**第一章 绪论**

**1.1研究背景**

随着互联网的高速发展，运营商承载网络从最初简单Internet服务的“尽力而为”网络，逐步发展发展成能够提供涵盖文本、语音、视频等媒体业务的融合网络，其应用领域也逐步的向社会生活的各个方面渗透，深刻改变着人们的生产和生活方式。近年来云计算、大数据等新技术的兴起，面对云时代、大数据时代的高效、灵活的业务承载需求，传统网络的网络架构日益臃肿，面临一系列挑战：

1. 管理运维复杂：传统网络采用的是分布式控制平面，控制协议数量多，标准数量数以千计，如此庞大的控制协议体系，使得管理和维护网络变得愈发困难。

同时，设备厂商在实现这些标准协议时，都进行了一些特定的私有扩展，使得设备的操作维护变得更加复杂，进一步加剧了网络管理员操作维护网络的难度，同时大幅增加了网络的运维成本。

2. 网络封闭，创新困难：由于传统网络采用“垂直集成”的模式，控制平面和数据平面深度耦合，缺乏标准、开放的接口，且在分布式网络控制机制下，当需要在网络中部署新业务时，首先需要解决需求标准的定义，使得新技术的部署周期较长，严重制约网络的演进发展。

3. 设备日益臃肿：由于传统网络的技术体系采用“打补丁”式的演进策略，随着设备支持的功能和业务越来越多（例如，目前IETF发布的RFC标准超过7000个，且还在不停的增加新的RFC和Draft标准），其实现的复杂度显著增加。

传统网络的诸多限制导致网络架构需要改变。在这一背景下，业界一直在研究开发更加开放的新型的网络架构，促进网络逐渐向智能、开放、优化整合等方向转变。这种转变推动SDN软件定义网络的兴起。软件定义网络作为一种新型的网络架构，逻辑上集中的控制层面能够支持网络资源的灵活调度，灵活开放的接口能够支持网络能力的按需调用，将部分或全部网络功能软件化，更好地开放给用户，让用户更好地使用和部署网络，以适应快速变化的云计算、大数据以及更多的创新业务。

SDN作为一种对运营商网络具有重大影响的新技术，其价值已经被业界普遍认可，并在近些年发展迅速。但是随着对SDN架构开发和部署的不断深入, 安全性问题成为制约其发展的一个重要因素。一方面，SDN的出现给传统的网络安全研究带来了很多新的思路和解决方式；另一方面，作为一种全新的网络设计理念，其具有的集中控制性和开放性也会产生很多新的安全问题，比如控制器、基础设施层、控制器与应用层之间以及控制器和转发设备之间的安全问题等。

**1.2国内外研究现状**

**1.3论文研究内容**

**1.4论文结构**

**第二章 相关技术综述**

**2.1 SDN技术**

**2.2 SDN开源控制器调研分析与选型**

**2.3 访问控制技术**

**2.4 web开发技术**

**第三章 SDN应用访问控制系统的设计**

**3.1需求分析**

**3.2 总体设计**

**3.2.1 系统整体架构设计**

**3.2.2 模块设计**

**3.2.2 系统整体设计流程图**

**3.3 算法描述**

**第四章 SDN应用访问控制系统的实现**

**4.1 开发框架介绍**

**4.2 总体实现**

**4.3 主要功能模块实现**

**第五章 系统功能测试和性能分析**

**5.1功能测试**

**5.2 性能分析**

**第六章 总结和展望**

**6.1全文总结**

**6.2 展望**

**第三章 SDN应用访问控制系统的设计**

**3.1需求分析**

SDN网络应用程序和控制器之间的交互在整个北界接口(NBI)中进行。目前，各类控制器在北向接口(NBI)方面没有统一的规范，具有的安全防范措施较少。通过北向接口(NBI)暴露出来的漏洞，攻击者可以向控制器发起攻击，从而使得对来自应用层的安全威胁的防护工作变得尤为重要。应用程序通过北向接口与控制器进行交互主要包括两个方面：读取网络状态（Reading Network State）和写入网络策略（Writing Network Policies）。所面临的基本的安全问题是恶意应用程序随意访问网络状态信息和操纵网络流量，破坏网络的正常状态，威胁网络安全。针对这种情况，通过对控制器上应用程序的访问权限分析，设计一种细粒度的SDN应用访问控制系统。本系统需要对SDN应用进行应用身份信息的注册和权限的授予、以及创建较为灵活的基于属性的访问控制策略，当应用访问控制器上的资源时，先对应用进行身份认证，防止未经注册的非法应用对控制器的访问尝试；然后对经过身份认证的应用进行权限检查，确保应用只能访问具有访问权限的那些控制器资源，对权限范围外的控制器资源的试图访问予以拒绝，防止越权访问，最后对通过权限检查的应用依据之前设定好的访问控制策略进行访问控制判决，应用通过判决后才能访问控制器资源，读取相关的网络状态或写入网络策略。同时，网络管理人员可以通过系统中的UI界面查看控制器上接入的所有应用的状态信息，进行相应的操作。

本SDN应用访问控制系统的重点在于对SDN应用的身份认证、权限核查、以及进行基于属性的访问控制。因此，本系统实现的功能需求如下：

1 网络管理员能够对应用程序进行注册，在注册时除了进行身份信息的记录外，还可以对应用程序的访问权限在初始化时按应用需求进行分配。同时，根据不同情况，创建合适的访问控制策略，为应用的访问控制提供策略依据。

2 当应用程序试图访问控制器资源时，对其进行身份认证，若身份信息验证通过则可以继续访问，否则视为非法应用，对访问请求予以阻止，并写入系统异常行为监测日志中。

3 当应用程序通过身份认证后，对其试图使用的权限进行检查，若满足权限集合的要求则请求可顺利通过，否则将请求信息视为无效请求，写入系统异常行为监测日志中。在该应用程序的生命周期内，访问控制系统严格按照应用程序访问权限集合对应用程序的每个访问请求进行检验，通过这种细粒度的访问权限检查方法，实现了对应用程序访问行为的监测，防止越权访问。

4 当应用通过权限检查后，视为合法应用。依据设定好的基于属性的访问控制策略，对应用进行访问控制判决，只有通过判决的应用才能在最终成功地访问控制器上的网络资源。同时将未通过判决的应用的有关信息写入系统异常行为监测日志中。

5网络管理员可以对应用程序的身份信息和其所具有的访问权限进行查询、修改和删除。同时，可以重置和修改访问控制策略。

6网络管理员可以通过系统查看到全局的网络状态信息，包括网络拓扑、网

节点和网络设备等。还能够查看接入控制器的所有应用的信息。

7 将所有非法的应用访问请求记录到日志文件中以进行审计。

**3.2 总体设计**

**3.2.1 系统整体架构设计**

依据上一小节的需求分析，提出了系统的整体框架图，如图所示

**XACML**

**访问控制**

**应用身份**

**信息管理**

**身份认证**

**应用权限管理**

**权限检查**

**内存数据库**

**日志记录**

**前端页面**

由图可以看出，本访问控制系统分为三层，分别是前端视图层、逻辑控制层和数据存储层。

1.前端视图层：网络管理员可以通过登录页面进入系统，能够查看整体的网络状态，包括控制器信息、网络拓扑信息、交换机和主机信息等。同时通过身份信息管理页面、权限管理页面、策略创建页面等三个页面与逻辑层进行数据交互，给逻辑层传递相关的数据信息。并显示应用身份、权限、策略等信息。

2.逻辑控制层：逻辑层作为本系统的核心部分，与前端视图层和数据存储层进行交互，完成对应用访问控制的大部分功能。逻辑层负责对访问控制器资源的应用进行身份认证、权限检查、XACML访问控制。SDN应用只有全部通过这三个流程的审查后，才能顺利的建立网络策略，获得需要的网络信息。同时逻辑层还负责管理和维护应用的身份信息、权限信息以及访问控制的策略信息。能够把非法的访问请求记录到特定的日志文件中，为以后恶意应用的检测提供依据。

3 数据存储层：负责存储应用的身份信息、权限信息等。由于逻辑层对应用进行身份认证、权限检查时会频繁的查询数据存储层中的数据，为了提高系统认证和检查的效率，数据存储层实际的数据储存是在内存中进行的。

**3.2.2 模块设计**

**3.3.2.1前端视图层**

前端视图层负责系统UI界面的显示工作，同时方便网络管理员进行相应的操作。实质上是一个HTTP客户端，与逻辑控制层的信息交互模块使用HTTP协议进行数据交互。按功能需求可划分为五个模块,分别是管理员登录页面、应用身份信息管理页面、权限管理页面、访问控制策略创建页面、网络视图页面。下面对各模块进行详细的介绍。

1. 管理员登录页面：网络管理人员使用用户名和管理员密码登录SDN应用访问控制系统，进行网络的监管。
2. 应用身份信息管理页面：此模块完成应用的注册、应用身份信息列表的显示、应用身份信息的修改和应用注销等功能。
3. 权限管理页面：此模块具有应用权限的初始化、权限显示、权限的增加与移除等四个功能。
4. 访问控制策略创建页面：网络管理员可以通过此页面录入有关属性的信息，为逻辑控制层中XACML访问控制模块创建基于属性的访问控制策略policy提供信息来源。
5. 网络视图页面：网络管理员可以在此模块查看到控制器的运行状态信息和全局的网络视图，包括网络拓扑图、交换机和主机设备等网络节点的详细信息。

**3.3.2.2 逻辑控制层**

逻辑控制层实现了本系统的核心功能，包括对应用的身份认证，权限检查，基于属性的访问控制等。如图所示，共划分为七个模块，其中身份认证模块、权限检查和XACML访问控制模块的本层的核心模块，而应用身份信息管理和权限管理模块则是上述三个重要模块的基础，负责维护所需的信息。日志记录模块负责对非法应用接入、越权访问等事件的监测记录。信息交互模块通过HTTP协议，解析前端视图层发送过来的HTTP请求，并返回相应的数据。以下是详细介绍：

1. 应用身份信息管理模块

应用的身份信息（身份证书）的结构如下图所示:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| APPID | APPNAME | APPKEY | REGISTRY | REGDATE | EXPDATE | ATL |

APPID:SDN应用的ID,作为其标识，每个SDN应用只有唯一一个。

APPNAME：SDN应用的名称。

APPKEY：SDN应用的秘钥。

REGISTRY：SDN应用所属的注册商。

REGDATE：SDN应用的注册时间。

EXPDATE：SDN应用的有效期。

ATL：SDN应用的信用评级，为以后恶意应用的检测提供一个参考指标。

应用身份信息管理模块实现了对每个SDN应用身份信息的增加、删除、更新、查找等四个功能。

1. 权限管理模块：

权限定义：Wen 等人在论文《Towards a Secure Controller Platform for Open Flow Applications》中分析的控制器上应用程序的15种访问权限，如图所示，主要分为read、write、notification三类，并将每种权限和控制器上特定的资源做了一一映射，应用程序需要访问该资源，必须具有对应的权限。

table1：权限目录分类表（映射到控制器Floodlight中相对应的API）

|  |  |  |
| --- | --- | --- |
| Category | Permission | Screening method(s) |
| Read | read\_topology | getAllSwitchMap:Controller.java |
| getLinks:LinkDiscoverManager.java |
| read\_all\_flow | getFlows:StaticFlowEntryPusher.java |
| read\_statistics | getSwitchStatistics:SwitchResourceBase.java |
| getCounterValue:SimpleCounter.java |
| read\_pkt\_in\_payload | get:FloodlightContextStore.java |
| read\_controller\_info | retrieve:ControllerMemoryResource.java |
| Notification | pkt\_in\_event | addToMessageListeners: Controller.java  addListener:ListenerDispatcher.java |
| flow\_removed\_event |
| error\_event |
| Write | flow\_mod\_route | insertRow:AbstractStorageSource.java |
| flow\_mod\_drop | deleteRow: AbstractStorageSource.java |
| set\_flow\_priority | insertRow: AbstractStorageSource.java |
| set\_devices\_config | setAttribute:OFSwitchBase.java |
| set\_pkt\_out | write:IOFSwitch.java |
| writeThrottled:IOFSwitch.java |
| flow\_mod\_modify\_hdr | parseActionString:StaticFlowEntries.java |
| modify\_all\_flows | setCommand:OFFlowMod.java |

每个SDN应用都具有一个权限列表PERLIST，记录应用所具有的权限集合，描述了应用可以访问控制器资源的最大范围。

权限管理模块负责对应用的权限列表PERLIST的初始化、查询、权限增加、权限移除等工作。

1. 信息交互模块：

采用REST思想，把信息看成一种资源，通过URL定义资源的访问方式，通过GET/POST/PUT/DELETE方法实现对资源的CRUD操作,接受来自前端视图层的HTTP请求，响应，最后返回RESTFUL JSON格式的数据。

1. 身份认证模块：

身份认证模块的流程图如下图所示：

**是否通过认证**

**写入日志**

**应用程序请求访问控制器**

**获得应用的APPID和APPKEY**

Y

N

**权限检查**

应用在北向接口接入floodlight控制器，开始对控制器的资源的发起访问时：

身份认证模块首先获取应用请求中携带的ID和应用密钥KEY，然后利用APPID在数据存储层（内存数据库）中查找相关的应用信息，对ID和KEY进行匹配核对，完成对身份信息的识别，产生认证结果。若为未经注册的非法应用，则认证结果为拒绝，同时交给日志记录模块处理；若为已注册应用，则认证结果为通过，再交给权限检查模块进行权限的核查。

1. 权限检查模块：

权限检查模块的流程图如下图所示：

**得到应用试图使用的权限PER0**

**在内存数据库中查询与该APPID对应的权限列表PER**

**PERLIST是否含有PER0**

Y

N

**XACML访问控制**

**写入日志**

应用成功通过身份认证后，首先根据应用的访问请求，得到应用试图使用的权限PER0，然后在数据存储层（内存数据库）中通过根据应用的APPID查找到对应的权限列表，最后判断PER0是否在PERLIST中，即是否应用具有访问该资源的权限，如果具有，则通过审核，再交给XACML访问控制模块进行基于属性的访问请求的判决。如果不具有，则被视为越权访问，应用无法访问该资源，并交给日志记录模块处理。

1. XACML访问控制模块

XACML访问控制模块采用了一种用于决定请求/响应的通用[访问控制](http://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6)策略语言和执行授权策略的访问控制算法XACML，实现了基于属性的访问控制。首先通过与属性控制管理前端页面交互得到关于主体属性（应用注册商）和环境属性（允许访问的时间段）这两个属性的访问控制策略policy,然后把通过身份认证和权限检查的应用的访问请求转化为Request，策略执行点PEP通过上下文处理器把Request交给策略决策点PDP进行评估，PDP把请求Request和访问控制策略policy进行匹配，若应答结果Response为Permit，则允许访问，若是Deny则拒绝。这种基于属性的访问控制策略在一定程度上使得访问控制具有较好的灵活性。

**写入日志**

**从前端页面**

**获得属性的相关信息**

**创建访问控制策略Policy**

Deny

**策略执行点PEP将应用的访问请求转化为Request**

**将Policy交给策略管理点PAP**

**PEP通过上下文处理器将Request转交给策略决策点PDP**

**PDP通过PAP查找相关的Policy**

**PDP生成对Request的评估结果**

**应用成功访问控制器资源**

Permit

**3.3.2.3 数据存储层**

应用访问权限管理系统整体的框架图如上图所示，分为八个模块，并选取floodlight作为系统实现所依赖的开源控制器。其中前端页面包含四个子页面，包括应用身份信息管理页面，权限信息管理页面，属性控制管理页面，网络视图页面。应用身份信息管理页面具有应用的注册，身份信息的查询，修改，应用注销等功能，与后台的应用身份信息管理模块进行数据交互。权限信息管理页面具有应用权限初始化，权限查询，权限增加，权限删除等功能，与后台的应用权限管理模块进行数据交互。属性控制管理页面具有创建基于属性的访问控制策略的功能，与后台的XACML访问控制模块进行数据交互，为XACML判决提供策略依据。网络视图页面整合了floodlight本身具有的全局网络拓扑视图webUI界面，使整个系统的功能比较完整，系统管理员可以通过此页面查看整个网络中各个网络节点以及节点之间的链路等信息。

后台各模块采用Restlet框架，把身份信息、权限信息等数据封装成REST资源，实现web-service服务，从而达到与前端页面交互的功能。

应用身份信息管理模块负责维护应用的身份信息，身份信息包括应用ID，应用名称，应用密钥，应用注册商等属性，将身份信息等数据存储在内存数据库中，实现了信息的增删改查等功能。

权限管理模块负责调整应用所具有的权限，同时将权限信息存储在内存数据库中，实现了对应用的权限授予，查询，移除等功能。

当应用在北向接口接入floodlight控制器，对控制器的资源的发起访问时：

身份认证模块通过应用的ID和应用密钥对应用进行身份识别。若为未经注册的非法应用，则认证结果为拒绝；若为合法应用，则认证结果为通过，再交给权限检查模块进行权限的核查。

权限检查模块首先在内存数据库中通过的ID找到应用的权限列表，然后查看应用是否具有访问该资源的权限，如果具有，则通过审核，最后交给XACML访问控制模块进行基于属性的访问请求的判决。如果不具有，则被视为越权访问，应用无法访问该资源。

XACML访问控制模块采用了一种用于决定请求/响应的通用[访问控制](http://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6)策略语言和执行授权策略的访问控制算法XACML，实现了基于属性的访问控制。首先通过与属性控制管理前端页面交互得到关于主体属性（应用注册商）和环境属性（允许访问的时间段）这两个属性的访问控制策略policy,然后把通过身份认证和权限检查的应用的访问请求转化为Request，策略执行点PEP通过上下文处理器把Request交给策略决策点PDP进行评估，PDP把请求Request和访问控制策略policy进行匹配，若应答结果Response为Permit，则允许访问，若是Deny则拒绝。这种基于属性的访问控制策略在一定程度上使得访问控制具有较好的灵活性。

日志记录模块：采用java日志框架logback实现。当应用的访问请求在身份认证模块、权限检查模块、XACML访问控制模块中的判决结果为拒绝（即不允许访问）的时候， 日志记录模块会将这些非法的访问请求记录到日志文件中，为以后恶意应用的检测提供依据。