



SDN 技术优化的最新研究综述

肖子玉

(中国移动通信集团设计院有限公司网络技术研究所, 北京 100080)

摘要:在 SDN 技术从学院走向商用的背景下,介绍并总结了 OpenFlow 协议优化、面向应用的流表设计、SDN 多域控制、数据中心组网路由优化和安全可信网络架构 5 个领域的研究成果,提出了面向未来引入 SDN 技术的应用场景和研究方向建议。

关键词:SDN;OpenFlow;控制器;优化

中图分类号:TN915

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2015377

A review of the latest research on SDN technology optimization

XIAO Ziyu

Department of Network Technologies, China Mobile Design Institute Co., Ltd., Beijing 100080, China

Abstract: Under the background of SDN technology from the college to commercial, the research results of OpenFlow protocol optimization, application oriented flow table design, SDN multi-domain control, data center network routing optimization and requirements of security network architecture were introduced and summarized. At last, the application scenarios and research directions for the future SDN technology was proposed.

Key words: SDN, OpenFlow, controller, optimization

1 引言

SDN (software define networking, 软件定义网络) 技术的创新点就是提出了 OpenFlow 这一概念^[1]。它利用网络控制器获取全视角网络拓扑和统计反馈,简化了网络和流量的管理控制功能,实现了 IP 数据网络控制与转发相分离的架构。SDN 提出后,产业界致力于将新技术与现有产品和技术结合,采用控制与转发分离的架构、现有成熟的网络协议,扩展 SDN 技术的范畴,减少革命性技术对产品的影响。而学术界则致力于进一步完善 OpenFlow 等创新技术的架构和算法,提出满足大规模数据中心和虚拟化组网等商用需求的优化方案。本文将着重介绍学术界对 SDN 技术的优化思路和进展。

2 面向商用,SDN 技术有待进一步优化

从 SDN 架构和 OpenFlow 协议本身看,SDN 控制器需要获取全视角拓扑和网络的统计反馈才能实现集中资源管理和分配。这就要求 SDN 交换机与控制器之间进行频繁的交互,且 OpenFlow 协议最初的设计头域过大,这些问题都增大了商用的投入,难以适应高性能网络的需求。

从大型数据中心引入 SDN 应用和组网需求看,现代数据中心都运行着大量的服务器,形成大规模虚拟化数据中心,这就要求数据中心具有灵活配置和业务移植功能。传统数据中心采用分层的组网结构,由三层网络设备连接二层节点群。“扁平化”设计方法虽然灵活,但受到数据风

暴和虚拟化地址查询的影响无法达到预期效果。而引入 SDN 技术,通过优化实现主动路由功能(paris),可实现大规模数据中心的灵活配置管理需求。

从广域网络引入 SDN 技术的需求看,SDN 广域网络将形成多域多控制中心的架构。相邻控制中心间需进行交互以实现域间连接控制策略,而通过优化的局部分布式算法(locality),进一步优化了 SDN 多域控制的灵活实现。

从引入 SDN 技术的网络安全领域看,通过实现软件定义网络,为运营商提供了对网络的灵活定制和管理能力。但从安全领域,如接入控制和多路径控制等目前只能依靠 SDN 技术自身,SDN 技术亟待解决安全架构的问题。

3 SDN 优化方案

3.1 OpenFlow 优化方案 DevoFlow

OpenFlow 的核心是获取全网视角拓扑和统计反馈,以实现有效的集中化管理。集中化有效避免了针对不同流量类型逐台交换机进行配置的繁琐,通过负载均衡和节能感知路由有效优化流量管理,交换机功能简洁化而提高了性能。但 OpenFlow 设计中频繁的控制器—交换机的交互,增大了信令面负荷。而控制器对流的控制将引入至少 4 ms 的时延,使流量受限于几百个流/s 的处理能力。对于控制器从交换机收集流量的统计反馈中,OpenFlow 支持的 3 种计数器,分组、比特和流时长均影响交换机性能,引入过多的控制负荷。

参考文献 [2] 中提出的 DevoFlow (devolve flow from controller, 下移流量控制)则是在 OpenFlow 基础上保留有效集中控制的优势。DevoFlow 即设计了一套新方案对 OpenFlow 进行优化,打破原有管理和全视角拓扑的依存关系,在交换机网络层维护有价值的拓扑关系。

3.1.1 优化方案一:下移控制的机制

下移控制的机制,即规则克隆(rule cloning)和本地操作(local action)。

(1)规则克隆

在标准 OpenFlow 机制中,通配规则意味着所有匹配规则的流都执行同一转发路由。这虽可避免逐流的控制交互,但却导致了所有匹配的微型流量进入同一转发路由并积累统计反馈到单一组计数器上,影响统计反馈的性能。

为解决此问题,在 DevoFlow 中引入一个布尔克隆标志(boolean clone flag)扩展了通配规则中的操作部分

(action part)。如果标志被清除,交换机则执行标准通配规则。否则交换机在本地克隆通配规则并生成一条新规则,在这条新规则中,所有匹配这一微型流量的值替换原有通配规则中的通配值,其他未被替换的值继承原有通配规则。后续匹配这种特定微型流量规则的数据分组将被分配到该规则指定的统计计数器上,实现了统计功能的负载均衡。同时这条规则进入了精确匹配查询表,减少对高速内存(TCAM)的使用,有效降低了商用成本。

(2)本地操作

在标准 OpenFlow 中,某些流需要控制器在高负荷控制或直接由特定端口转发这两者间进行抉择。在 DevoFlow 中,通过对本地路由操作(local routing action)进行很小的扩展,即可减少控制器对这些流量的控制。本地操作包括多路径支持和快速路由。

多径功能支持交换机为可克隆的通配规则选择不同的输出端口,交换机可随机执行概率或循环选路规则。后续特定流量将继承已选定端口进行传输。该功能与等价路由(ECMP)功能相似,但该功能更灵活、更便宜。ECMP 针对不对称或容量差别较大的多路由的负载均衡能力不强,而 DevoFlow 通过允许可克隆通配规则依据概率分布输出端口的方式解决了上述问题。

快速重路由功能为交换机提供了多条回落路径,当原设计输出端口故障时采用。如果交换机能够在本地执行此决定,则其可在路由失败时立即恢复,否则需要报告控制器并等待指令,这将使业务恢复时间延迟一个或几个来回时间(RTT)。OpenFlow 只需进行稍许优化,即配置重叠规则和路由优先级,并设定灵活的策略使交换机实现端口失败后,由重叠路由替换原有路由。

3.1.2 优化方案二:有效的统计数据收集

DevoFlow 提出了 3 种方案优化统计反馈数据的收集,分别是样本法、触发报告法和近似计数器法。

样本法是交换机交互推送或提取收集数据,特别是传送协议允许交换机随机选择分组头上报控制器时。样本是均匀选择的,推荐值是 1/1 000 个数据分组,由于上报的统计分组不是完整数据分组,因此统计占用负荷小于 0.1%,由于其可在数据面实施,因此也不会过多占用 CPU 资源。

触发报告法是在 OpenFlow 中增加一种推送机制—基于阈值触发计数器。触发条件满足,交换机即会送出统计报告,也可设计为多个报告打包传送。最简单的触发条件就是基于原有的分组、比特和时长 3 类统计计数器,该方

法很容易在数据面部署。

最后一种方法是近似计数器法,该方法适用于所有匹配转发规则表的流量分组。这类计数器维护最大的 K 个流的行为模式统计视图,执行简单高效的流算法。该优化方案较上述其他几种难于实现,但该方案可提供更实时精确的网络视图。

总结一下,DevoFlow 从控制协议本身和统计反馈数据的收集方案对 OpenFlow 进行了优化,使其更灵活,开销更小,更适用于商用部署。

3.2 面向应用的流表设计

在 IP 网络中有 NAT、防火墙过滤、基于内容转发的需求等,这些需求均需要特定功能的设备实现。在 SDN 中可以通过控制器面向业务的北向接口进行软件定义,实现业务功能。但这就提高了交换机与控制器交互在转发面产生的时延,也使控制器成为业务瓶颈。

参考文献[3]提出的数据转发层感知应用方案如图 1 所示,在 OpenFlow 交换机流表处理流程中增加一级应用流表(app table),它与标准流表执行方式相同。如果数据分组匹配应用流表成功,则执行相应转发操作;如果数据分组匹配应用流表失败,则生成上报数据分组,送 SDN 控制器,控制通过标准流表命令对交换机安装新的应用流表并删除无效应用流表,供后续数据分组转发执行。应用流表可以对应一个或多个应用,并形成应用流表链。应用流表的执行顺序由策略决定。下面以防火墙和负载均衡两个应用组成的应用链为例说明数据面应用感知的原理。

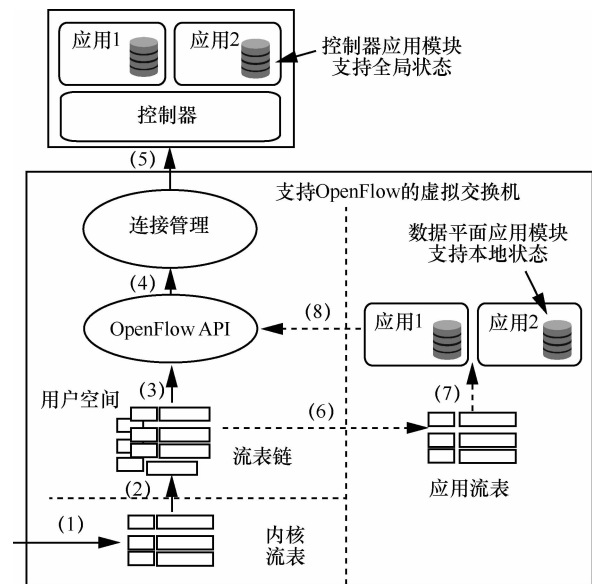


图 1 OpenFlow 交换机数据转发层应用感知示意

防火墙和负载均衡器应用感知说明如下。

- 假设防火墙策略为:任何目的地址是 ServerX 的分组均需经过防火墙过滤,且最大 TCP 连接数为 1 000。
- 负载均衡器策略为:经防火墙的分组再经负载均衡器,按源 IP 地址进行散列,将负载分配给服务器 S1 或服务器 S2。

为执行以上策略,控制器首先向应用流表插入规则:(dst_ip=x, tcp, dport=80:fw, lb, fwd, install),其中:fw:防火墙,lb:负载均衡,fwd:转发,install:安装应用功能。

当新数据分组 (src_ip=a, sport=6000, tcp, dst_ip=x, dport=80) 抵达时,它将从内核—用户空间第一级流表(匹配失败)—应用流表(匹配)—顺序执行 4 项操作—防火墙,if nFlow<1000,(src_ip=a, sport=6000, tcp, dst_ip=x, dport=80:null)—负载均衡,hash(src_ip)=S1, (src_ip=a, sport=6000, tcp, dst_ip=x, dport=80:set dst_ip=s1)—转发, (src_ip=a, sport=6000, tcp, dst_ip=x, dport=80:set dst_ip=s1, out pt1)—安装应用功能,调用 API_add_flow 安装应用功能到流表管道。SDN 交换机根据网络策略不经控制器成功生成了流规则,实现了应用感知。

为了检验数据面感知应用的有效性,搭建内容感知服务器分发应用进行验证,如图 2 所示。

经验证,当 TCP 请求较少时,应用感知流表的执行对交换机影响很小;但当 TCP 请求数量逐渐放大,交换机时延显著放大。分析原因,结果受验证环境和编码优化程度影响较大。

对于 IP 网络中大量的应用需求,如果按 SDN 原有设计控制与转发完全分离,将导致大量特殊应用需求由控制器处理,造成时延和业务瓶颈。而数据面应用感知的优化思路又从集中处理回到分布式处理。经验证,简单逻辑的应用感知对交换机影响不大,但复杂应用在数据面感知对交换机性能影响较大。

3.3 局部分布式算法实现 SDN 多域控制

大型 SDN 将分成多个控制域,每台控制器负责本域内的转发控制,相邻接域间控制器通过彼此通信生成全网转发策略,形成分布式的 SDN 控制网络。因此在 SDN 设计中需要满足两个要求:形成 SDN 的物理架构,适合引入新的控制器,并形成新的控制域;有效应对新的事件请求,基于现有流量模式快速计算出优化路由。

SDN 分布式控制网络可以采用两种架构,分别为分级架构和扁平架构,如图 3 和图 4 所示。

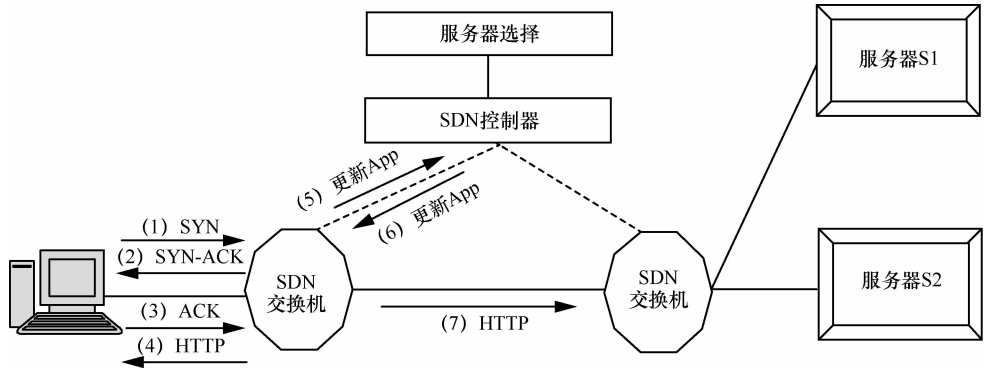


图2 内容感知验证示意

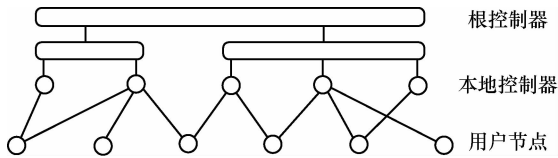


图3 SDN 控制器分级架构示意

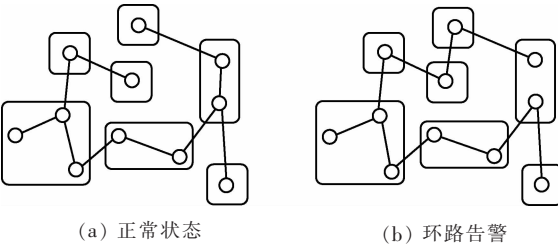


图4 SDN 控制器扁平组网示意

在SDN控制网分级架构中,根控制器通过与局部控制器的通信获取全视角信息,以便有效进行域间优化路由计算。在SDN控制扁平架构中,每个域控制器不仅需要获取直接相邻接域局部信息,还需要通过邻域控制器获取全网各域控制器信息,以便进行域间路由优化和环路检测。否则无法完成环路检测。参考文献[4]提出了局部分布式算法在SDN控制网络中的应用。

在经典分布式系统中,每一个设备均是计算节点。起初,它只知道直接邻接的周边环境,如节点标识和各链路连接状态等。但通过与邻接节点的信息交换,它逐步获取了全网架构的相关信息。通常用距离(distance)这个变量来描述节点间的邻接关系,distance=1表示为直接直邻的节点。距离在网络中与时延、通信、同步、业务量负荷和控制器协作等方面有关,距离值越大,则完成控制的网络成本越高。图5所示网络中,控制器 v 通过局部算法计算出节点 u 是到控制域 w 的最短距离,因此控制器发出交换信息到节点 u ,节点 u 转发信息到控制器 w ,控制器 w

通过计算的最短路径反馈信息给控制器 v ,依此类推实现了局部算法的全局应用。

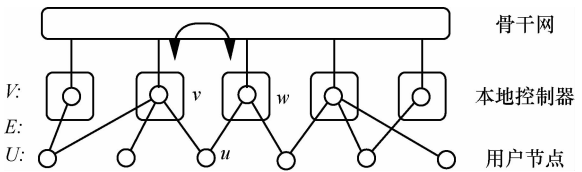


图5 局部算法的应用示意

从以上分析可知,在实际组网中,分级架构由于各域控制仅与根控制器邻接,与其他域控制器的距离均为2,因此从控制成本上看有一定优势。但分级控制网络较适合于统一组织和管理的网络,如运营商的网络。而扁平架构的网络在实际组网更为灵活,适用于互联网中各对等网络的组网,不需要统一的管理,但带来控制成本的提高。如何有效降低分布式控制成本是目前学术界研究的关键性问题。以下局部分布式算法主要用于优化扁平控制架构。

(1)扁平架构环路验证算法

首先任意选择节点 r 作为根节点,网络中每个节点 v 均获得两条信息:所选取的根节点 r 、根节点 r 与节点 v 间的距离。该算法公平简洁地将网络变为局域可自检的扁平网络。当网络中存在环路时,至少有一个节点能发现,因为距离标签不能为恒定值。

(2)链路分配算法

当节点 u 与节点 v 相连时,如果同时还有 c 个节点与 v 相连,则赋予 u 成本值 $c(cost_u=c)$,算法的任务就是优化网络总成本值,使其达到最小值。

在实际SDN控制网络设计中,需要首先完成架构设计。当有新的控制域部署并要求加入网络时,需要触发新一轮计算收集网络物理拓扑信息,同时还需要知道当前网络流量信息。为了快速计算出优化路由,局部算法具有较



强的优势。建议的两步算法模型为:网络中每个节点提供以下两类信息,一是全网物理拓扑信息 G ,二是网络中节点 v 的半径为 r 的邻接节点状态信息 $H(v,r)$,依据以上信息节点 v 即可找到最优输出路由,并形成全网优化路由表。

局部分布式算法可有效应用在 SDN 控制器多域组网中。该算法较适用于互联网等对等网络组成的扁平架构控制平面组网。

3.4 数据中心组网优化方案

SDN 技术的一大应用场景是应用于大型数据中心组网。现代化的大型数据中心需具备大规模扩展服务器能力,并提供虚拟机的灵活部署和迁移能力。而传统数据中心划分为许多小集群,在群内提供灵活的虚拟机部署和迁移较容易,但群间交互和虚拟机迁移的有效性不高。主动路由就是一种有效解决上述问题,实现大规模虚拟化数据中心的灵活配置和管理的方案。参考文献[5]提出了主动路由方案(paris)。

paris 路由采用 IP 地址寻址,利用传统的层三交换机基于目的地址前缀进行数据分组的转发。组网设备采用 SDN 控制器和交换机。SDN 控制器通过记录每台虚拟机的地址和位置预制网络转发状态。底层与主机相连的交换机存储着下辖所有虚拟机的入口。控制器跨核心交换机实现转发状态分区管理,而交换机存储细粒度的 IP 地址转发表。该方案的优势如下:

- 全部层三转发设计避免了采用 MAC 地址的地址空间过大和广播风暴;
- 控制器基于全网视角的转发表主动预制和下发,交换机分布式存储转发表,核心交换机存储分区转发信息,低层交换机存储区内细粒度转发表,避免了扁

平化路由转发表过大的问题,并减小了转发时延;

- 集群内转发在集群内完成。低端底层交换机存储集群内所有虚拟机转发地址,实现群内快速转发。目前低端交换机可满足存储上千台运行 32 个虚拟机的主机的转发表需求。

经计算机模拟分析评估,主动路由方案有效提高了大型数据中心虚拟机的可扩展性、部署的灵活性和可移植性的空间。

主动路由方案采用两种组网方式的应用:无弹力拓扑(no-stretch topology)(如图 6 所示)和高带宽拓扑(high-bandwidth topology)(如图 7 所示)。

网络分三层设置,低层为边缘交换机,中间层为聚合交换机,上层为核心交换机。边缘交换机存储所有相连的虚拟机转发路由,并与本分区节点内聚合交换机相连。聚合交换机存储节点内所有主机转发信息,核心交换机存储分区转发信息,即核心交换机存储虚拟 IP 地址前缀对应的指定前缀交换机(aps)。无弹力拓扑和高带宽拓扑的主要区别在于聚合交换机及核心交换机的组网方式。无弹力拓扑中,聚合交换机连接所有核心交换机,并需要存储所有虚拟前缀以便实现跨节点转发,核心交换机互不连接;高带宽拓扑中,每台聚合交换机连接两台核心交换机,核心交换机自组网状网。

由于两种拓扑边缘到聚合交换机的组网方式是一样的,因此分析两者组网优势时可重点分析聚合交换机和核心交换机端口占用。假设参数如下:核心网交换机 m 台,每台交换机单端口速率 r ,聚合交换机 k 台。

聚合交换机数量越多,系统支持的容量越大,所需端口越少,组网越优,见表 1。

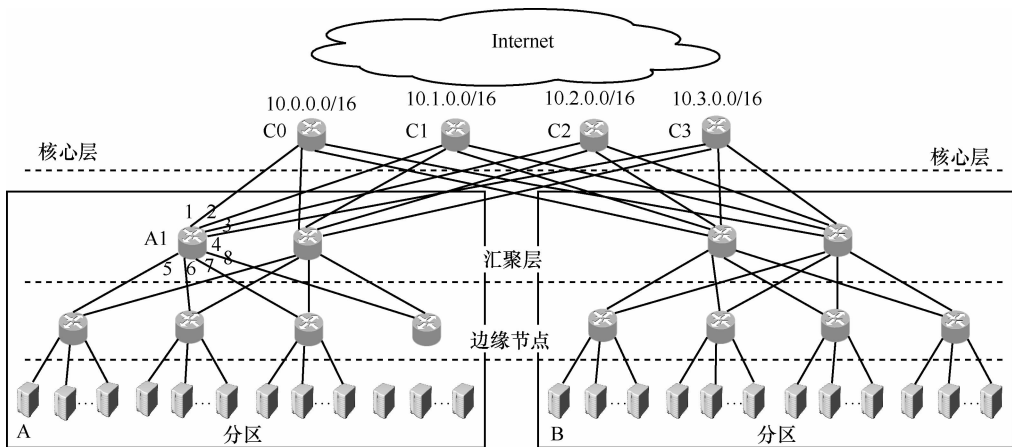


图 6 无弹力拓扑组网示意

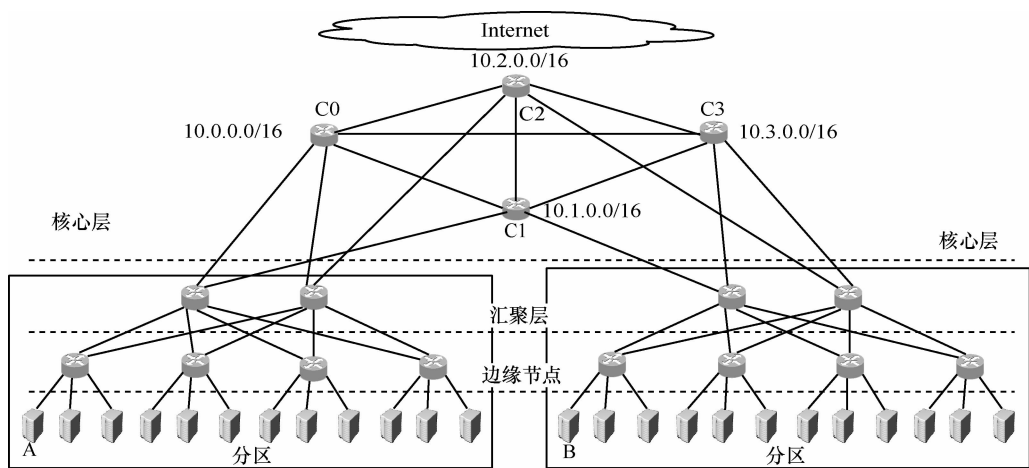


图 7 高带宽拓补组网示意

表 1 两种拓扑比较

比较	无弹性拓扑	高带宽拓补	分析
核心端口需求/个	$m \times k$	$m(m-1)+2k$	当 $m \geq 3$ 时,随着 k 的增大,无弹性拓扑对端口的需求将会大大高于高带宽拓补
聚合上联端口/个	$m \times k$	$2k$	
扩展性	较强	强	高带宽拓补新增集群只需连接两个端口,控制器配置更简便
路由数/条	m	2^3	高带宽拓补负载均衡路由更多样,容错性更高
核心转发带宽	输入 r 单路由转发 r	输入 r 单路由转发 $2r/m$	高带宽拓补核心层转发能力更强
核心转发次数/次	1	2	转发次数越多,时延越高

数据中心组网时高带宽拓补组网方案更优,以上分析已经过计算机模拟评估。

利用SDN集中控制功能,采用扁平化IP地址主动路由方式可建立扩展性强、灵活性高的数据中心。转发层交换机的组网拓扑和分布式转发表的存储可优化数据中心性能。

3.5 SDN 安全需求和安全架构

SDN 为网络运营者提供了更灵活更强大的运营能力,通过构建软件系统完成网络的管理和调试。作为一个开放系统,SDN 本身同时允许安全和可信机制相关的技术应用,因此有必要探讨通过网络设计构建安全和可信的SDN。SDN 软件控制全网的能力和集中化智能控制的能力是安全威胁的隐患。参考文献[6]分析了网络中引入SDN技术的安全威胁。

SDN 网络的七大安全威胁如图 8 所示。

(1)伪造数据流

来自恶意用户或恶意服务器,用于攻击 OpenFlow 交换机和控制器。

(2)交换机漏洞攻击

单个交换机的攻击即可导致分组丢失、减速。

(3)控制平台通信攻击

可能发生 DoS 攻击及数据窃取。TLS/SSL 并不能保证安全。

(4)控制平台漏洞攻击

这对 SDN 是最严重的风险,一台错误或恶意的控制器可导致妥协。

(5)缺乏信任机制

控制器和应用管理系统间缺乏信任机制。

(6)管理平台漏洞攻击

传统网络中也存在。

(7)缺乏可信数据源用于取证和修复

为了观察和建立事实数据,需要依靠网络中所有域和节点。进一步说,该数据只有可信才能举证。

以上 7 种安全风险,通信攻击、漏洞攻击、缺乏信任机制是 SDN 特有的,其他也存在于传统网络中。在 SDN 系统中没有确保控制器与交换机间信任关系的机制,也没有技术保证控制器间通信的可信度。作为一个高稳定性的系统,SDN 应具备应对故障和入侵的能力。而设计一个安全可靠的 SDN 系统控制平台有助于提高 SDN 系统的稳定性。

SDN 安全可靠控制平台逻辑架构如图 9 所示。

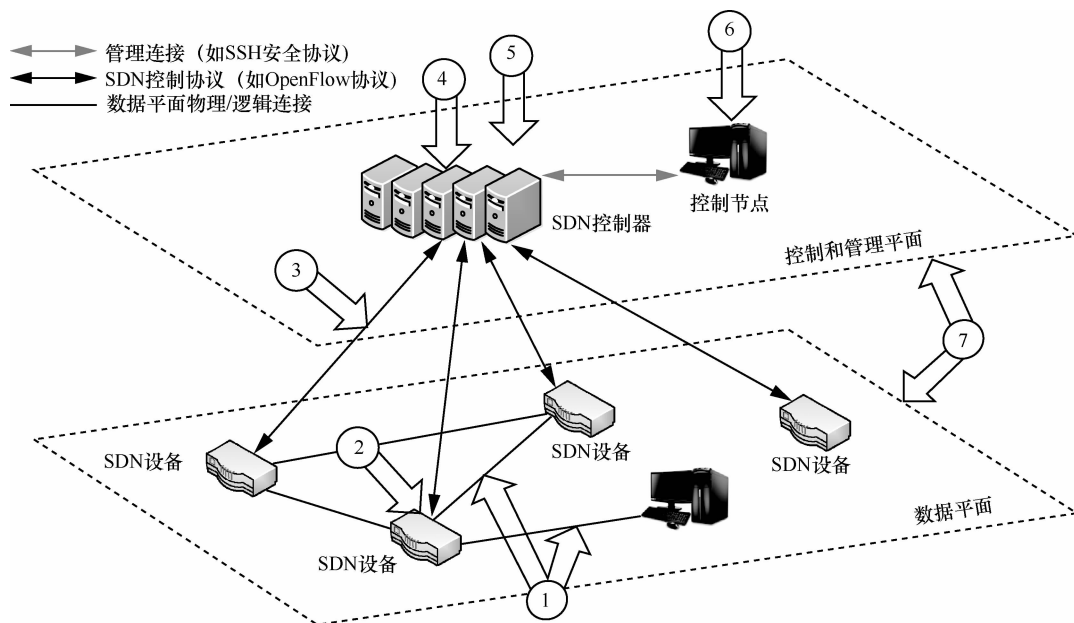


图 8 SDN 安全威胁示意

如图 9 所示,安全可靠的 SDN 系统需要以下机制。

(1)可复制性

这是最重要的提高 SDN 系统稳定性的机制。除了控制器的可复制外,上层应用也应是可复制的。这不仅提高了由软硬件故障带来的系统稳定性,也有效隔离了恶意攻击带来的故障和系统崩溃。

(2)多样性

系统设计的基本原则是尽量避免共同故障模式,如软件的 bug 或漏洞。现有的来自不同家族的操作系统很少有相交的漏洞,换句话说操作系统的多样性可提高系统的稳定性。因此在 SDN 系统中相同的应用应尽可能加载到不同(或异构)的控制器中。

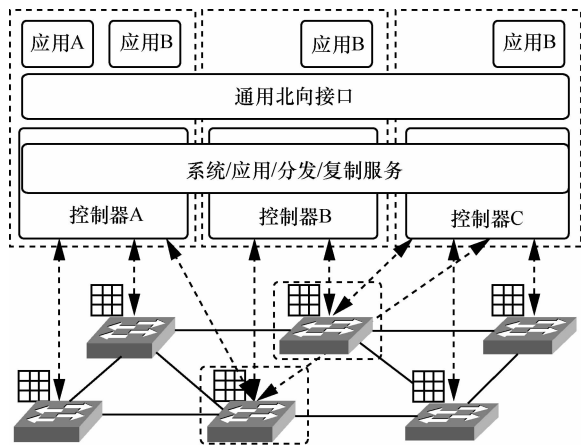


图 9 安全可靠的 SDN 控制平台示意

(3)自愈机制

主动和被动恢复机制可将系统带回健康状态,更换受损器件,保持系统正常运行。在更换受损器件时,应尽可能更换为新的或不同版本设备,以保证多样性的原则。

(4)动态系统关联机制

一台交换机应动态地与多台控制器通过安全手段相关联。这可以形成自动容错机制,同时通过选择最快响应控制器提高控制平面的吞吐量减小控制时延。但这就要求交换机具有一定的可编程能力。

(5)设备与控制器的信任机制

最简单的信任机制是建立在控制器中的可信设备的白名单,但这种方式缺乏必要的灵活性。另一种方式是信任所有交换机直到它的诚信受到质疑。基于异常或故障算法,恶意或异常行为将会被其他交换机或控制器报告,一旦该交换机或控制器的诚信度低于可接受阈值,该设备将被自动与所有其他设备隔离。

(6)应用与控制器软件的信任机制

软件由于老化、bug 或攻击都可能呈现出异常行为。基于软件系统的诚信度自动评价模型,即通过观察和测量设备的可用性、可靠性、诚信、安全性、可维护性和保密性等特征指标,自动评估设备的可信度。

(7)安全域设置

安全域隔离是通用技术手段。在 SDN 控制平面中,安全域可以探索使用沙箱和模拟器,这些工具可以设计出强大的

隔离模式,通过接口设计,可实现仅有少数跨域通信需求。

(8)安全设备部署

部署安全设备如可信计算机等防篡改设备用于存储敏感数据,增强系统的稳定性。

(9)快速和可靠的软件包升级机制

快速和可靠的软件补丁和升级是减少漏洞的基本要求,因此 SDN 控制平面应部署安全可靠的系统升级机制。

SDN 安全可靠架构的优化思路总结如下。

- 面向大规模商用组网的 SDN 系统设计,应用和控制器的可复制性、多样性和动态关联机制是必不可少的。这就要求控制器支持 pool 方式的部署,交换机多归属,由多个控制器动态控制,一组控制器和交换机应采用异构操作系统形成多样性,保证整套系统的稳定性。
- 面向应用于开放网络环境的 SDN 系统设计,应具备设备软硬件的诚信机制。建立黑白名单认证机制或恶意行为检测评价机制。
- 面向 SDN 的管理运营系统设计,应具备系统自动升级管理机制。

4 结束语

SDN 技术正在向着适宜商用网络大规模部署方面发展。优化方案和思路正在逐步解决 SDN 商用面临的问题。即将引入 SDN 作为下一代网络发展的关键技术,需求一是面向数据中心组网应用,二是面向骨干承载网络的组网应用。比较而言,数据中心组网可预测性、可管理和可控性强,SDN 技术实现数据中心组网更容易。而骨干承载网络的大流量和不可控性的业务需求正是 SDN 集中控制动态调整路由功能最适合的场景,因此承载网引入 SDN 将是未来的发展方向。面向这两类需求,未来应该着重研究的领域包括:

- 面向数据中心引入 SDN 组网方案研究、对 SDN 设备的技术需求和解决方案研究;
- 面向 IP 骨干承载网引入 SDN 组网方案研究、对

SDN 设备的技术需求和解决方案研究;

- 引入 SDN 技术的安全需求和安全设计要求研究。

参考文献:

- [1] OpenFlow switch specification, V1.3.0[S]. 2012.
- [2] CURTIS A R, MOGUL J C, TOURRILHES J, et al. DevoFlow: scaling flow management for high-performance networks[C]//The ACM SIGCOMM 2011 Conference, August 15-19, 2011, Toronto, Canada. New York: Association for Computing Machinery, 2011: 254-265.
- [3] MEKKY H, FANG H, MUKHERJE S, et al. AMC: application-aware data plane processing in SDN [C]//The Third Workshop on Hot Topics in Software Defined Networking, August 17-22, 2014, Chicago, USA. New York: Association for Computing Machinery, 2014: 13-18.
- [4] SCHMID S, SUOMELA J. Exploiting locality in distributed SDN control [C]//The Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, August 12-16, 2013, Hong Kong, China. New York: Association for Computing Machinery, 2013: 121-126.
- [5] ARORA D, BENSON T, REXFORD J. ProActive routing in scalable data centers with PARIS [C]//The ACM SIGCOMM 2014 Workshop on Distributed Cloud Computing, August 17-22, 2014, Chicago, USA. New York: Association for Computing Machinery, 2014: 5-10.
- [6] KREUTZ D, RAMOS F M V, VERISSIMO P. Towards secure and dependable software-defined networks[C]//The Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, August 12-16, 2013, Hong Kong, China. New York: Association for Computing Machinery, 2013: 55-60.

[作者简介]



肖子玉(1969-),女,中国移动通信集团设计院有限公司网络技术研究所总工程师、教授级高级工程师,2014-2015 年美国北卡罗莱纳州立大学计算机科学系访问学者,主要研究方向为 5G、VoLTE、IMS、信息安全。