



IP 网络智能感知能力的构建与分析

徐向辉, 张园, 杨锋

(中国电信股份有限公司北京研究院 北京 100035)

摘要: 聚焦在运营商 IP 网络中构建智能感知能力。首先对多层面的 IP 网络感知技术及其现状进行分析, 其次对大规模网络中应用层感知技术的部署进行探讨, 最后对运营商网络中构建完善的智能感知能力的若干关键问题进行剖析, 力求从实践、可操作的视角使读者对感知体系的构建有所启迪。

关键词: 智能感知; DPI 系统; 感知与控制联动; 大数据分析

doi: 10.11959/j.issn.1000-0801.2015264

Construction and Analysis of Intelligent Perceive Ability in IP Network

Xu Xianghui, Zhang Yuan, Yang Feng

(Beijing Research Institute of China Telecom Co., Ltd., Beijing 100035, China)

Abstract: It was focused on the construction of intelligent perception ability in IP network. Firstly, multi-level IP network perception technology and its current situation were analyzed. Secondly, perception technology application of large-scale network were discussed. Finally, some key problems in building perfect perception capabilities of operators' network were analyzed, trying to explain perception system construction to readers from practice and operable perspective.

Key words: intelligent perception, DPI system, linkage of perception and control, big data analysis

1 引言

IP 互联网正处于蓬勃发展的鼎盛时期, 人们习惯于依赖互联网后, 对互联网的期望也不断提升。同时, 云计算、SDN、智能终端等技术的发展, 使得互联网向规模化、产业化、智能化的发展成为必然, 智能性已成为未来网络的一个核心特征。在未来网络的诸多智能能力中, 智能感知能力是实现智能网络的基础。从用户到应用、从终端到网络、从流量到行为, 只有可知才可控。全面感知网络中流量的多维特

征, 一方面是提供智能应用和服务的必要前提, 另一方面也是运营商调整优化网络、增强网络安全性的重要条件。

国内外运营商都十分重视智能感知能力的建设和布局, 以期望在深度感知的基础上实现智能的控制和优化。本文将从感知技术发展和部署现状出发, 对运营商构建感知能力的思路和关键问题进行探讨。

2 多维感知技术

一般来讲, 智能感知技术是指通过自动化手段采集、

收稿日期: 2015-06-02; 修回日期: 2015-10-10

论文引用格式: 徐向辉, 张园, 杨锋. IP 网络智能感知能力的构建与分析. 电信科学, 2015264

Xu X H, Zhang Y, Yang F. Construction and analysis of intelligent perceive ability in IP network. Telecommunications Science, 2015264

分析识别并统计包括用户标识、网络标识、应用特性、用户行为等在内的各类有用信息。

从 OSI 分层的角度,智能感知技术包括对 2~7 层等各层信息的识别,如图 1 所示。例如,对 MAC 地址、IP 五元组等网络层信息的感知,对应用、用户行为等应用层信息的感知和分析。不同层面的信息可能是相关联的,例如,2 层的 MAC 地址、3 层的源 IP 地址、应用层 cookie 中的用户账号、应用层中的终端信息,这些信息会共同指向同一个用户,在后续的分析中,这些信息也可能会组合起来使用。一般的,网络层信息的感知可通过 IP 网络设备的相关检测功能及 DFI 技术实现,应用层信息的感知需要通过 DPI 技术实现。

从检测方式和粒度来看,感知技术通常又可分为 DFI (深度/动态流检测)和 DPI。DFI 是一种基于网络数据流的深度检测技术,针对不同的 flow 进行深度检测,代表技术是 NetFlow,主要通过路由器在到达的数据分组中按照流量采样比采样数据分组中 IP 层和 TCP 层的字段,获得流的信息并分析处理。DFI 一般用于网络实时监测和网络规划等。DPI 是一种基于应用层的流量检测和控制技术,通过读取 IP 分组载荷的内容来对应用层信息进行分析,从而识别到应用协议层面。

近来,随着大数据技术的飞速发展,大数据分析在智能感知领域的作用不断提升。通过一些基础的流量镜像及信息采集,再结合大数据技术针对特定的目的和场景进行筛选、匹配,可以对用户行为进行更深入地分析。不难看出,DFI、DPI 以及大数据等多种技术的结合,是未来网络

智能感知技术发展的必然趋势。

3 IP 网络感知能力部署现状

目前,运营商 IP 网络的智能感知能力部署主要包括以下几个方面:一是网关 BRAS/MSE 及边缘路由器已有的网络层感知能力,主要是对 IP 五元组等信息进行感知;二是 AAA 服务器认证等支撑系统具备的用户感知能力,主要是对宽带账号及 IP 会话的感知;三是在城域网出口/省出口部署的 DPI 系统,主要是对应用协议层面进行感知;四是在 IDC 出口部署的 ISMS(也是一种 DPI 系统),主要负责对互联网访问安全进行感知。

4 应用层感知技术的部署

针对应用层感知,IP 网络中不同层面的检测点提供的感知能力和侧重点不同,如图 2 所示。从底至顶,终端上部署的感知技术主要是通过软件增强区分不同类型的业务流,需要可控终端并具备终端管理系统,如 IMS 硬终端。在家庭网关/企业网关上部署的感知技术主要是通过软件增强,对上行流量完成一些相对简单的识别,如特定目的地址的应用,由于靠近用户侧,根据识别结果对接入网带宽进行控制会变得更加容易。在网关 BRAS/MSE 上的感知技术主要通过内置串接 DPI 板卡方式,基于应用层分析完成特定流的识别及后续控制,如 QoS 控制、流更改等。城域网出口、省出口或 IDC 出口一般会并/串接专门的 DPI 设备对流量进行抽样检测,进行应用协议级的分析统计。一般来讲,检测点越靠近用户侧,感知的粒度越细,信息越全,但

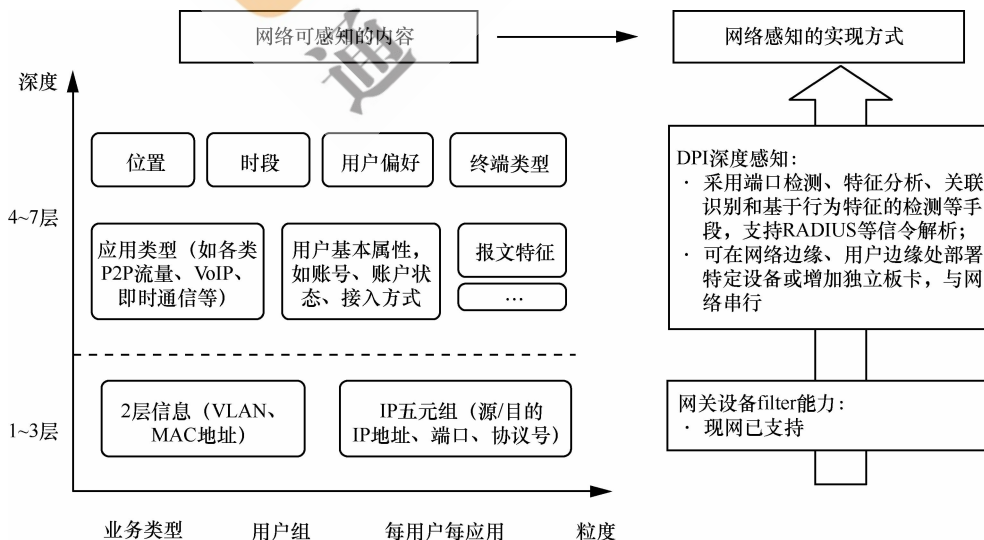


图 1 OSI 多层次感知示意图

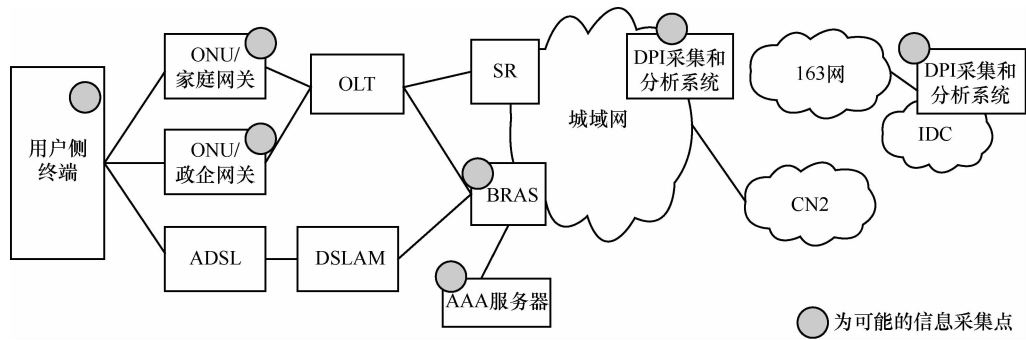


图2 智能感知在网络的布局示意

同时由于检测点越小越分散、数量众多,因此部署的难度也越大,得到细粒度感知效果的代价也越高。

国内运营商一般通过在城域网出口或省出口的部分链路部署 DPI 系统来实现对流量的感知,采用并接轮询监控方式,不影响正常流量传送且降低了部署成本。而很多国外运营商由于网络规模较小,一般通过在 BRAS 上内置 DPI 板卡,采用串行方式对用户流量进行感知,这样可以感知到基于单用户的会话,便于完成细粒度的流量控制。

5 感知能力构建的关键考虑

网络层感知能力一般随 IP 网络设备(如网关、边缘路由器等)按需部署,作为特定功能配置在设备中。这里主要讨论应用层感知能力的部署要素。

应用层感知能力的构建以 DPI 系统的部署为核心。一般来讲,无论是串行部署还是旁路部署,DPI 系统都需要随链路的扩容而扩容,以达到一定的抽样比例,得到理想的感知分析结果。但由于 IP 网络规模增长十分迅速,城域网/省/IDC 出口的链路以 10 Gbit/s 甚至 100 Gbit/s 粒度不断扩张,DPI 系统的同比扩容必然带来成本的大量投入。因此,运营商网络在 DPI 系统构建中需要结合感知需求、感知分析效果、投资成本、后续管理要求等方面,综合考虑 DPI 系统的部署规模、部署位置、部署方式以及与其他系统的联动方案。

首先,在部署规模上,现网试验表明,对于非实时的离线分析,如应用占比分析、用户行为分析等,由于这类分析是一个相对长期的过程,链路覆盖率较低,如 10%~20%,即可达到较准确的分析效果。而对于实时数据输出,要求感知特定条件下用户的即时行为,例如某个用户群组访问某个特定 URL、搜索关键词的动作,这种情况下,较低的覆盖率必然造成较高的漏报率,因此需要较高的链路覆盖率

才能达到预期效果。不同的场景对 DPI 系统的覆盖规模有不同的需求,在实际部署中,可根据主要场景,并结合其他技术手段,力求以较小的覆盖规模达到相似的感知效果。例如,先通过端口镜像或其他粗过滤方式将目标流量筛选出来再送入 DPI 系统进行深度感知。通过 L2TP 隧道方式将目标流量送至集中的 DPI 系统进行处理,这样都有助于降低 DPI 系统的部署规模,从而节约投资。

其次,在部署位置和方式上,以整体分析需求为主的宜将 DPI 系统部署在较高的层面,如城域网出口或省出口,采用旁路方式;以单用户会话级别的精细化分析和控制为主的,宜将 DPI 系统部署在更靠近用户侧的位置,如网关侧,采用串行方式。

再次,智能感知的最终目的是为了感知分析基础上的控制和开放。感知与控制联动必然成为主要的技术趋势,智能感知系统用于感知网络状态及用户行为,其感知分析的结果输入策略控制系统,用于策略控制系统进行全网策略或单用户策略的制定和执行。策略执行的结果也可以再次被感知以作为对执行效果的评估。这样就可以逐步形成闭环的反馈机制和控制机制,形成智能的管理体系。同时,可以将用户、网络层面的感知信息有控制地提供给第三方开发者,与能力开放技术相结合,用于网络能力的开放和新业务创新。

最后,智能感知系统本身也应该在不断发展中走向规范化、标准化。目前现网中部署的 DPI 系统大多由前置的 DPI 设备和后台分析统计平台组成,各厂商架构各异,前后台之间也均为私有接口。从产业链发展的角度,将 DPI 系统架构标准化,制定统一的架构和接口,是促进感知领域良性发展的必要举措。此外,将固定 IP 网络、移动网络、IDC 等各类网络中需要感知信息的需求整合起来,利用统一的 DPI 系统来提供,也是一个最大程度上发挥系统能力的好思路。

6 结束语

智能感知所获取的各类信息是网络规划、网络流量优化、灵活精准的策略控制以及安全性管理的基础,其价值不言而喻。但在这个信息爆炸的互联网大环境中,如何更有效、有针对性地获取有用信息,如何利用大数据分析和挖掘技术、更高效的深度分组检测等技术攫取信息,如何使感知真正成为可动态配置、可集中呈现、可自动联动、可灵活扩展的智能网络的基础能力,这些将随着智能网络的不断发展继续被深入研究。

参考文献

- 1 陈运清,张文强,徐向辉等.面向应用的智能管道关键技术新解.北京:电子工业出版社,2013
Chen Y Q, Zhang W Q, Xu X H, *et al.* New Perspective of Applications-Oriented NICE Technologies. Beijing: Publishing House of Electronics Industry, 2013
- 2 中国通信标准化协会.基于分离架构的深度包检测系统技术要求, 2014
China Communications Standards Association. Deep Packet Inspection System Technical Requirements Based on Separation Architecture, 2014
- 3 锐捷网络. DPI 技术白皮书, 2009

[作者简介]



徐向辉,女,中国电信股份有限公司北京研究院工程师,主要研究方向为智能网络关键技术、IP 宽带网络关键技术等。



张园,女,中国电信股份有限公司北京研究院智能网络产品线总监,主要研究方向为核心网、SDN/NFV、网络智能化等关键技术。



杨锋,男,中国电信股份有限公司北京研究院工程师,主要从事 IP 网络技术和承载方案、智能管道技术、DPI 技术和设备等研究工作。