



# 基于 SDN/NFV 的 DPI 智能化网络体系的构建

潘 洁<sup>1</sup>, 郝卓宁<sup>2</sup>, 林 鹏<sup>1</sup>

(1. 中国移动通信集团设计院有限公司 北京 100080;

2. 中国移动通信集团公司 北京 100033)

**摘 要:** DPI(深度分组检测)设备广泛应用于多种流量和业务分析系统,是完成流量识别和处理的第一步,并已经被广泛部署在现网中。随着 DPI 技术的不断深入,大量的 DPI 设备嵌入带来的管理和资本成本上升也日益凸显。在此基础上,阐述了传统 DPI 设备部署的现状和存在的问题,并基于 SDN/NFV 技术给出了更先进的嵌入 DPI 软件的新型智能化网络体系和部署方案。

**关键词:** 软件定义网络;网络功能虚拟化;DPI 部署;智能网络体系

**doi:** 10.11959/j.issn.1000-0801.2015143

## Construction of DPI Intelligent Network System Based on SDN/NFV

Pan Jie<sup>1</sup>, Xi Zhuoning<sup>2</sup>, Lin Peng<sup>1</sup>

(1. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China;

2. China Mobile Communications Corporation, Beijing 100033, China)

**Abstract:** DPI devices are widely used in a variety of analysis system of network traffic and business. It is the first step to complete the traffic identification and processing, and has been widely deployed in the network. With the development of DPI technology, the rise of administrative cost and capital cost brought by massive embedded DPI devices is also increasingly prominent. The current situation and existing problems of traditional DPI deployment scenarios were elaborated, and a more advanced intelligent network system and deployment scenarios with DPI software embedded on the basis of SDN/NFV technology were described.

**Key words:** SDN, NFV, DPI deployment, intelligent network system

### 1 引言

传统分组检测技术只分析 IP 分组的 4 层以下的内容(源地址、目的地址、源端口、目的端口以及协议类型),DPI(deep packet inspection,深度分组检测)<sup>[1]</sup>还增加了应用层分析,以识别各种应用及其内容。DPI 作为一种灵活有效

的业务识别技术,近年来已经在网络中得到了广泛使用。根据不同的管理检测要求,可以选择将设备部署在不同的网络位置。这样满足了对各种层次网络检测的要求,但是在不同的硬件平台上多次实现 DPI 技术所需成本高,同时应用程序之间的互通也比较困难。于是,如何解决这一问题成为新的研究热点。

收稿日期:2015-05-15;修回日期:2015-06-10

论文引用格式:潘洁,郝卓宁,林鹏. 基于 SDN/NFV 的 DPI 智能化网络体系的构建. 电信科学,2015143

Pan J, Xi Z N, Lin P. Construction of DPI intelligent network system based on SDN/NFV. Telecommunications Science, 2015143



近年来随着 SDN (software define networking, 软件定义网络) 和 NFV (network functions virtualization, 网络功能虚拟化) 技术的研究日渐成熟, 将 DPI 从嵌入的网络设备中解耦出来, 转成托管在标准服务器上的共享功能, 成为了解决上述问题的有效方法。这样 DPI 只需要在更少的机器上实现, 不仅减少了能源消耗, 而且可以有效地降低部署 DPI 所需的投资。同时, 不同功能和 DPI 应用程序之间的互通也将得到有效简化。

## 2 传统的 DPI 部署方案

根据不同的流量管理、检测要求, 可以选择在不同的网络位置部署 DPI 设备, 例如在城域网、省网、骨干网, 或者网间互联链路以及国际出口。控制位置不同, 控制要求和方式也不尽相同。例如, 在骨干网进行控制比在城域网控制对设备的性能和吞吐量等的要求都要高。下面以网间互联链路为例, 介绍常用的控制方式。

### 2.1 串接方式

串接方式是直接将 P2P 流量控制设备串接到网间互联链路中, 如图 1 所示。

这种方式一般是二层透传, 不需要配置 IP 地址。串接方式对设备性能、可靠性要求很高。串接方式的优点在于流量控制效果好, 利用令牌桶和流量整形可以精确地控制流量。但存在引入故障点的缺陷。为了增强设备的可靠性, 一般在设备前端配置光路保护器, 从而在流量控制设备需要升级或者出现故障时, 把对现网的影响降到最小。

### 2.2 并接方式

并接方式是用分光器将网间互联链路的光信号分一

部分到 DPI 设备, 不影响原链路中数据传输, 如图 2 所示。

采用并接方式部署 DPI, 传统的基于流量整形的流量控制和管理技术不再适用, 而是采用干扰的方式进行流量控制, 干扰分组将由流量控制设备发送到网络中。同时, 并接方式对 TCP (transmission control protocol, 传输控制协议) 流和 UDP (user datagram protocol, 用户数据报协议) 流采用不同的控制策略。由于 TCP 是面向连接的, 并接方式对其控制方式就是发送 reset 或 fin 分组, 拆除连接。对于无连接的 UDP, 并接方式目前对其还没有有效的控制方法, 常用的就是发送伪造分组, 劣化通信质量。

### 2.3 传统 DPI 部署的局限性

在选择接入方式时, 可以从以下几个方面考虑:

- 设备接入的法律风险;
- 流量控制功能的覆盖范围;
- 对加密业务的适应能力;
- 检控粒度的精确程度;
- 工程部署的合理性;
- 检控的时效性。

通常情况下, 采用串接方式进行 DPI 部署是更为合理和高效的方法, 也是目前运营商广泛采用的部署方案<sup>[2]</sup>。然而, 目前运营商在网络运营方面建设的系统, 对部署 DPI 进行数据和功能支撑的需求不断增加, 这也形成了层次丰富, 但功能集互有重叠的 DPI 部署结构。同时, 受相关应用系统的建设周期、集成厂商、投资预算以及 DPI 系统本身对外支持能力等因素影响, 当前的 DPI 系统建设重复性较强。例如, 某用户业务链路环境中, 为满足多个应用需求, 采用了统一分光, 独立部署各自 DPI 系统的方案, 如图 3 所示, 这样就造成了多个 DPI 系统并存的局面, 同时带来了

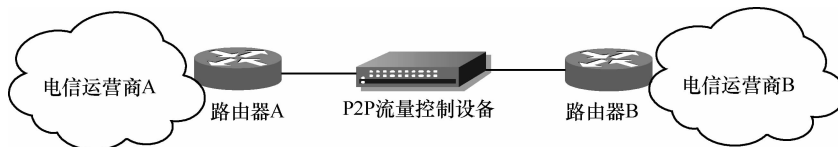


图 1 DPI 设备的串接方式

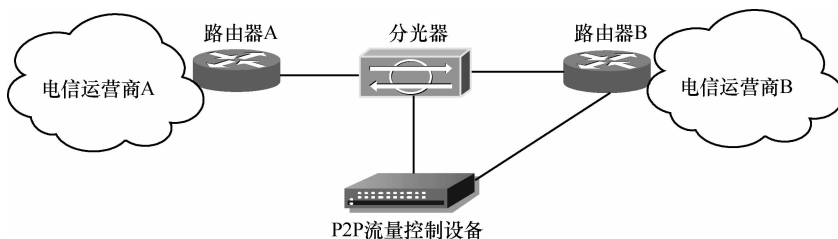


图 2 DPI 设备的并接方式

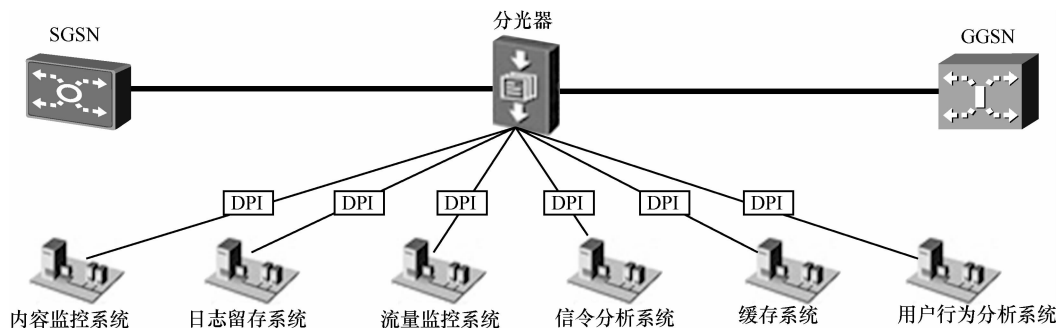


图3 多DPI系统并行接入拓扑

诸多方面的冗余。

### 2.3.1 重复投资

多个DPI系统并存将导致相同功能的重复购买,投资效益低下。

DPI系统的功能和应用方式是统一的,基本围绕解析报文协议字段内容、识别业务特征、采集指定特征报文、执行管理中心下发的流量管控策略等方面展开。各家厂商产品横向之间对比,区别在于设备架构设计、功能实现性能、对外支撑方式等。因此,重复购买的DPI系统,本质上超过70%的功能都能够被合并。这就使得面向DPI系统的重复投资产生了巨大的浪费。那么,如果集中精力投资建设一套功能丰富、性能优异,尤其是扩展和支撑能力强的DPI系统,即使初期投资规模大,但从长远考虑将能够实现节约投资,从而达到最高总体效益。

### 2.3.2 多方维护

多个DPI系统并存还增加了设备、系统维护的成本与难度。

每个厂商DPI系统都有各自的维护体系、操作界面和优化方法。即使能够通过外包、协作等方式降低运营商管理人员的工作强度,但对于多个系统的基本理解、外包工作的指导和考核合作伙伴绩效等工作,也会对管理实施人员带来极大困扰。当上层应用系统的功能需求发展时,DPI系统的功能升级、技术提升也必须随之提升。多套DPI系统并存就意味着要面向开发能力、持续发展能力不一的多个厂商展开技术提升,因此必将导致系统扩展/升级过程多头并进、参差不齐,会为系统的维护管理带来极大困扰。

### 2.3.3 网络整体安全存在隐患

多个DPI系统并存无谓地引入了系统环节,增加了系统故障机率。

为了给多个DPI系统提供原始流量,通常会采用在主

干链路上进行一级分光,然后通过光功率放大器附加多路分光的方案。显然,在流量真正被处理之前,系统就已经引入了多级分光和光放设备,这样增加了系统的不稳定性。同时由于在这种模式制约下,最终能够分流出的可用的光信号路数是有限的,因此能够获取到原始流量的应用系统数量是极为有限的。

## 3 在SDN/NFV网络中部署DPI

通过以上的分析,目前纷繁复杂的DPI部署,不管从经济方面、管理维护方面还是安全性方面都存在各种各样的问题,这就催生了将DPI功能从传统硬件中解耦出来的一系列技术方案。这里将介绍通过SDN/NFV技术实现这一目的的方法。

### 3.1 SDN/NFV技术及其对网络发展的影响

SDN和NFV是IT领域出现的有前景的新技术<sup>[3]</sup>。SDN通过将网络功能和业务处理抽象化,将网络业务的控制和转发进行了分离。这一技术屏蔽了来自底层网络的差异,使得网络的控制权得到解放。NFV则是在SDN的基础上,进一步将网络功能从特定硬件设备上解耦并托管于通用服务器上。这项技术通过功能抽象,实现资源充分灵活共享,进一步完成网络体系的智能化<sup>[4]</sup>。

#### 3.1.1 SDN技术与发展

SDN技术是网络虚拟化的一种实现方式,其核心是将网络控制与数据相分离,通过标准化实现网络的集中控制和网络应用的可编程,如图4所示。基于未来网络对灵活性更高的要求,SDN可以对网络设备的控制权进行集中管理,并在需要的时候进行有针对性的策略自定义,更好地完成网络的智能化。同时,由于控制层和数据层的分离,SDN可以通过各种上层应用更智能地操作数据流的路径,进行更细粒度的规则匹配和功能优化<sup>[5]</sup>。

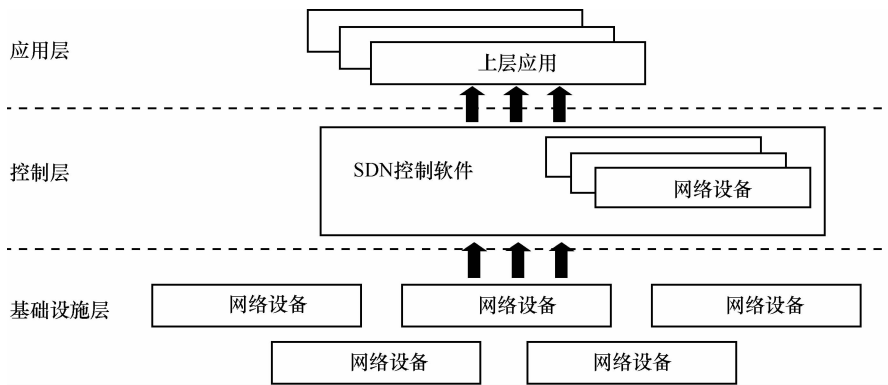


图4 SDN 架构

### 3.1.2 NFV 技术与发展

NFV 技术是能够与 SDN 相辅相成的一种虚拟化技术<sup>[6]</sup>。其通过将网络功能和业务应用从专用硬件设备中分离出来<sup>[7]</sup>,并托管于通用服务器上,完成软硬件的解耦,如图 5 所示。NFV 技术降低了功能和业务对专用设备的依赖性,为更灵活的管理网络功能和业务应用提供了条件并节约了巨大的成本投资。NFV 是非常适合运营商的一项技术,在 SDN 解决网络全局抽象视图的集中整体控制和数据合理转发问题时,NFV 则解决网元的合理虚拟化,减少空间和能源消耗,相互结合以达到运营商利益的最大化。

### 3.2 SDN/NFV 架构中的 DPI

按照之前的分析,传统 DPI 部署方式是把 DPI 嵌入各种网络设备中,如会话边界控制器(SBC)、流量检测功能(TDF)、网关 GPRS 支持节点(GGSN)等。基于 SDN/NFV 的虚拟化功能,就可以将 DPI 服务从嵌入的网络设备中迁移出来,成为托管标准服务器上的共享功能。这种方式降低了 DPI 所需的总投资,因为这样一来 DPI 只需要在更少的机器上实现(减少固定资产投入),而且减少能源消耗(减少操作成本)。此外,不同功能和 DPI 应用程序之间的互通

不再那么复杂,因为对应用程序 ID 和元数据执行一致的格式,相对而言更容易一些。

有了 SDN/NFV,DPI 可以不只驻留在现有的位置,而是在现有基础上,实现更加复杂的功能<sup>[8]</sup>。例如,实现流量的实时监控、异常流量的智能汇聚、集中处理。还可以使用机器学习等方式对应用层的数据进行分类等深入分析,在满足更高吞吐量需求的同时,获得高准确率<sup>[9]</sup>。

### 3.3 在 SDN/NFV 网络中部署 DPI

SDN/NFV 网络架构包括丰富的层次,DPI 功能可以在几个层次嵌入,如图 6 所示。这些部署方案通过使用提供 DPI 服务的基础设施来避免合并 DPI 设备,从而可以简化 DPI 的管理。下面通过几种情况来说明。

#### 3.3.1 节点层

在网络节点上运行 DPI 软件,相当于将检测点放在了网络最前端,通过其进行信息的收集,并作为网络的第一道屏障。此时,SDN/NFV 就可以作为接受者和决策者,与上层应用进行交互并将得到的策略指示给节点或者直接给节点上的 DPI 软件下达预设的策略。这样的设置,可以将 DPI 软件的等待时间降到最低,成为反应最快速的分析

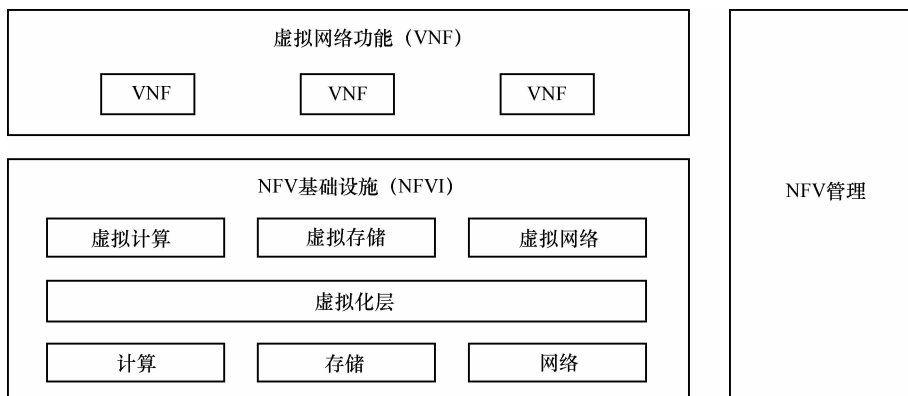


图5 NFV 架构

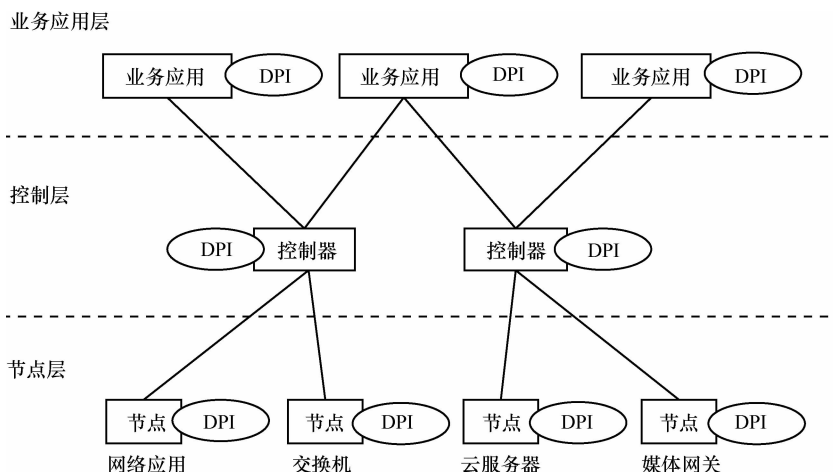


图 6 可嵌入 DPI 的层次

源。但是,这种部署方式也是成本最高的,DPI 软件的实例数目将随着节点数的激增,产生大量的消耗。

### 3.3.2 控制层

将 DPI 软件部署在控制器中可以避免随节点数增加造成的 DPI 实例激增,从而减小开销。同时,这种部署方式能更好地将网络智能应用于控制服务,成为连接应用与节点的桥梁。此时,DPI 的功能将成为控制决策中重要的组成部分,相当于整个 SDN/NFV 智能网络“大脑”的一部分,参与决策的制定,并为上层应用提供数据。当然,这种部署方式也存在相应的问题:其将影响到网络的可扩展性和分析性能。此时将需要更高的分布式控制架构来减少这些问题造成的影响。

### 3.3.3 业务应用层

相对于前两种部署方式,DPI 软件可以轻松地被嵌入业务应用中。此时,DPI 软件成为了大量网络数据涌入的分析主力军。同时数据在到达 DPI 之前可能经历了较长的通信时间,例如一些数据流将通过节点到控制层再到达应用层,使得此时的分析不再是严格实时性的,将产生一定的时延。针对这种情况,可以通过扩展应用程序来充分发挥其分析的效力。比如,针对不同数据源采用更有针对性的分析策略,建立更复杂、更有效的分析模型,挖掘数据中更深层次的信息,从而使其成为网络智能化的信息提供者。

## 4 结束语

本文阐述了现有的传统 DPI 部署方案,描述了传统方案的现状和面临的问题,并描述了在 SDN/NFV 基础上嵌入 DPI 程序构建智能化网络体系的方案。SDN 技术将网络的

控制权与数据的转发进行了分离,并在此基础上通过 NFV 技术将软件和硬件解耦来重新构架网络。通过将这两种技术引入 DPI 部署中,将其虚拟化来实现更低成本、更智能的网络体系。该网络体系能最大限度地实现架构的可扩展性,降低重复性消耗,使其具有更强的向未来网络演进的能力。

同时,运营商基于 SDN/NFV 部署、利用 DPI 实现的智能网络能提供新的服务,并可以更好地管理带宽,同时降低了投资和维护成本。这样一个智能化网络体系将更好地为运营商针对其网络提供更多控制权,使得网络功能运行在一般硬件平台上的复杂性也降低,通过灵活的数据接口为上层应用系统提供更好的数据支撑和管理功能支撑,也为新服务的推出创造了条件。

## 参考文献

- 1 朱永庆. DPI 技术应用场景探讨. 广东通信技术, 2007, 27(7): 27~29  
Zhu Y Q. Discussion on application scenarios of DPI technology. Guangdong Communication Technology, 2007, 27(7): 27~29
- 2 Lu X, Cao W, Huang X, et al. A real implementation of DPI in 3G network. Proceedings of Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA, 2010
- 3 Hata H. A study of requirements for SDN switch platform. Proceedings of 2013 International Symposium on IEEE Intelligent Signal Processing and Communications Systems (ISPACS), Naha-shi, Japan, 2013: 79~84
- 4 薛森, 符刚, 朱斌等. 基于 SDN/NFV 的核心网演进关键技术研究. 邮电设计技术, 2014 (3): 16~22  
Xue M, Fu G, Zhu B, et al. Research on key technologies of core network evolution based on SDN/NFV. Designing Techniques of Posts and Telecommunications, 2014 (3): 16~22

(2015143-6 接排在 2015060-6 后)

- Wu Z H. Cloud Computing Core Technology Dissecting. Beijing: Posts & Telecom Press, 2011
- 8 王庆波, 金津, 何乐等. 虚拟化与云计算. 北京: 电子工业出版社, 2009
- Wang Q B, Jin X, He L, *et al.* Virtualization and Cloud Computing. Beijing: Publishing House of Electronics Industry, 2009
- 9 刘鹏. 云计算. 北京: 电子工业出版社, 2010
- Liu P. Cloud Computing. Beijing: Publishing House of Electronics Industry, 2010
- 10 任永杰, 单海涛. KVM 虚拟化技术实战与原理解析. 北京: 机械工业出版社, 2013
- Ren Y J, Shan H T. KVM Virtualization Technology Practice and Principle Analysis. Beijing: China Machine Press, 2013
- 11 戢友. OpenStack 开源云——云计算、虚拟化、Nova、Swift、Quantum 与 Hadoop. 北京: 清华大学出版社, 2014
- Ji Y. OpenStack Open Source Cloud Computing——Cloud Computing, Virtualization, Nova, Swift, Quantum and Hadoop. Beijing: Tsinghua University Press, 2014
- 12 张子凡. OpenStack 部署实践. 北京: 人民邮电出版社, 2014
- Zhang Z F. OpenStack Deployment Practice. Beijing: Posts & Telecom Press, 2014
- 13 Joysula V, Orr M, Page G. 云计算与数据中心自动化. 张猛译. 北京: 人民邮电出版社, 2012
- Joysula V, Orr M, Page G. Cloud Computing and Data Central Automation. Translated by Zhang M. Beijing: Posts & Telecom Press, 2012
- 14 陈驰, 于晶. 云计算安全体系. 北京: 科学出版社, 2014
- Chen C, Yu J. Security Architecture of Cloud Computing. Beijing: Science Press, 2014
- 15 Krutz R L, Vines R D. 云计算安全指南. 张立强译. 北京: 人民邮电出版社, 2013
- Krutz R L, Vines R D. A Comprehensive Guide to Secure Cloud Computing. Translated by Zhang L Q. Beijing: Posts & Telecom Press, 2013

## [作者简介]



宋阿芳, 女, 中国电信股份有限公司上海研究院高级工程师, 主要从事网络演进及运行维护方面的技术研究工作。

林联, 女, 中国电信股份有限公司上海研究院高级工程师, 主要从事网络演进及运行维护方面的技术研究工作。

王发光, 男, 中国电信股份有限公司上海研究院工程师, 主要从事云计算与数据通信方面的技术研究工作。

2015060-6

(上接 2015143-5)

- 5 Gelberger A, Yemini N, Giladi R. Performance analysis of software-defined networking (SDN). Proceedings of IEEE 21st International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), San Francisco, CA, USA, 2013: 389~393
- 6 Batalle J, Ferrer Riera J, Escalona E, *et al.* On the implementation of NFV over an OpenFlow infrastructure: routing function virtualization. Proceedings of 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 2013: 1~6
- 7 Veitch P, McGrath M J, Bayon V. An instrumentation and analytics framework for optimal and robust NFV deployment. Communications Magazine, 2015, 53(2): 126~133
- 8 Omnes N, Bouillon M, Fromentoux G, *et al.* A programmable and virtualized network & IT infrastructure for the internet of things: how can NFV & SDN help for facing the upcoming challenges. Proceedings of the 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015: 64~69
- 9 Li Y, Li J. MultiClassifier: a combination of DPI and ML for application-layer classification in SDN. Proceedings of the 2nd International Conference on Systems and Informatics (ICSAI), Shanghai, China, 2014: 682~686

## [作者简介]



潘洁, 女, 中国移动通信集团设计院有限公司工程师、项目经理, 主要研究方向为数据网络。

郝卓宁, 男, 中国移动通信集团公司高级工程师、项目经理, 主要研究方向为数据网络。

林鹏, 男, 博士, 中国移动通信集团设计院有限公司高级工程师、项目经理, 主要研究方向为数据网络。

2015143-6