综述

SDN 架构及安全性研究 *

王淑玲[1],李济汉[2],张云勇[1],房秉毅[1]
(1.中国联通集团研究院 北京 100048;2.北京邮电大学 北京 100876)

摘 要:随着云计算、移动互联网等新技术的发展和成熟,网络业务的多样化、基础资源能力的大力提升等给数据中心网络的可扩展性、可管理性、安全性等提出了新的要求。SDN 体系架构的出现为目前网络问题的解决提供了新的方向,因而在产业界和研究领域得到了深入的研究和应用。但随着 SDN 相关网络设备的出现,安全问题成为制约其发展的一个重要因素。本文首先分析了 SDN 架构的产生背景,阐述了 SDN 的网络技术架构原理及目前的发展现状;随后对 SDN 架构中的安全特点、安全威胁进行了分析;最后,提出了一种 SDN 架构下的安全技术框架,从威胁分析、防御规则、防御方法 3 个方面对 SDN 中的安全问题提出了建议。

关键词:软件定义网络;安全;OpenFlow
doi: 10.3969/j.issn.1000-0801.2013.03.020

Research on SDN Architecture and Security

Wang Shuling[1], Li Jihan[2], Zhang Yunyong[1], Fang Bingyi[1]
(1.China Unicom Research Institute, Beijing 100048, China;
2.Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: With the rapid development of cloud computing and mobile internet, the features that network exhibits, such as diversity, declare for urgent requirements for scalability, manageability and security of the data center. The SDN architecture shows a promising way of dealing with the above requirements of network through revolutionary innovation of the traditional network architecture, which attracts great interest of companies and research institutes. However, according to the recent research and progress of SDN, security problem has not been addressed, which will be a significant issue. Based on the situation, the basis of SDN, including the origination, architecture, standardization work and standardized protocol, were described, and the security issue was also analyzed. In the security part, the exhibiting new features of security problem for SDN, were analyzed, by listing the undergoing work, and then the security threats in SDN were concluded. Finally, a suggested architecture for security research of SDN was proposed.

Key words: software defined network, security, OpenFlow

1 引言

云计算、移动互联网等相关技术的兴起和发展加快了数据中心的变革进程,网络带宽需求的攀升、网络业务的丰富化、服务交付的个性化需求等都给新一代数据中心提出了更高的要求。面对日趋复杂的网络环境,传统的以 IP

* 国家自然科学基金资助项目(No.1172134),"新一代宽带无线移动通信网"国家科技重大专项基金资助项目(No.2012ZX03002001-002,No.2013ZX03002004-002,No.2013ZX03002003-005)

为核心的数据中心网络架构的局限性逐渐凸显出来。为了适应今后互联网业务的需求,业内形成了“现在是创新思考互联网基本体系结构、采用新的设计理念的时候”的主流意见[1],并对未来网络的体系架构应具备的性质和功能提出了要求[2]。近年来,软件定义网络[3](software defined network,SDN)的兴起为未来网络的发展提供了方向。

SDN 的思想起源于斯坦福大学的 Clean State[4]项目,此后随着技术的发展和研究的深入,SDN 架构从实验室走向了产业界,并得到了学术界和工业界的广泛认可,且进一步推进了 SDN 的产业化演进和相关技术的标准化进程。

SDN 技术架构通过把原有封闭的体系解耦为数据平面、控制平面和应用平面,将网络控制功能从网络设备中分离出来,并为网络应用提供可编程的接口,从而革命性地改变了现有的网络架构。在数据中心采用 SDN 架构,可以方便地实现路由路径的优化、网络维护代价的降低、网络设备利用率的提高、网络设备的可管理性和灵活性的增加等。

但在当前的环境下,SDN 的发展面临着许多关键性问题,安全就是其中之一,并且随着 SDN 架构的普及和推广,安全问题的重要性呈逐步上升的趋势。目前,SDN 的安全问题也引起了工业界的关注,企业组织、研究团体及标准化组织都纷纷启动了相关方面的研究工作。

基于 SDN 的强劲发展势头和解决安全问题的迫切性,本文首先阐述了 SDN 技术架构的原理、发展现状,分析了 SDN 技术架构中存在的安全问题,并给出了相应的安全防护建议,以期为 SDN 安全方面的科研和产业发展做出有益的探索。

2 SDN/OpenFlow 技术原理和现状

2.1 SDN/OpenFlow 的起源

SDN 的思想起源于斯坦福大学的 Clean State[4]项目。该项目旨在创建一个全新的互联网架构,使其摆脱当今互联网基础架构的限制,采纳新技术,支持新应用、新服务,提供创新服务平台。作为 Clean State 项目在企业网安全方面的一个子项,Martin Casado 和其他几位团队成员提出了 Ethane 架构,通过一个中央控制器向基于流的以太网交换机下发策略,从而对流的准入和路由进行统一管理,实现基于网络流的安全控制策略。受到该项目的启发,Martin 和他的导师 Nick McKeown 教授发现,如果将 Ethane 架构设计得更一般化,将传统网络设备的数据转发和路由控制两个功能模块分离,通过集中式的控制器以标准化的接口对各种网络设备进行管理和配置,那么将为网络资源的收集、管理和使用提供更多的可能性,从而更容易推动网络的革新和发展。于是,提出了 OpenFlow 的概念,并在 2008 年发表了题为“OpenFlow: Enabling Innovation in Campus Netwrok”的论文,详细描述了 OpenFlow 的工作原理,并列举了 OpenFlow 可使用的应用场景,包括创新性结构网络的测试、网络管理和访问控制、VLAN 等。基于 OpenFlow 为网络带来的可编程的特性,Nick 和他的团队进一步提出了 SDN 的概念。

2.2 SDN 技术架构

SDN 是一种新兴的控制与转发相分离并直接可编程的网络架构,其核心思想是将传统网络设备紧耦合的网络架构解耦成应用、控制、转发 3 层分离的架构,通过标准化实现网络的集中管控和网络应用的可编程,如图 1 所示。

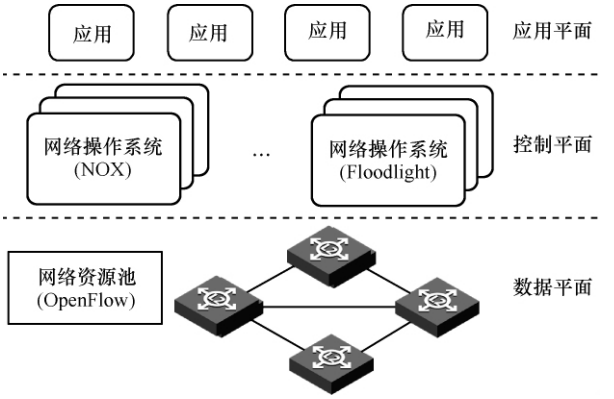

图 1 SDN 技术架构

在这一架构下,开放和标准化是核心关键点,表现为:标准化数据面与控制面的接口(又称为南向接口),屏蔽网络基础设施资源在类型、支持的协议等方面的异构性,使得数据面的网络资源设施能够无障碍地接收控制面的指令,承载网络中的数据转发业务;标准化控制层和应用层的接口(又称为北向接口),为上层应用提供统一的管理视图和编程接口,使得用户可以通过软件从逻辑上定义网络控制和网络服务。

SDN 的技术架构改变了网络在产业链结构中的价值,实现了从成本中心至核心竞争力的转变。基于 OpenFlow 的 SDN 技术带给企业和用户更加灵活的网络管控、更高效的资源利用率、更弹性的资源调度,具体介绍如下。

- 更加灵活的网络管控：首先，标准化的南向接口屏蔽了设备的异构性，实现了异构网络设备的集中化统一管控；其次，SDN 控制器能够实现网络的统一管控，无需手动地更改每一个网络设备的配置。
- 更高效的资源利用率：由于 SDN 控制器监控着网络基础设施的状态，能够更加智能和灵活地调配网络资源，减少盲目的网络资源投资，提高资源利用率。
- 更弹性的资源调度：应用层可通过标准的北向接口制定符合其业务需求的网络策略，由 SDN 控制器将策略配置到网络设备中，实现资源的弹性调度。

2.3 SDN 的相关标准

开放网络基金（open network foundation，ONF）协会由德国电信、Facebook、Google、Microsoft、Verizon、Yahoo！等 7 家公司联合推进，组建起来的一个非盈利性的组织机构，致力于发展创新型网络结构 SDN，并积极推进 SDN 架构的标准化和商业化进程，是国内外从事 SDN 相关标准研制工作较为权威的组织之一。目前，ONF 拥有 7 家董事会单位、70 多家成员单位，包含 Extensibility、Configuration & Management、Testing & Interoperability、Hybrid、Market Education、Architecture & Framework、Forwarding Abstractions 共 7 个工作组以及 Northbound API、Transport、Skills Certification 等讨论组。标准的讨论范围涵盖 SDN 的南向接口、北向接口、市场应用、控制器等各个方面。截至 2012 年 12 月，ONF 协会发布的标准包括 OpenFlow 规范和 OpenFlow 管理配置协议。

OpenFlow 规范是 SDN 技术架构中控制平面和数据平面间的第一个通信标准。自 2010 年年初发布第一个版本 OF1.0[5]以来，OpenFlow 逐步完善，先后经历了 OF1.1、OF1.2 版本。同时，各设备厂商也积极推动支持 OpenFlow 标准的交换机的研发和生产。

OpenFlow 规范的技术架构如图 2 所示，主要定义了交换机的功能模块以及其与控制器之间的通信信道方面的接口。通过该接口，OpenFlow 控制器将制定好的转发策略通过安全的通信信道发送给交换机，对交换机处理流的方式进行控制。具体的控制策略是由流表（FlowTable）和表项来表示的。每个交换机可以有一个或多个流表，从 0 开始依次编号。编号的大小标明了流表的跳转顺序，只能从编号小的流表依次或越级跳转至编号大的流表。每个流表又包含一系列的流表项，每条流表项由匹配域（match field）、计数域（counter）和指令（instruction）等字段组成。在流表项

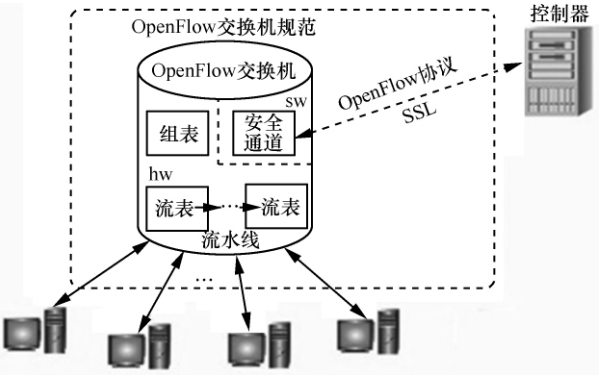

图 2 OpenFlow 技术架构

中，可以根据网络分组在 L2、L3、L4 等网络报文头的任意字段进行匹配，如以太网帧的源 MAC 地址、IP 分组的 IP 地址等。在 OpenFlow 的未来计划中，还支持对整个数据分组的任意字段进行匹配。当数据分组进入流表后，必须从流表 0 开始向后进行匹配。如果数据分组与流表 i 的某条表项匹配成功，则首先更新该表项对应的计数器（更新匹配数或者匹配字节数等），然后根据该表项定义进行数据分组的处理，包括启动后续流表的匹配、执行数据分组的操作等。如果数据分组已处于最后一个流表，并且仍未匹配任何规则，则执行默认设置，如转发数据分组到控制器或丢弃。

OpenFlow 管理配置协议的目的是规范支持 OpenFlow 交换机中的数据流配置，保证数据流在 SDN 控制器、OpenFlow 交换机之间的顺利传输。OpenFlow 管理配置（OF-Config）协议与 SDN 其他组成部分的关系如图 3 所示。

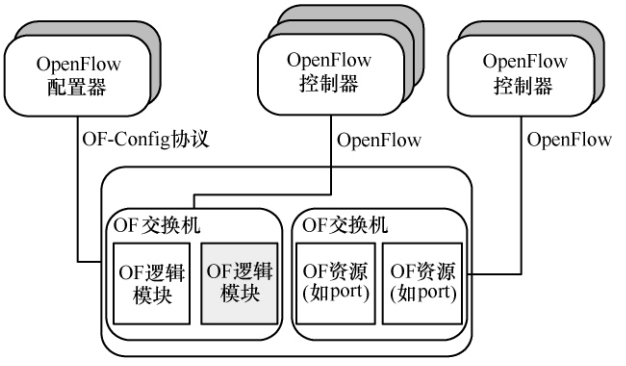

图 3 OpenFlow 管理配置协议在 SDN 架构体系中的位置

3 SDN 安全的特点

SDN 架构实现了传统网络架构中网络管理功能的集中，是对传统网络架构的革命性创新。这种创新除了带来管理、运营等方面的灵活性，也使得 SDN 中的安全问题呈

现出其特有的特点。

SDN 安全问题的独特性与 SDN 的管理集中性和开放性是密不可分的。

管理集中性使得网络配置、网络服务访问控制、网络安全服务部署等都集中于 SDN 控制器上。攻击者一旦成功实施了对控制器的攻击,将造成网络服务的大面积瘫痪,影响控制器覆盖的整个网络范围。在 SDN 的这种架构下,攻击者的攻击对象愈来愈集中,极大地降低了攻击难度。同时,云计算的发展为攻击者提供了超大规模计算能力,对于原来只有资金雄厚的大型组织才能实施的网络攻击任务,普通用户在云计算平台的支持下,也可以轻松实现攻击。

开放性是 SDN 的另一个重要特征,是 SDN 实现统一管理、配置异构网络设备、提供可编程特性的重要原因。但开放性也使得 SDN 面临着更多的安全威胁。首先,开放性使得 SDN 控制器的安全漏洞、策略的不完备性等充分地暴露在攻击者面前,给予了攻击者足够的信息制定攻击策略。其次,SDN 架构通过 SDN 控制器给应用层提供大量的可编程接口,这个层面上的开放性可能会带来接口的滥用,如引发 DDoS 攻击等,因而需要对应用层制定准入策略,防止意图不轨的攻击者利用开放接口实施对网络控制器的攻击。最后,开放性使得 SDN 控制器需要谨慎评估开放的接口,以防止攻击者利用某些接口进行网络监听、网络攻击等。

SDN 的网络架构特性使得 SDN 呈现出以下 3 个特点。

- 在传统的网络架构中,网络安全控制集中于 OSI 体系架构的 4~7 层,在 SDN 架构下,通过控制器可以实现 2~7 层的安全策略配置,提供了更加细粒度的安全控制。
- SDN 的安全威胁将更加集中,而不是传统的分散在网络中各个相关的网元部分。
- SDN 的安全威胁将更加不可视化。随着网络控制权从用户到网络控制器的更迭,用户对于自己的网络状态将越来越不能很好地监控。

4 SDN 安全现状

随着 SDN 研究的深入和厂商的大量参与,SDN 的安全问题越来越受到重视。

2012 年 11 月 4 日,互联网工程任务组(IETF)的SAAG(Security Area Advisory Group)发布了 SDN 架构中的安全要求,主要探讨 SDN 控制器和应用层之间的安全要求,包括控制器与应用层的安全接口、认证、授权,应用与内嵌应用之间安全策略的可见性等安全问题[6],但并未给出 SDN 中安全威胁的应对方案。

随着虚拟化技术的深度应用,产业界内已经有较为成熟的计算资源、存储资源的虚拟化解决方案,而且虚拟化给各组织带来的管理灵活性、高效率、低成本等优势也日渐凸显,但目前网络和安全仍然固化在单一的设备上,未与计算等基础设施资源的发展步调保持一致,因而成为云计算高速发展下强有力的制约因素。为此,VMware 公司率先推出 vCloud,提供了一套功能完整的云计算基础设施解决方案,可用于构建和管理能够满足 IT 最重要需求的完整的云计算基础架构。

其中,vCloud Networking & Security 组件(如图 4 所示)是一个关键的安全组件,从终端、虚拟数据中心内部、虚拟数据中心边缘保护虚拟化数据中心,防止其受到攻击和滥用。在终端层面,通过限制授权应用的网络访问、敏感数据的授权访问以及安全管理流程的制定 3 方面,保证虚拟桌面部署的安全;在虚拟数据中心内部,通过加强内部虚拟机间的通信控制,实现自适应的信任区域保护和隔离,保证敏感业务信息不泄露,以提供安全可靠的网络服务;在虚拟数据中心边缘,通过集成式的防火墙和网管服务,隔离数据中心外部的安全威胁,提供敏捷、可信赖的数据中心服务。

5 SDN 安全的挑战

尽管 SDN 架构可以解决数据中心的网络管理、运营维护和成本问题,但从目前的发展阶段来看,SDN 技术的应用还需要长时间的发展和普及,尤其是 SDN 中的安全问题,将成为制约 SDN 架构商用化和普遍推广的一个决定性因素。

从 SDN 的架构来看,SDN 中的安全问题主要集中在控制平面和应用平面。

(1)控制面的安全

集中化的控制面承载着网络环境中的所有控制流,是网络服务的中枢机构,其安全性直接关系着网络服务的可用性、可靠性和数据安全性,是 SDN 安全首先要解决的问题。在控制面中,面临的威胁包括以下方面:

- 网络监听,攻击者从 Internet 上获取控制器的网络切入点后,对控制器上的控制信令进行伪造和修改,威胁网络资源的配置;

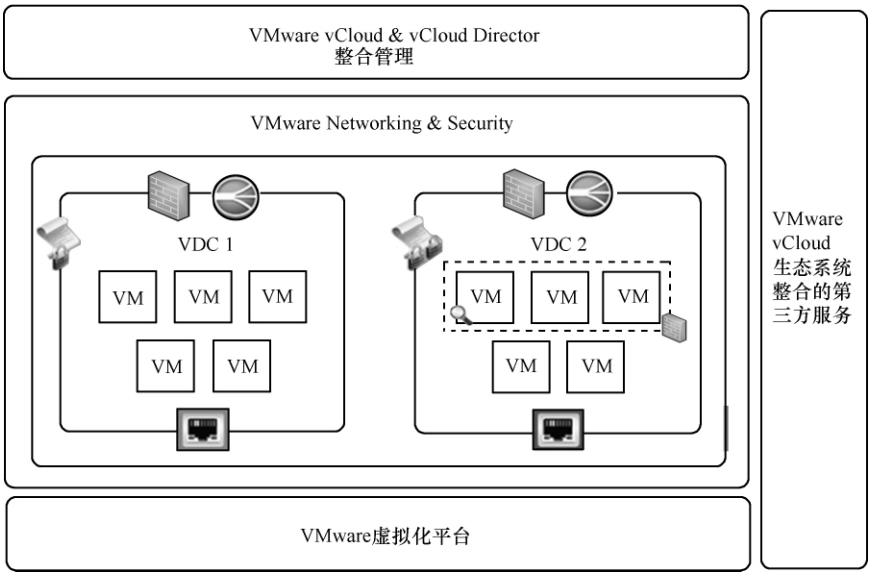

图 4 VMware vCloud Networking & Security 组件技术架构

- IP 地址欺骗,攻击者通过网络监听,将其伪造的控制信令 IP 地址篡改为控制器的 IP 地址,骗取交换机的信任,对网络进行破坏;
- DDoS 攻击,攻击者向控制器发送多个服务请求,并且所有请求的返回地址都是伪造的,直到控制器因过载而拒绝提供服务;
- 病毒、蠕虫及木马攻击,攻击者通过控制器中存在的漏洞,获取控制器的控制权,执行恶意代码等。

(2)应用面的安全

随着 SDN 的推广和发展,应用层将通过应用提供各种复杂的网络服务,安全问题也将随之而来。主要包括以下两种。

- 恶意应用:通过在应用层的应用中植入蠕虫、间谍程序等,达到窃取网络信息、更改网络配置、占用网络资源等目的,从而干扰控制面的正常工作进程,影响网络的可靠性和可用性等。
- 应用的安全规则冲突:为了提供各类网络服务,应用层需要制定安全规则,以访问控制器的某些安全接口。随着应用的复杂化,多个应用之间会出现安全规则冲突,从而带来网络服务的混乱和增加管理复杂度。

6 SDN 安全技术框架建议

为了构建安全的 SDN,需要对 SDN 中的设备、应用、安全策略、服务管理等进行有效管理,并针对 SDN 中易于受到安全攻击的控制器进行重点监控,及时发现和排除异常情况。为此,本文从威胁分析、防御规则、防护方法 3 方面对 SDN 中的安全问题进行分析,构建了如图 5 所示的安全技术框架。

数据层面的安全性策略控制等都由控制器负责配置和管理,并通过控制器下发的控制指令执行。

在易于受到攻击的控制器层面,首先,需要制定一系列严密的授权、访问控制、安全管理等规则;其次,能够及时对感知到的异常网络设备、异常行为进行隔离,避免造成大范围的破坏;最后,控制器需要具备分析网络行为的能力,从日志、流量、当前服务等状态分析网络行为的特征,对于异常的网络行为需及时报警和隔离。

在应用层面,首先,制定一系列安全服务准入规则,对应用提供的服务、需要控制器提供的接口等进行鉴定,负责规则的应用才允许成为 SDN 中合法的应用;其次,利用可编程的接口,针对目前存在的安全威胁,利用已有的技术对安全威胁进行监控和排除,加强控制器的安全防护。

除此之外,安全技术架构还提出了跨越数据层、应用层、控制层的安全评价体系和安全管理。安全评价体系制定一系列的安全评价标准,对网络设备、服务、应用等的安全进行评价和分级,将安全级别低的应用或服务通知给控制器,由控制器执行相应的处理。安全管理通过可视化的

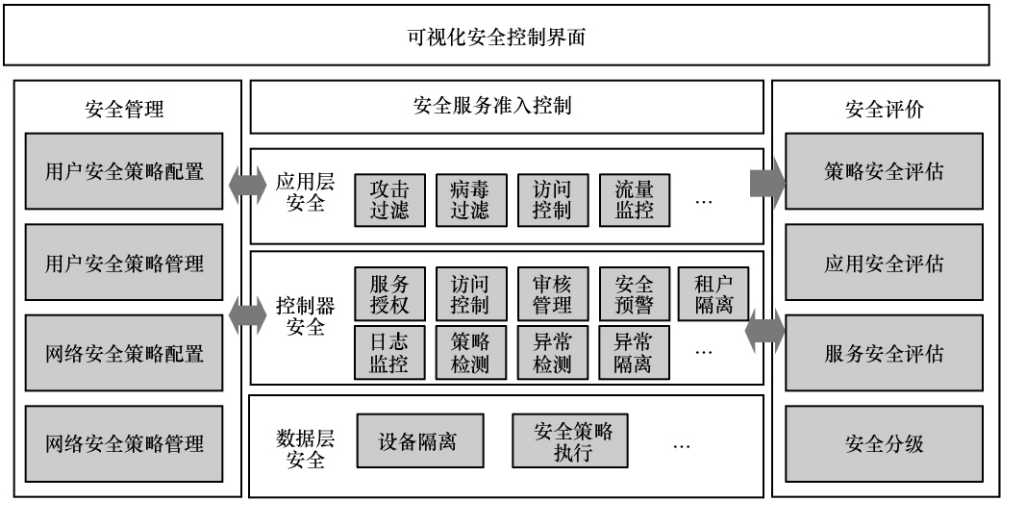

图 5　SDN 安全技术架构建议

控制界面,为不同的管理人员提供差异化的安全策略配置和管理。

7　结束语

在新的网络环境下,随着网络的可扩展性、灵活性、有效性等特性要求的提高,传统网络架构的局限性凸显。因而,SDN 架构从提出到现在，迅速地从实验室走向了产业界,引起了科研界和企业界的极大关注,相继出现了一系列的相关标准和设备。但 SDN 方面的安全研究仍处于起步阶段。本文首先分析了 SDN 的产生背景,阐述了其技术原理和发展现状，在此基础上，对 SDN 架构中的安全特点、安全威胁进行了分析,并提出了 SDN 安全技术架构建议，以期为 SDN 安全方面的科研和产业发展做出有益的探索。

参考文献

1　吕博. 网络虚拟化资源管理架构与映射算法研究. 北京邮电大学博士学位论文, 2011

2　林闯,贾子骁,孟坤. 自适应的未来网络体系架构. 计算机学报, 2012, 35(6)

3　ONF Market Education Committee. Software-defined networking: the new norm for networks.https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf, 2012

4　Clean slate. http://cleanslate.stanford.edu/, 2012

5　OpenFlow. OpenFlow configuration and management protocol OF-CONFIG 1.0. https://www.opennetworking.org/images/stories/downloads/of-config/of-config1dot0-final.pdf, 2012

6　IETF SAAG. Security requirements for software defined networks. http://www.ietf.org/ proceedings/85/slides/slides-85-saag-4

[作者简介]

王淑玲,女,博士,中国联通集团研究院工程师,主要研究方向为云计算、下一代网络。

李济汉,男,主要研究方向为人工智能、机器学习。

张云勇,男,博士后,中国联通集团研究院平台与云计算研究中心主任，教授级高级工程师,中国通信学会、电子学会、计算机学会高级会员,中国人工智能学会会员,主要研究方向为下一代开放网络、固定移动融合核心网、移动互联网及业务、公共运算。

房秉毅,男,博士,中国联通集团研究院高级工程师,主要研究方向为云计算、核心网新技术。

(收稿日期:2013-02-25)