基于 SDN 技术的网络入侵追踪与响应系统的研究

程俊，龚俭，杨望，臧小东
（东南大学网络空间安全学院，江苏 南京 211189）

摘　要：针对当前基于 SDN 的网络入侵阻断系统 HYDRA 的不足，设计并实现了基于 SDN 技术的网络入侵追踪与响应系统。新系统将控制逻辑和响应逻辑解耦，提高系统的可扩展性。控制层改进任务调度模型，提高系统的顽健性。完善的系统接口规范提高系统可用性。对 RYU 控制器的研究和改进进一步挖掘控制器潜力，使系统与 SDN 联系更加紧密。

关键词：软件定义网络；入侵追踪；可扩展性；规范接口
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018185

Research on network intrusion tracking and response system based on SDN technology

CHENG Jun, GONG Jian, YANG Wang, ZANG Xiaodong
School of Cyber Science and Engineering, Southeast University, Nanjing 211189,China

Abstract: In view of the shortcomings of the current network intrusion blocking system based on SDN, the network intrusion tracking and response system based on SDN technology was designed and implemented. The logic and response logic were decoupled, and the scalability of the system was improved. The task scheduling model and the robustness of the system were improred. Perfect system interface specification improves the availability of system. The research and improvement of RYU controller further explore the potential of the controller, so that the system is more closely related to SDN.

Key words: software define network(SDN), intrusion traceback, scalability, specification interface

1　引言

随着计算机网络应用的快速发展，网络安全问题也变得日益突出。因此，如何有效加强对网络安全事件的应急响应能力，不断提高系统的安全防护水平已成为人们越来越关注的问题。虽然网络安全技术的不断发展为网络安全管理人员提供了大量的工具和数据，可是每个组织内部应急响应队伍中的人员数量仍然有限。一方面，每个组织每天新产生的事件数都远远超过了现有人员的处理能力，同时，如果让安全管理人员每天超负荷地处理事件，会让管理人员产生懈怠的情绪并可能会忽视真正需要处理的事件。因此需要引入自动化响应[1]手段。

面对传统网络的复杂体系结构，传统网络安全解决方案显得臃肿而迟钝，而且网络设备需要人工配置，无法实现高效的自动化响应。软件定义网络（SDN, software-defined networking）[2]技术的出现为这些问题的解决提供了新的思路。接下来本文将围绕中国教育科研网（CERNET, China education and research network）的实际情况，使用 SDN 技术对相关网络安全问题解决方案进行探索和验证。

目前，在 CERNET 主干网运行管理与安全保障

收稿日期：2018–09–19
基金项目：赛尔网络下一代互联网技术创新资助项目（No.NGII20160409）
Foundation Item: CERNET Innovation Project (No. NGII20160409)

系统中包含了一个大型分布式应急响应服务管理系统 CHAIRS(cooperative hybrid aided incidence response system)[3], 该系统已部署在 CERNET 的 38 个主节点, 为各节点的网络安全事件响应组（CERT, Computer emergency response）提供应急响应服务管理功能，提高 CERNET 内安全事件响应的效率。对于 CHAIRS 系统提供的安全警报，需要各节点的安全管理员进行应急响应，发现并解决网络中存在的安全问题。为了帮助管理员对 CHAIRS 提供的安全警报进行应急响应，设计并实现了 HYDRA(hybrid detection response agent)[4]系统，该系统利用 SDN 强大的网络自动化管理和控制能力实现对网络攻击的自动化响应和恶意流量的样本采集工作。

随着 CERNET 主干网运行规律和安全保障内容的扩展，产生了新的应用要求和应急响应要求，使得现有的 HYDRA 系统不能满足这些新出现的需求。目前的 HYDRA 系统需要满足以下 3 点需求。

第一，完善的接口需求，HYDRA 系统不仅需要从 CHAIRS 系统接收安全事件信息，还需要与应用层子系统反馈响应任务的执行情况。因此需要设计一套完善的接口。第二，完善的响应任务管理与调度需求, HYDRA 作为一个具有入侵跟踪和应急响应功能的系统，需要有完善的响应任务管理机制。第三，SDN 控制器功能拓展需求，目前的系统仅仅将控制器作为一个下发流表规则到 openflow[5-6]交换机的工具，不能应对复杂的响应任务，因此系统需要对 SDN 控制器进行一定的功能拓展。

基于上述研究背景和现状，本文研究实现一种基于 SDN 架构的网络入侵追踪与响应系统，在原有系统基础上加入分层思想，将响应逻辑从控制逻辑中剥离，通过松耦合的架构来实现原有系统的新需求，提高系统的可扩展性。

2　系统设计

2.1　系统总体架构设计

根据 SDN 的分层架构和 HYDRA 系统实际功能需求，HYDRA 系统结构如图 1 所示。HYDRA 系统通过系统接口接收来自 CHAIRS 的案件，然后将案件转发给相应的响应模块执行响应逻辑，生成响应任务。响应任务通过自定义北向接口传到控制层，进入任务管理模块。在任务管理模块中执行调度策略后通过控制器接口将待执行任务交给控制器中的任务执行模块。控制器中的任务执行模块根据响应任务要求生产相应的流表项，流表项经过流表冲突检测模块解决流表项冲突后通过南向接口下发到 SDN 交换机。

2.2　接口规范设计

HYDRA 系统中的接口全部采用 REST API, 用 JSON 格式交换数据。HYDRA 系统的接口按功能可以分为 4 类：系统外部接口、系统北向接口、系统控制层内部接口以及系统南向接口。

1) 系统外部接口。该接口对 CHAIRS 系统开放，根据功能可分为下行接口和上行接口。下行接口主要功能有案件接收、案件解析和任务路由。上

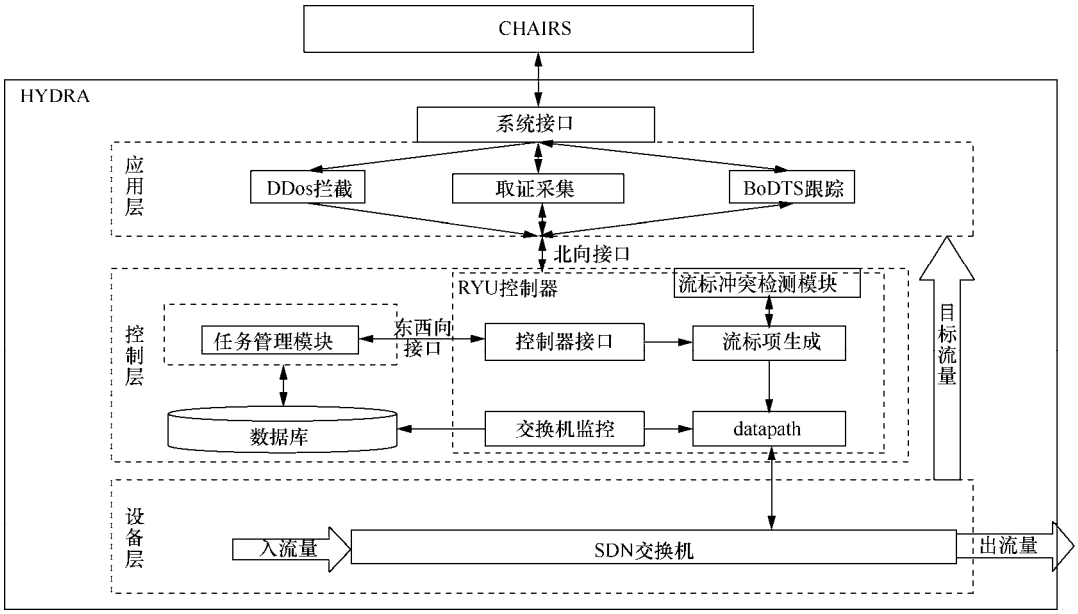

图 1　HYDRA 系统结构

行接口主要功能是将应用层响应模块的响应结果反馈给 IDS。系统外部接口如图 2 所示。

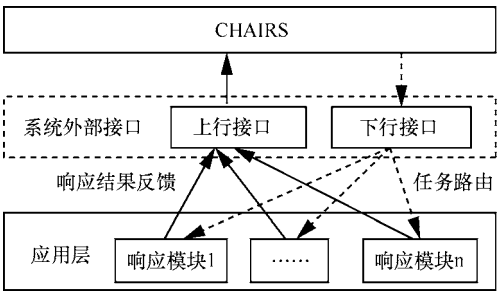

图 2 HYDRA 系统外部接口

2) 系统北向接口。系统北向接口即为应用层和控制层之间的接口。北向接口也是双向接口，下行接口主要功能是将应用层响决策模块生成的响应任务发送到控制层响应任务管理模块处理，上行接口负责将控制层必要的任务执行结果反馈到应用层任务响应模块。系统北向接口如图 3 所示。

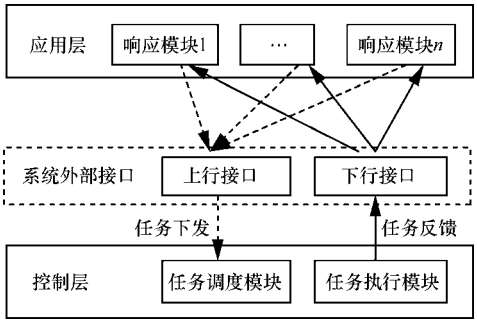

图 3 HYDRA 系统北向接口

系统北向接口的设计目标是使应用层的应用能够方便地获得调用底层资源的能力。因此北向接口的设计需要根据具体的应用需求来定，具有多样化的特征。针对不同的应用需要不同的接口数据结构。表 1 和表 2 分别为当前系统支持的取证采集任务和 BoDTS(botnet detect and tracking system,僵尸网络检测和追踪系统)追踪任务的接口数据结构。

3) 系统控制层内部接口。系统响应任务到达控制层后首先经过任务调度模块调度处理，然后发往控制器中的执行模块，这里需要控制层之间的接口。控制层内部接口也是双向接口，从任务调度模块到任务执行模块方向的接口负责响应任务的提交，从任务执行模块到任务调度模块方向的接口负责响应任务执行情况的反馈。HYDRA 系统控制层内部接口如图 4 所示。

表 1 取证采集任务接口数据结构

字段名	类型	描述	备注
ticketed	long	应用标识符	取证采集任务标识
priority	long	任务优先级	
flowdirection	int	流向标识符	出入流量标识符
srcport	int	源端口号	
dstport	int	宿端口号	
srcipdstip	int	源宿 ip 关系	0 表示或，1 表示且
srcportdstport	int	源宿端口关系	0 表示或，1 表示且
protocol	int	ip 协议号	
hard_time	int	任务持续长	单位：s
thresholdpkts	int	采集报文阈值	
iplist	list	追踪 ip 列表	

表 2 BoDTS 任务接口数据结构

字段名	类型	描述	备注
taskID	long	应用标识符	Bodts 应用唯一标识
priority	long	任务优先级	
starttime	long	任务开始时间	0 表示立即执行
outport	int	交换机输出端口	
matchfield	list	Bodts 目标流量特征	

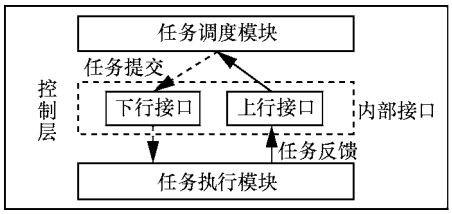

图 4 HYDRA 系统控制层内部接口

4) 系统南向接口。由于 HYDRA 采用 ONF 提出的基于 openflow[7-8]协议的南向接口，该接口功能由控制器提供，所以 HYDRA 系统南向接口的设计和实现不在本文的讨论范围之内。

2.3 任务管理模块设计

HYDRA 系统的目标是设计成一个支持多任务响应的网络安全应急响应平台，这里的多任务不仅指任务的数量多，同时任务类型也是非单一的。因此当网络安全事件经过系统应用层相应的响应决策模块处理成响应任务到达控制层后，需要有一个完善的管理机制保证这些响应任务能够正常执行。在任务管理模块中，包括任务建立、任务调度和任务撤销 3 个过程。

其中任务调度是任务管理模块的核心，对于一个面对多类型响应任务的系统，到达系统的响

应任务数量是不可控的，因此考虑到在出现系统资源不足的情况下，后续任务即使到达系统，也无法执行。因为资源的有限性，必须按照一定的原则有选择的让一部分响应任务得到执行。考虑到系统不同类型任务重要性是有所差别的，例如应急响应任务的重要程度一般要比普通采集任务的重要程度高，同类型响应任务的优先级也可能会不一样，因此采用基于优先级的调度策略。考虑到固定优先级调度策略可能导致低优先级任务饥饿问题以及避免某些长时间持续的任务长期占用系统资源，HYDRA 系统将采用基于动态优先级的可抢占式调度策略。

由于 HYDRA 是面向多响应任务类型的系统，不同响应任务提供的优先级仅能代表某一种类型响应任务的重要性，在系统控制层需要从全局的角度对不同类型的响应任务的重要性重新定义，因此需要重新设计响应任务优先级。响应任务的优先级设计如图 5 所示。

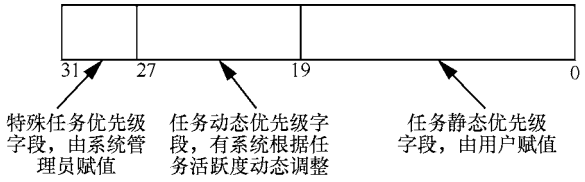

图 5　任务优先级字段

这种优先级字段划分的方案有两方面优点，一方面提高了任务调度的灵活性，另一方面简化了实现细节，因为不同字段有不同权值，调度的时候不需要对细节做过多讨论，直接比较优先级字段的值即可。具体的调度过程如图 6 所示。

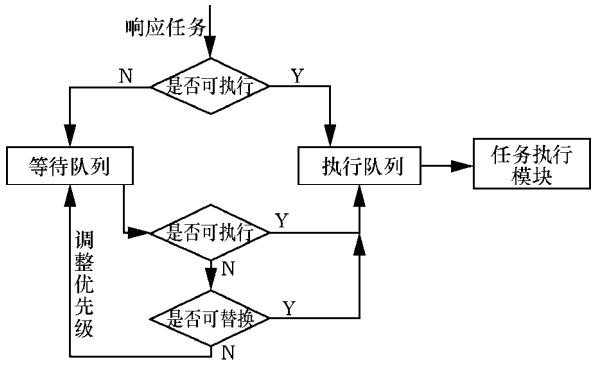

图 6　响应任务调度过程

根据图 6，在一个调度周期内，调度线程从等待队列中按优先级次序取出当前满足执行条件的任务，然后判断当前系统剩余资源是否能够满足该任务，如果满足加入执行队列送往控制器中的任务执行模块，否则执行任务替换算法，到当前执行队列中找到优先级较低的任务取而代之。如果无法找到合适的替换任务，提高该任务优先级，重新加入等待队列，等待下一个调度周期的调度。

2.4　控制器功能拓展设计

系统采用的 SDN 控制器是 RYU，目前只使用了其提供的 API 将流表项规则下发到交换机的功能，但这无法满足复杂的任务需求。因此为了充分挖掘 RYU 控制器的潜力，将系统的任务执行模块迁移到控制器中，通过对 RYU 的功能扩展和 RYU 提供的丰富组件来完成响应任务的执行工作。任务执行模块主要包括流表项生成模块和交换机监控模块。

流表项生成模块主要功能是监听自定义的 RYU 事件，根据不同的事件做不同的操作。对于任务执行事件，根据事件中任务信息，按照 openflow 协议从任务信息中提取流表项信息，然后将生成的流表项构造 openflow 消息，然后由 RYU 控制器通过南向接口将流表项下发到交换机执行相应的任务。

交换机监控模块是一个相对独立的 RYU 应用，主要功能是不断向交换机发送 openflow 协议中定义的状态请求消息，交换机收到该消息后会自动将流表项统计信息封装到状态回复消息返回，进而可以获取当前交换机中的流表项统计信息。

3　系统实现与实验

HYDRA 系统的目的就是为了帮助管理员实现对网络安全事件的自动化响应，接下来会通过一个案例来展现系统自动化响应的效果。同时，HYDRA 是面向多任务类型的系统，当任务类型及数量较多时，就需要进行任务调度，接下来会对系统的任务调度策略进行评估，进而判断策略的优劣。

3.1　自动化响应案例

HYDRA 系统目前支持的响应任务有 2 种，分别是取证采集任务和 BoDTS 追踪任务。以取证采集任务为案例，响应大体流程如图 7 所示。CHAIRS 系统先将响应案件信息发到 HYDRA 系统外部接口，然后将接收到的案件以系统定义的任务格式发送到响应任务管理模块，经过该模块调度后提交给控制器响应任务执行模块执行，响应执行模块将目标流量特征翻译成 openflow 流表项下发到交换机，

实现对目标流量的采集，最后将结果反馈给 CHAIRS，做进一步的分析。

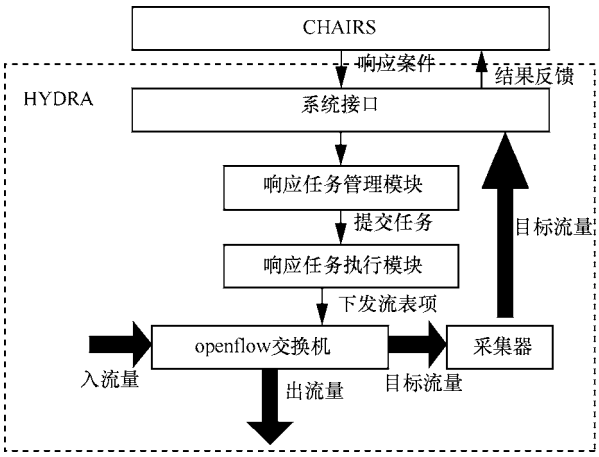

图 7 取证采集任务响应流程

对一个正在响应的取证任务 21 184 进行跟踪，图 8 和图 9 为跟踪结果。图 8 表明任务进入 HYDRA 系统并处于运行状态。图 9 为取证任务 21 184 在交换机中生成的流表项。图 10 为取证任务 21 184 对应的安全事件在 CHAIRS 中的反馈概要。图 11 为取证任务 21 184 在 CHAIRS 系统中的具体反馈结果，该结果显示当前 HYDRA 系统已为该安全事件采集了 3.18 MB 的可疑报文，并从这些报文中检测到了 2 822 条警报。

图 8 取证任务 21 184

图 9 取证任务 21 184 对应的流表项

图 10 取证任务 21 184 在 CHAIRS 系统反馈结果 1

图 11 取证任务 21 184 在 CHARIS 系统反馈结果 2

3.2 任务调度策略的评估

首先，先从理论上分析对比 FIFO(first iput first outpwt)调度策略和基于静态优先级可抢占式调度策略以及基于动态优先级可抢占式调度策略 3 种调度策略，来证明系统采用的基于动态优先级可抢占式调度策略的优越性。然后根据系统实际情况来展示任务调度策略的可行性和优越性。

确定一个响应任务的调度过程需要的几个时间属性：1) 到达时间：任务到达系统的时间点。2) 服务时间：任务执行需要的时间。3) 开始时间：任务第一次获得执行权的时间点。4) 完成时间：任务完成的时间点。然后评估一个任务调度的效率有 2 个指标：1) 任务周转时间=完成时间−到达时间；2) 任务带权周转时间=$\frac{\text{周转时间}}{\text{服务时间}}$。为了减少理论分析的复杂度，先不考虑系统资源对任务的限制情况，系统同一时刻只能执行一个任务。假设系统将要接收 5 个任务，任务相关属性如表 3 所示。

表 3 模拟任务属性

任务	到达时间	服务时间	优先级
A	0	4	3
B	1	3	4
C	2	5	1
D	3	2	3
E	4	4	5

对于 FIFO 调度策略，其调度结果如表 4 所示。对于静态优先级可抢占式调度策略，其调度结果如表 5 所示。对于动态可抢占式调度策略，因为涉及优先级的改变，这里约定一下优先级调整策略：对于被抢占执行权的任务，优先级−1，对于等待队列中的任务，每等待 3 个时间单位优先级+1。其调度结果如表 6 所示。

表 4　　FIFO 调度策略结果

任务	到达时间	服务时间	优先级	开始时间	完成时间	周转时间	带权周转时间
A	0	8	3	0	8	8	1
B	1	4	4	8	12	11	2.75
C	2	5	1	12	17	15	3
D	3	2	3	17	19	16	8
E	4	4	5	19	23	19	4.75
平均时间						13.8	3.9

表 5　　静态优先级可抢占式调度策略结果

任务	到达时间	服务时间	优先级	开始时间	完成时间	周转时间	带权周转时间
A	0	8	3	0	16	16	2
B	1	4	4	1	9	8	2
C	2	5	1	18	23	21	4.2
D	3	2	3	16	18	15	7.5
E	4	4	5	4	8	4	1
平均时间						12.8	3.34

从结果来看，FIFO 调度策略的平均周转时间和平均带权周转时间都是最长的，并且后续高优先级任务并没有得到优先执行权。将策略改进成基于静态优先级的调度策略后，平均周转时间和平均带权周转时间有所改进，但是静态优先级的缺点是可能出现“饥饿”现象，即低优先级任务长期得不到执行。经过对静态优先级调度策略调整后，基于动态优先级的可抢占式调度策略的平均周转时间和平均带权周转时间又有所进步。故得出结论：基于动态优先级可抢占式的调度策略优于 FIFO 调度策略。

目前，HYDRA 系统从 CHAIRS 系统处获取的取证采集任务数量将近 2 000 个，由于 SDN 交换机的流表资源有限，最多容纳流表项数不超过 1 K。这导致系统无法将任务同时转换成流表规则，下发到交换机。因此需要采用相应的任务调度策略，保证部分任务先得到执行。基于上面的理论分析，然后结合系统实际运行情况，可以得到不同策略下，平均带权周转时间与任务数量的关系。不同策略下的调度效果如图 12 所示。

根据图 12 可知，当任务数量不超过 500 时，流表资源充裕，可以并行执行全部任务。当任务数量超过 500 时，流表资源无法同时满足所有任务，这时就要触发任务调度机制，很明显动态优先级调度策略的平均带权周转时间最短，适用于作为本系统的任务调度策略。

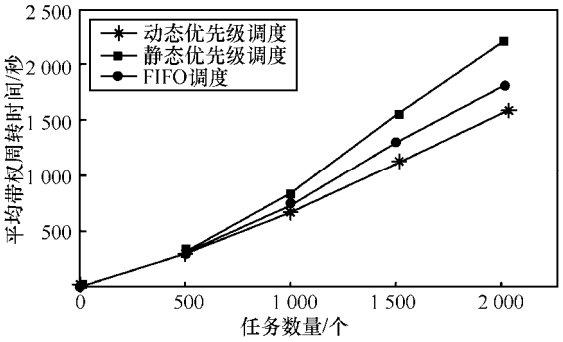

图 12　不同策略下的调度效果

4　结束语

本文结合 CERNET 南京主节点的实际需求，针对现有系统的不足，基于 SDN 架构，提出并实现一个松耦合的系统，将响应决策放与响应执行分开，增加了系统的可扩展性。设计了 RESTful

表 6　　动态优先级可抢占式调度策略结果

任务	到达时间	服务时间	优先级	开始时间	完成时间	周转时间	带权周转时间
A	0	8	3→2→3→4→5	0	18	18	2.25
B	1	4	4→5	1	9	8	2
C	2	5	1→2→3→4	18	23	21	4.2
D	3	2	3→4→5	9	11	8	4
E	4	4	5	4	8	4	1
平均						11.8	2.69

的北向接口，加入基于动态优先级的任务调度模型，使得系统能够响应更多、类型更丰富的响应请求。对 RYU 控制器的改造加大了控制器在系统中的作用，也为进一步挖掘控制器潜能打下了基础。

参考文献：

[1] 杨望. 安全事件响应:自动化引领未来[J]. 中国教育网络, 2017(8):53-54.

[2] SHIN M K, NAM K H, KIM H J. Software-defined networking (SDN): A reference architecture and open APIs[C]// International Conference on ICT Convergence. IEEE, 2012:360-361.

[3] 朱礼智，龚俭. 分布式网络应急响应管理系统 CHAIRS 的设计与实现［D］. 南京：东南大学计算机科学与工程学院，2015.

[4] 金磊，龚俭. 基于 SDN 技术的网络入侵阻断系统 HYDRA 的设计与实现［D］. 南京：东南大学计算机科学与工程学院，2016.

[5] Open Networking Foundation. OpenFlow Switch Specification Ver 1.3.5 [S]. 2015.

[6] 左青云，陈鸣，赵广松. 基于 OpenFlow 的 SDN 技术研究[J].软件学报，2013,24(5): 1078-1097.
ZUO Q Y, CHEN M, ZHAO G S, Research on SDN technology based on OpenFlow[J]. Journal of Software, 2013, 24(5): 1078-1097.

[7] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[8] CAI Z. Design and implementation of the maestro network control platform[J]. Dissertations & Theses-Gradworks, 2009.

［作者简介］

程俊（1994–），男，河南固始人，东南大学硕士生，主要研究方向为软件定义网络。

龚俭（1957–），男，上海人，博士，东南大学教授、博士生导师，主要研究方向为网络安全、网络管理。

杨望（1979–），男，安徽宣城人，博士，东南大学讲师，主要研究方向为网络安全、网络管理。

臧小东（1985–），男，山东济宁人，东南大学博士生，主要研究方向为网络安全、网络管理。