作用在 read_statistics 权限上的过滤器。

（e）、组表过滤器：可以设置 APP 是否可以下发组表的权限。在开放流（openflow）中，组表可用于组播、多路径、故障恢复等。

例如：

PERM insert_group_table_entry LIMITING

IP_DST 10.13.0.0 MASK 255.255.0.0

限制只能对特定的子网才可以插入（insert）组表项（group_table_entry）

（f）、流量整形过滤器：可以限制 APP 只有对特定的交换机的特定端口才可以进行流量整形。在 openflow 中，控制器可对网络中的流进行整形，如将 10M 的端口限速为 3M。

例如：

PERM insert_meter_table_entry LIMITING SWITCH 1

限制只有对交换机 1 才可以插入 meter 表项。

本发明实施例中，当权限过滤器包括多个原子过滤器时，所述多个原子过滤器之间通过逻辑运算符进行连接。

其中，逻辑运算符包括和（AND）、或（OR）、否（NOT）。

例如，可以授予 APP read_flow_table 的权限，但只限制到先前由该 APP

发布的流，或影响子网 10.13.0.0/16:

PERM read_flow_table LIMITING OWN_FLOWSOR

IP_SRC 10.13.0.0 MASK 255.255.0.0 OR IP_DST 10.13.0.0 MASK 255.255.0.0

这样，本发明实施例中，控制器可以利用权限过滤器生成权限清单。

例如:

ERM pkt_in LIMITTING EVENT_INTERCEPTION AND FROM_PKT_IN

允许监听截获回调事件，允许在回复 pkt-in 消息的前提下发送 pkt-out 消息。

再例如:

PERM pkt_in LIMITTING EVENT_INTERCEPTION AND ARBITRARY

允许监听截获回调事件，允许在任何情况下发送 pkt-out 消息。

具体地，本发明实施例中，控制器中可以包括约束引擎，并由该约束引擎生成权限清单。

可理解，与应用程序对应的权限清单是指：控制器对该应用程序所开放的一系列权限范围的集合。

在图 1 所示的实施例中，101 中的访问请求可以是 APP 对 API 的访问请求。那么，在 101 之后，控制器可以根据该对 API 的访问请求对应到特定的权限上。

具体地，控制器中可以预存储有“API/权限”的对应关系，这样，控制器可以查找该对应关系，确定与访问请求所对应的权限。

举例来说，该对应关系可以如表二所示。

表二

| API | 对应的权限 |
|---|---|
| OFSwitchImpl.write(OFType.FLOW_MOD) | insert flow |
| addOFMessageListener | read pkt in payload |
| …… | …… |

相应地，可以理解，在 102 中，控制器判断访问请求是否属于权限清单，可以包括：控制器判断与访问请求所对应的权限是否属于权限清单。

102 中，如果访问请求是对 API 调用的一个属性维度的访问请求，那么 102 可以与权限清单中的对应的原子过滤器的过滤表达式进行比较。

也就是说，原子过滤器可以直接比较。例如，同一种原子过滤器，需要比较具体参数，如对应统计过滤器，需要比较属于 FLOW_LEVEL、PORT_LEVEL 或者 SWITCH_LEVEL。

不同种类的原子过滤器显然不相同。对于不同种类的原子过滤器，判断包含的规则也不完全相同，如统计过滤器 SWITCH_LEVEL 包含了 FLOW_LEVEL 和 PORT_LEVEL，而 PORT_LEVEL 包含了 FLOW_LEVEL。而流过滤器中的 action 过滤中 DROP 和 FORWARD 就不能互相包含。

应注意，本发明实施例中，对原子过滤器之间的比较的方式不再赘述。

如果访问请求是对 API 调用的多个属性维度的访问请求，那么 102 可以与权限清单中的对应的由逻辑运算符连接的多个原子过滤器的过滤表达式进行比较。那么，102 可以包括：将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；判断所述析取范式是否属于所述合取范式。

例如：假设权限清单可以表示为 A，访问请求可以表示为 B。那么，判断访问请求是否属于权限清单可以等价为，判断 A 是否包含 B。

第一步，将 A 转化为合取范式（a and b and c and …），将 B 转化为析取范式（x or y or z or …）。

其中，转化过程是通过利用离散数学中命题公式的双重否定律、德摩根定律和分配律等来完成的。

（1）将 A 转化为合取范式。

先运用否定律，递归分解 not 操作。

例如：not (a and b) => (not a) or (not b)。

再运用分配律，递归分解 or 操作。

例如：(a and b) or c => (a or c) and (b or c)。

（2）将 B 转化为析取范式。

先运用否定律，递归分解 not 操作。

例如：not (a or b) => (not a) and (not b)。

再运用分配率，递归分解 or 操作。

例如：(a or b) and c => (a and c) or (b and c)。

应注意，本发明实施例中，将 A 转化为合取范式，将 B 的转化为析取

范式的方式可以参见现有技术，为避免重复，这里不再赘述。

第二步，判断合取范式是否包含析取范式。

具体地，需判断合取范式的每一个子句是否都包含析取范式的每一个子句。

例如，假设合取范式表示为 a1 and a2 and a3 and ... 的形式，析取范式表示为 x1 or x2 or x3 ... 的形式，那么，需判断是否满足 ai 包含 xj。其中，i=1,2,3...； j=1,2,3...。

应注意，若 a1=a11 or a12，x1=x11 and x12。那么，在判断 a1 是否包括 x1 时，需要满足 a11 包括 x11 且 a11 包括 x12；或者 a12 包括 x11 且 a12 包括 x12。

应注意，本发明实施例中，关于判断合取范式是否包含析取范式的方式，可以参见与逻辑判断有关的现有技术，为避免重复，这里不再赘述。

作为一例，在 102 中，假设权限清单可以表示为 A，访问请求可以表示为 B。并且，A 和 B 可以表示如下。

A= {
PERM read_statistics LIMITING SWITCH_LEVEL
PERM network_access LIMITING
IP_DST 192.168.0.0 MASK 255.255.0.0
}

B = {
PERM read_statistics LIMITING PORT_LEVEL
PERM network_access LIMITING
IP_DST 192.168.1.0 MASK 255.255.255.0
or IP_DST 192.168.2.0 MASK 255.255.255.0
}

那么，判断 B 是否属于 A，即判断是否满足 B < = A。

首先可以将 A 转化为合取范式，即：

A => (SWITCH_LEVEL) and (IP_DST 192.168.0.0 MASK 255.255.0.0);

将 B 转化为析取范式，即：

B => (PORT_LEVEL and ((IP_DST 192.168.1.0 MASK 255.255.255.0)) or (PORT_LEVEL and ((IP_DST 192.168.2.0 MASK 255.255.255.0))。

然后，便可以通过判断合取范式是否包含析取范式，来确定 A 是否包含 B，进而确定访问请求是否属于权限清单。

具体地，本发明实施例中，控制器中可以包括权限引擎，并由该权限引擎执行 102 中的判断过程。

这样，控制器通过判断访问请求是否属于权限清单，来判断应用程序的访问是否合法。如果确定访问请求属于权限清单，便可以执行 103。

图 2 是本发明实施例的控制应用程序权限的方法的流程图。其中，如果 102 中控制器经过判断之后，确定访问请求不属于权限清单，可以进一步执行 104，即，控制器不允许该应用程序进行访问。

或者，也可以理解为，若控制器确定访问请求不属于权限清单，可以认为该应用程序的访问不合法，即该应用程序可能存在对控制器进行恶意攻击的可能性，便阻止该应用程序的进一步访问，进而能够保障网络的安全。

图 3 是本发明一个实施例的控制器的结构框图。图 3 所示的控制器 300 包括接收单元 301、判断单元 302 和执行单元 303。

接收单元 301，用于接收应用程序的访问请求。

判断单元 302，用于判断接收单元 301 接收的所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限。

执行单元 303，用于在判断单元 302 确定所述访问请求属于所述权限清单时，允许所述应用程序进行访问。

本发明实施例中，控制器判断应用程序的访问请求是否属于与该应用程序对应的权限清单，这样根据权限清单限制该应用程序的访问权限，进而能够避免应用程序的恶意攻击，保障网络安全。

本发明实施例中，应用程序对控制器的访问包括对资源的访问，其中，所述资源包括以下中的至少一种：流表、拓扑、统计信息和错误、组表、流量整形、操作系统、入包（Packet_in）和出包（Packet_out）。对资源的操作可以是读或写或事件回调。

可选地，控制器中存储有与所述应用程序对应的权限清单。该权限清单可以是由管理员进行预配置的，或者是由控制器根据自身所开放的权限范围进行预配置的。

可选地，作为一个实施例，接收单元 301，还用于接收所述应用程序发

送的权限请求；执行单元 303，还用于根据所述权限请求，生成与所述应用程序对应的所述权限清单。

本发明实施例中，权限清单可以用于表示对资源的操作的权限。如前述的表一所示的第三列包括本发明实施例所定义的权限。

具体地，执行单元 303，用于根据所述权限请求，采用权限过滤器，生成所述权限清单。

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的 API 调用的一个属性维度的过滤表达式。

可理解，所述权限过滤器可以包括多个原子过滤器，并且多个原子过滤器之间通过逻辑运算符连接。

可选地，作为另一个实施例，执行单元 303 具体用于根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围；当确定所述权限请求合法时，生成所述权限清单。

可选地，作为另一个实施例，判断单元 302，具体用于：将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；判断所述析取范式是否属于所述合取范式。执行单元 303，具体用于：在判断单元 302 确定所述析取范式属于所述合取范式时，允许所述应用程序进行访问。

控制器 300 能够用于实现前述图 1 或图 2 的实施例中由控制器执行的方法，为避免重复，这里不再赘述。

图 4 是本发明另一个实施例的控制器的结构框图。图 4 所示的控制器 400 包括处理器 401、接收器 402、发送器 403 和存储器 404。

接收器 402，用于接收应用程序的访问请求。

处理器 401，用于判断接收器 402 接收的所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单用于表示对资源的操作的权限。

处理器 401，还用于在确定所述访问请求属于所述权限清单时，允许所述应用程序进行访问。

本发明实施例中，控制器判断应用程序的访问请求是否属于与该应用程序对应的权限清单，这样根据权限清单限制该应用程序的访问权限，进而能够避免应用程序的恶意攻击，保障网络安全。

控制器 400 中的各个组件通过总线系统 405 耦合在一起，其中总线系统 405 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 4 中将各种总线都标为总线系统 405。

上述本发明实施例揭示的方法可以应用于处理器 401 中，或者由处理器 401 实现。处理器 401 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 401 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 401 可以是通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（Field Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 404，处理器 401 读取存储器 404 中的信息，结合其硬件完成上述方法的步骤。

可以理解，本发明实施例中的存储器 404 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（Synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）。本文描述的系统和方法的存储器 404 旨在包括但不限于这些和任意

其它适合类型的存储器。

可以理解，本发明实施例中的发送器 403 可以用于将处理器 401 的执行结果发送至与该控制器 400 进行通信的设备。例如，应用程序或者交换机等。

可以理解的是，本文描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路（Application Specific Integrated Circuits，ASIC）、数字信号处理器（Digital Signal Processing，DSP）、数字信号处理设备（DSP Device，DSPD）、可编程逻辑设备（Programmable Logic Device，PLD）、现场可编程门阵列（Field-Programmable Gate Array，FPGA）、通用处理器、控制器、微控制器、微处理器、用于执行本申请所述功能的其它电子单元或其组合中。

当在软件、固件、中间件或微码、程序代码或代码段中实现实施例时，它们可存储在例如存储部件的机器可读介质中。代码段可表示过程、函数、子程序、程序、例程、子例程、模块、软件分组、类、或指令、数据结构或程序语句的任意组合。代码段可通过传送和/或接收信息、数据、自变量、参数或存储器内容来稿合至另一代码段或硬件电路。可使用包括存储器共享、消息传递、令牌传递、网络传输等任意适合方式来传递、转发或发送信息、自变量、参数、数据等。

对于软件实现，可通过执行本文所述功能的模块（例如过程、函数等）来实现本文所述的技术。软件代码可存储在存储器单元中并通过处理器执行。存储器单元可以在处理器中或在处理器外部实现，在后一种情况下存储器单元可经由本领域已知的各种手段以通信方式耦合至处理器。

本发明实施例中，应用程序对控制器的访问包括对资源的访问，其中，所述资源包括以下中的至少一种：流表、拓扑、统计信息和错误、组表、流量整形、操作系统、入包（Packet_in）和出包（Packet_out）。对资源的操作可以是读或写或事件回调。

可选地，控制器中存储有与所述应用程序对应的权限清单。该权限清单可以是由管理员进行预配置的，或者是由控制器根据自身所开放的权限范围进行预配置的。

可选地，作为一个实施例，接收器 402，还用于接收所述应用程序发送的权限请求；处理器 401，还用于根据所述权限请求，生成与所述应用程序对应的所述权限清单。

本发明实施例中，权限清单可以用于表示对资源的操作的权限。如前述的表一所示的第三列包括本发明实施例所定义的权限。

具体地，处理器 401，用于根据所述权限请求，采用权限过滤器，生成所述权限清单。

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的 API 调用的一个属性维度的过滤表达式。

可理解，所述权限过滤器可以包括多个原子过滤器，并且多个原子过滤器之间通过逻辑运算符连接。

可选地，作为另一个实施例，处理器 401 具体用于根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围；当确定所述权限请求合法时，生成所述权限清单。

可选地，作为另一个实施例，处理器 401 具体用于：将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；判断所述析取范式是否属于所述合取范式。在确定所述析取范式属于所述合取范式时，允许所述应用程序进行访问。

控制器 400 能够用于实现前述图 1 或图 2 的实施例中由控制器执行的方法，为避免重复，这里不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间

的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器( Read-Only Memory, ROM )、随机存取存储器（Random Access Memory，RAM )、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

# 权利要求

1、一种控制应用程序权限的方法，其特征在于，包括:

控制器接收应用程序的访问请求;

所述控制器判断所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限;

如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问。

2、根据权利要求 1 所述的方法，其特征在于，在所述控制器接收应用程序的访问请求之前，还包括:

所述控制器接收所述应用程序发送的权限请求;

所述控制器根据所述权限请求，生成与所述应用程序对应的所述权限清单。

3、根据权利要求 2 所述的方法，其特征在于，所述根据所述权限请求，生成与所述应用程序对应的所述权限清单，包括:

根据所述权限请求，采用权限过滤器，生成所述权限清单;

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的应用程序接口 API 调用的一个属性维度的过滤表达式。

4、根据权利要求 2 或 3 所述的方法，其特征在于，所述根据所述权限请求，生成与所述应用程序对应的所述权限清单，包括:

根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围;

当确定所述权限请求合法时，生成所述权限清单。

5、根据权利要求 1 至 4 任一项所述的方法，其特征在于，

所述判断所述访问请求是否属于与所述应用程序对应的权限清单，包括:

将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式;

判断所述析取范式是否属于所述合取范式;

所述如果所述访问请求属于所述权限清单，所述控制器允许所述应用程序进行访问，包括:

如果所述析取范式属于所述合取范式，所述控制器允许所述应用程序进

行访问。

6、一种控制器，其特征在于，包括:

接收单元，用于接收应用程序的访问请求;

判断单元，用于判断所述接收单元接收的所述访问请求是否属于与所述应用程序对应的权限清单，其中所述权限清单是指对资源的操作的权限;

执行单元，用于在所述判断单元确定所述访问请求属于所述权限清单时，允许所述应用程序进行访问。

7、根据权利要求 6 所述的控制器，其特征在于，

所述接收单元，还用于接收所述应用程序发送的权限请求;

所述执行单元，还用于根据所述权限请求，生成与所述应用程序对应的所述权限清单。

8、根据权利要求 7 所述的控制器，其特征在于，所述执行单元，具体用于:

根据所述权限请求，采用权限过滤器，生成所述权限清单;

其中，所述权限过滤器包括至少一个原子过滤器，所述至少一个原子过滤器中的一个原子过滤器用于表示对所述控制器的应用程序接口 API 调用的一个属性维度的过滤表达式。

9、根据权利要求 7 或 8 所述的控制器，其特征在于，所述执行单元，具体用于:

根据安全约束判断所述权限请求是否合法，其中，所述安全约束用于表示所述控制器所开放的权限的范围;

当确定所述权限请求合法时，生成所述权限清单。

10、根据权利要求 6 至 9 任一项所述的控制器，其特征在于，

所述判断单元，具体用于：将所述访问请求转化为析取范式，并将所述权限清单转化为合取范式；判断所述析取范式是否属于所述合取范式;

所述执行单元，具体用于：在所述判断单元确定所述析取范式属于所述合取范式时，允许所述应用程序进行访问。

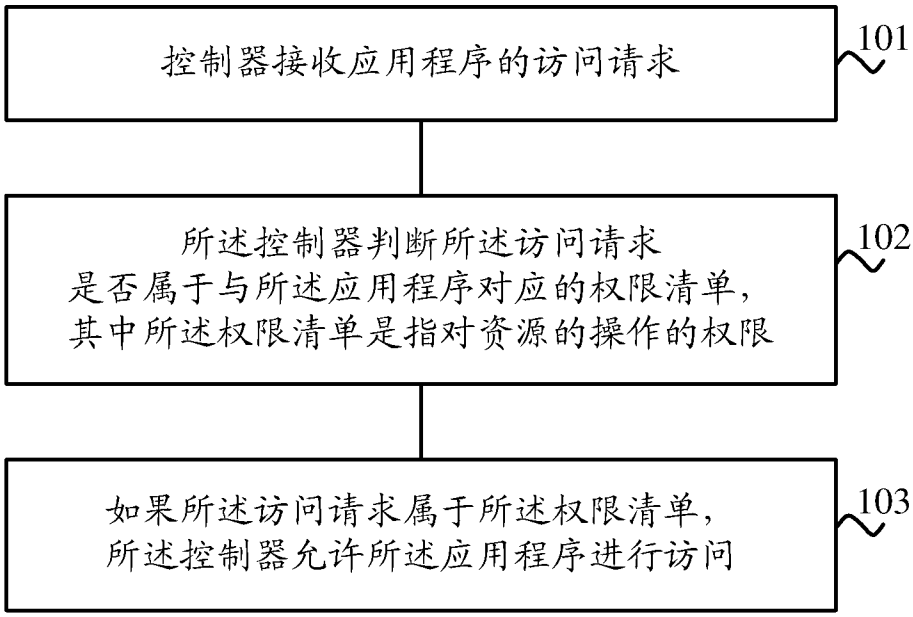
控制器接收应用程序的访问请求
101
所述控制器判断所述访问请求
是否属于与所述应用程序对应的权限清单，
其中所述权限清单是指对资源的操作的权限
102
如果所述访问请求属于所述权限清单，
所述控制器允许所述应用程序进行访问
103

图1

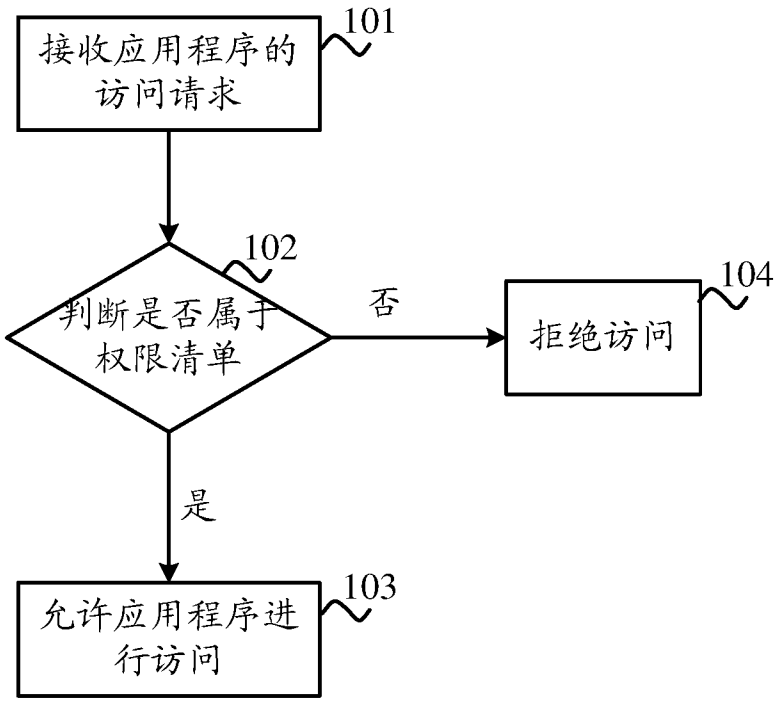
接收应用程序的访问请求
101
判断是否属于权限清单
102
否
拒绝访问
104
是
允许应用程序进行访问
103

图2

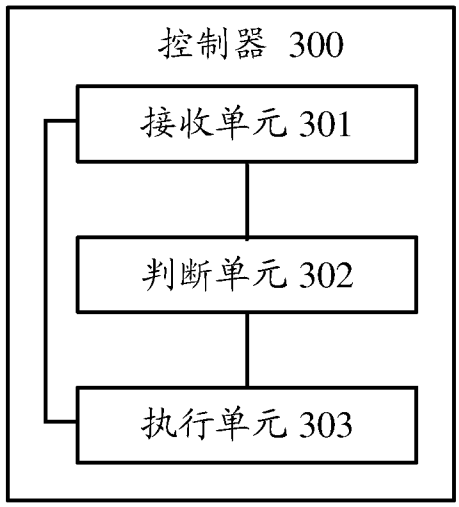
控制器 300
接收单元 301
判断单元 302
执行单元 303

图3

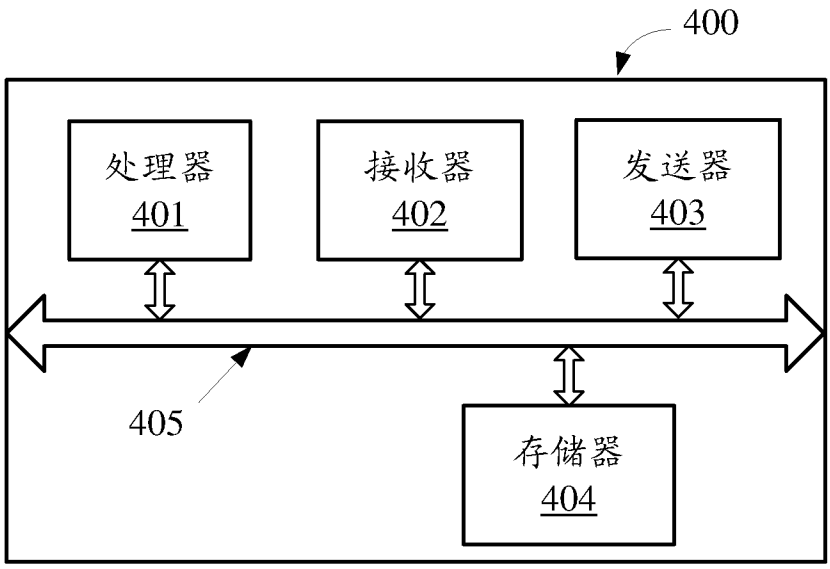
400
处理器
401
接收器
402
发送器
403
405
存储器
404

图4

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2015/083522**

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 21/56 (2013.01) 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)

CNPAT, WPI, EPODOC, CNKI: software-defined network, controller, authority, list, SDN, safety, match+, rule?, table

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 104113839 A (BLUEDON INFORMATION SECURITY TECHNOLOGIES CO., LTD.), 22 October 2014 (22.10.2014), description, paragraphs [0015]-[0029], and figures 1 and 3 | 1-10 |
| A | CN 103095701 A (ZTE CORP.), 08 May 2013 (08.05.2013), the whole document | 1-10 |
| A | US 2014/0359697 A1 (HANGZHOU H3C TECHNOLOGIES CO., LTD.), 04 December 2014 (04.12.2014), 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 |
|---|---|
| 24 August 2015 (24.08.2015) | **03 November 2015 (03.11.2015)** |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br>**WANG, Xiaofei**<br>Telephone No.: (86-10) **62414442** |

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
**PCT/CN2015/083522**

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN 104113839 A | 22 October 2014 | None | |
| CN 103095701 A | 08 May 2013 | None | |
| US 2014/0359697 A1 | 04 December 2014 | CN 104219218 A | 17 December 2014 |

# 国际检索报告

国际申请号 PCT/CN2015/083522

A. 主题的分类

G06F 21/56(2013.01)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）)

CNPAT, WPI, EPODOC, CNKI: 软件定义网络，控制器，权限，安全,列表,规则,匹配, SDN, safety, match+, rule?, table

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 104113839 A (蓝盾信息安全技术有限公司) 2014年 10月 22日 (2014-10-22)<br>说明书第[0015]段-[0029]段及附图1，3 | 1-10 |
| A | CN 103095701 A (中兴通讯股份有限公司) 2013年 5月 8日 (2013-05-08)<br>全文 | 1-10 |
| A | US 2014/0359697 A1 (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 2014年 12月 4日 (2014-12-04)<br>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 |
|---|---|
| 2015年 8月 24日 | 2015年 11月 3日 |

| ISA/CN的名称和邮寄地址 | 受权官员 |
|---|---|
| 中华人民共和国国家知识产权局(ISA/CN)<br>北京市海淀区蓟门桥西土城路6号<br>100088 中国<br>传真号 (86-10)62019451 | 王晓飞<br>电话号码 (86-10)62414442 |

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/083522

| 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 | 104113839 | A | 2014年 10月 22日 | 无 | | | |
| CN | 103095701 | A | 2013年 5月 8日 | 无 | | | |
| US | 2014/0359697 | A1 | 2014年 12月 4日 | CN | 104219218 | A | 2014年 12月 17日 |