5G 承载网数据采集和安全管控演进思路

侯慧芳，李雪芳，潘洁，丁志刚
（中国移动通信集团设计院有限公司，北京 100080）

摘　要：运营商通过在各网络节点部署 DPI 设备实现用户数据采集，结合上层安全管控系统，实现运营商级安全运维体系。5G 网络新架构、新技术和新业务满足前所未有的连接场景需求，也带来了新的安全风险。主要探讨了 5G 网络背景下承载网数据采集方案在部署位置和系统架构方面的演进方向以及随之带来的内容安全和网络安全管控系统的革新思路。

关键词：家宽侧 DPI；虚拟化 DPI；5G 内容安全方案；DDoS
中图分类号：TN929.5
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020272

5G carrier network data collection and security management evolution ideas

HOU Huifang, LI Xuefang, PAN Jie, DING Zhigang
China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstract: Operators collect user data by deploying DPI system at some network node, and combining with the security control system to achieve an operator-level security operation and management system. The new architecture, technologies and services of the 5G network meet the unprecedented demands of connection, but also bring new security risks. The evolution of the data collection scheme of the carrier network was mainly discussed under the background of 5G network, as well as the innovative ideas of content security and network security systems that follow.

Key words: DPI on broadband, vDPI, 5G content security solution, DDoS

1　引言

5G 时代是万物互联的时代，5G 网络高速的终端速率、超高的连接密度、丰富的业务类型对用户数据采集提出了新挑战，同时也对数据安全防护提出了更高的要求。目前运营商依托在各个网络采集点部署 DPI（deep packet inspection，深度分组检测）设备，实现业务数据采集和处理，同时也部署了一系列安全管控系统与 DPI 设备对接，构成全方位的安全运维体系，如图 1 所示。

5G 网络新架构以及切片化、服务化的新理念，除了对接入网、核心网的网元和系统产生直接影响，对承载网络的数据采集方案和安全管控系统也带来了新思考。

收稿日期：2020−08−20；修回日期：2020−09−10

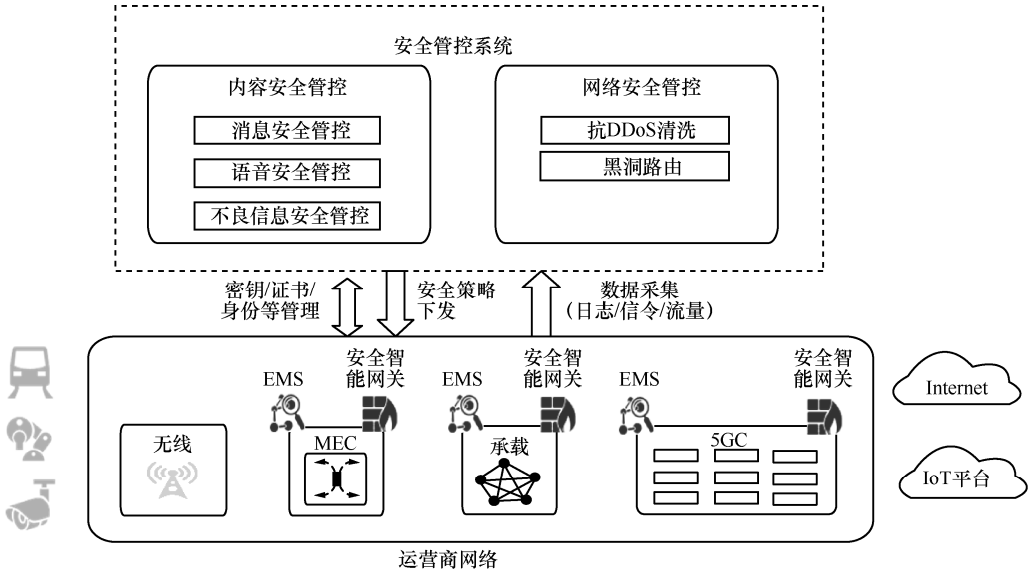

图 1　5G 网络数据采集和安全管控系统架构

2　5G 承载网数据采集方案演进思路

目前业界对 5G 无线侧数据采集方案的讨论较多，无线侧 DPI 设备根据 5G 网络架构和业务场景的变化，其采集位置调整至更靠近园区侧。5G 承载网的网络架构虽然没有实质性调整，但作为业务承载和流量交换网络，5G 对承载网提出了大带宽、低时延和高可靠的更高要求。为满足 5G 网络多业务接入需求和大流量采集场景，承载网流量采集方案也需进一步优化，考虑在承载网络的边缘部署 DPI 设备，在靠近用户侧获取细粒度用户业务数据，并对 DPI 架构提出更多的建设思路，以应对多种部署场景的需求。

2.1　DPI 部署方案

目前运营商承载网 DPI 设备主要部署在骨干网网间、省网出口和 IDC（internet data center）出口，整体部署位置较高，分析维度粒度较粗，无法从单用户维度进行数据分析及控制。可考虑在城域网核心层或城域网接入层部署 DPI 设备，获取更细粒度的用户数据。5G 时代，互联网流量突增、新业务更新加快，互联网电视、4K 高清、智能遥控、教育、智能家居等家庭宽带（以下简称“家宽”）业务种类增长迅速，业务的流量、流向更为复杂。城域网接入层是用户接入互联网的入口，而 BRAS（broadband remote access server，宽带接入服务器）作为承载网络的边缘以及用户接入的网关，也是家庭新业务的入口，考虑在家宽侧部署 DPI 设备，比城域网核心层能获取更细粒度、针对单用户的流量数据，做到精细化业务识别和故障定位。运营商可合理利用单用户单业务流量数据，提高运维效率，提供个性化增值服务。承载网整体 DPI 采集点部署方案如图 2 所示。

目前家宽侧已可通过软硬件探针、RADIUS（remote authentication dial in user service，远程用户拨号认证系统）和网管系统，提供网络环境和用户行为、上网统计数据以及链路告警状态等信息，在 BRAS 侧新增部署 DPI 设备，可协同已有的家宽侧用户数据共同构建覆盖用户整体网络分析的数据库，如图 3 所示。

BRAS 侧 DPI 设备可实现单用户精细化业务识别，并根据业务特征实现业务流分类，运营商可据此提供个性化增值服务。例如智能家居系统

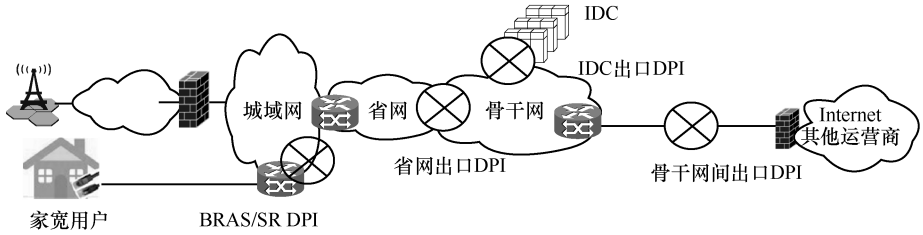

图 2　承载网 DPI 部署位置示意图

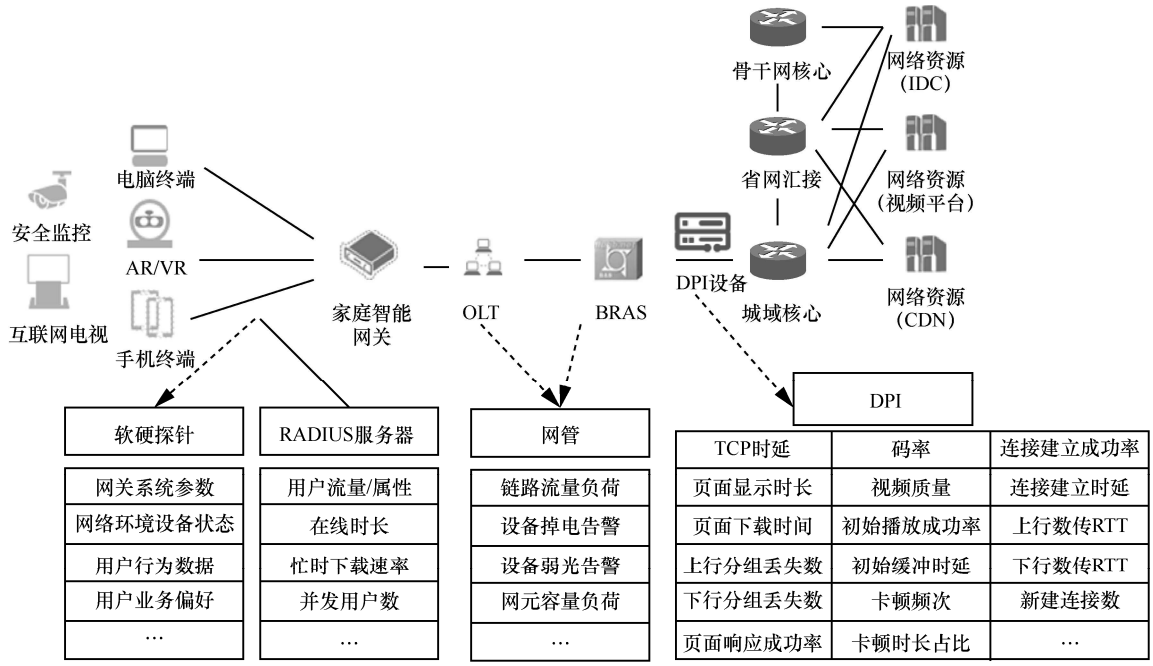

图 3　家宽侧整体网络分析数据库体系

需要传输控制信息和多媒体数据，控制信息数据量小但对实时性和可靠性要求高，高清视频等多媒体信息数量大但对实时性要求不高，DPI 设备对用户流量进行精细化分类后，通过策略与城域网路由器进行联动，提供高优先级或大带宽等网络环境，满足不同业务的个性化传输需求。

2.2　DPI 架构演进

5G 网络背景下，对于 DPI 设备部署位置较高的骨干网间、省网出口、IDC 出口等场景，均为各网络层次出口流量的汇聚节点，流量转发和处理要求高，可延续硬件 DPI 设备架构，但需考虑未来大容量接入端口的影响，做适当的硬件架构调整。对于家宽侧等互联网边缘节点，采集位置分布广泛，部署硬件 DPI 设备运维难度较大、成本较高，可考虑部署虚拟化 DPI 设备。基于以上两类场景考虑的承载网 DPI 架构演进方案如图 4 所示。

（1）硬件 DPI 架构调整

5G 时代，大量云化数据中心规模建设和迅速发展，进一步推动了承载网络技术和架构的演进。在以太网端口方面，100GE 端口开始捉襟见肘，400GE 端口加快测试和商用。DPI 设备以串接/并接方式接入路由器链路中，也需考虑针对 400GE 端口的架构升级。目前运营商互联网 DPI 设备主要采用路由器架构和 ATCA（advanced telecom computing architecture）架构，路由器架构的 DPI 设备因其天然具备良好的高速线速转发能力，可平滑升级。ATCA 架构 DPI 设备受限于 PICMG 3.0

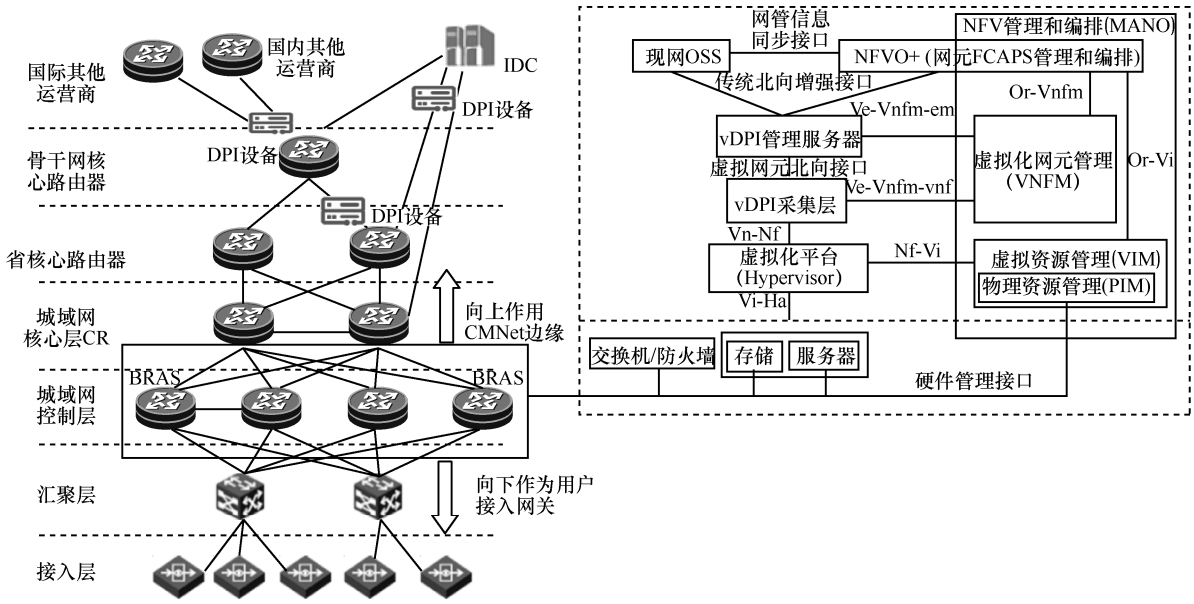

图 4　承载网 DPI 部署架构演进方案

规范定义的机框单板功耗限制，每个槽位散热功耗设计不能超过 200 W。在接入 400GE 端口后，单板处理能力提升导致单板功耗将超过规范限制，难以满足高处理性能板卡的部署需求。对于 400GE 端口接入场景，ATCA 架构的 DPI 设备可考虑向正交架构的能力平台迁移，正交架构至少能实现 1.6 Tbit/s 的背板带宽，且可以根据交换板卡的数量提升背板带宽能力，除此之外，还具备高密度端口能力和优秀散热能力等特点，满足未来 DPI 设备高线速转发、大规模数据处理的能力需求。

（2）虚拟化 DPI 架构

对于家宽侧 DPI 设备，因部署节点分散，设备管理、运维难度大，建设成本高，同时顺应 5G 时代大规模网元云化的趋势，可考虑流量引流，将传统硬件 DPI 云化部署。虚拟化 DPI 管理服务器部署在虚拟化平台上，虚拟化 DPI 设备作为 NFV 架构的虚拟化网元，由虚拟化资源池统一管理。硬件 DPI 设备已成熟商用多年，可实现业务识别、流量过滤、流量控制、日志分析和数据统计等功能，以目前的芯片能力，虚拟化 DPI 设备很难达到线速转发，如在虚拟机上实现所有硬件 DPI 功能（特别是流量控制功能），还需要芯片和硬件技术的大力发展作为支撑。但对于业务流量识别、分析和统计等功能，虚拟化 DPI 设备可实现灵活数据分析和管理[1]。因此，虚拟化 DPI 是未来 DPI 架构的演进趋势，但其商用还需依靠芯片技术的发展，分阶段推进。

3　5G 网络信息安全演进趋势

为积极应对 5G 网络带来的安全风险和挑战，5G 网络信息安全需重点关注内容安全和网络安全管控演进策略。内容安全包括 5G 新消息业务和 5G 数据类业务，网络安全包括 DDoS（distributed denial of service attack，分布式拒绝服务攻击）防护等。通过深入剖析 5G 网络对当前信息安全带来的冲击和影响，研究制定合理的安全管控解决方案，确保实现精准有效的 5G 网络信息安全防控[2]。

3.1　5G 新消息安全管控

目前，运营商针对传统短/彩信、融合消息的安全管控已比较成熟，安全管控技术应用全面，涵盖黑白名单监控、流量监控、行为监控等，并且取得了较为理想的监控效果。随着 5G 时代新消

息业务的大力推广，5G 新消息的安全管控将面临严峻挑战。5G 消息具备自由业务形态的特点，消息群发更快捷，且消息业务类型更多样，使消息的传播能力更强、影响范围更广、社会动员力更大，进一步提高了安全管控难度；且面对 5G 时代复杂多元的富媒体场景，例如方言音视频识别盲区、大视频和大文件识别研判效率低下等问题更加凸显，需切实提升消息安全管控技术手段。

面向 5G 新消息的安全管控，可有效结合人工智能和大数据等新技术手段，基于业务类型（点对点、群聊、MaaP（messaging as a platform）应用等）、消息内容（文本、图片、音频、视频等）、用户行为、用户画像、业务规则、应急管控等方面，对 5G 多媒体消息进行全面监控和识别。5G 新消息的安全管控思路如图 5 所示。

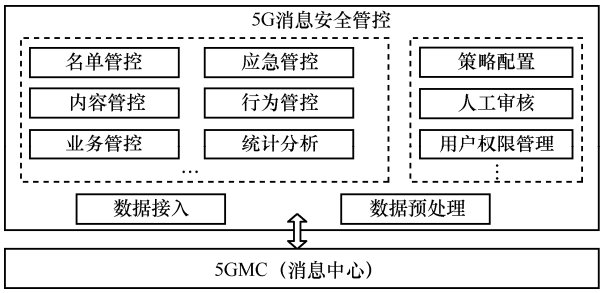

图 5　5G 新消息安全管控方案

初期，5G 新消息的安全策略运营依然沿用“两级共管、集中配置”的整体原则。集中侧制定策略运营工作管理要求，开展策略生成、部署、评估、优化等策略生产流程。端侧加强源头治理，参与样本分析、策略评估优化等工作，提出策略配置建议。

未来，随 5G 新消息业务的快速发展，为进一步积极应对 5G 消息复杂、灵活、变化快等带来的挑战，安全策略运营需逐步从面向 5G 业务的管控转变为面向 5G 消息生态的分级管控，实现精准治理。

3.2　5G 不良信息安全监控演进思路

不良信息监控主要针对网络中的关键节点（国际骨干网出口、自有 CDN（content delivery network）/缓冲业务和 IDC 机房等）的网络流量进行监控，通过流量还原，并结合 AI 和大数据技术，识别和发现恶意软件、恶意链接等不良信息并进行处置。未来随着 5G 新业态的不断涌现，针对 5G 不良信息的监控将面临巨大的挑战。

5G 时代大视频和高清直播等流量占比会持续上升，远远超过现有的文本和视频流量，大规模流量还原消耗的巨大计算能力、流量承载所需的巨大带宽资源都将是急需解决的问题，HTTPS（hyper text transfer protocol over secure socket layer）和私有加密协议的广泛应用，使加密流量的监控识别也面临巨大的技术挑战。

为有效应对 5G 不良信息的安全监控，可以从监控范围、系统架构和系统能力等方面考虑策略演进，具体分析如下。

（1）监控范围方面，针对大型的视频、直播类网站，可以通过管理手段，由这些网站承担内容监控责任，并向相关部门进行报备。针对小型视频直播类网站，数量众多、内容繁杂，可考虑由运营商进行统一监控。

（2）系统架构方面，近期可以考虑采用主动获取和被动还原相结合的方式，集中实现流量还原和监控识别，并具备爬虫能力；远期，在条件允许的情况下，流量还原和识别能力尽可能前置部署，并支持在边缘云上进行自动化部署。

（3）系统能力方面，近期可以采用爬虫方式访问加密网站进行不良信息监控；远期，对于直播类业务，不同的网站使用不同的 App，系统需要具备较强的灵活性，可通过不同网站的 App 对其加密内容进行访问和监控分析。

3.3　5G 抗 DDoS 系统演进思路

5G 网络融入行业应用和数据，海量 MEC（multi-access edge computing，多接入边缘计算）下沉到汇聚机房和园区，数量庞大，DDoS 攻击目标点激增；且 MEC 普遍带宽较小，DDoS 攻击易引发网络瘫痪；MEC 集成第三方应用，业务复杂多样，DDoS 防御难度增加。未来 MEC 有比肩固

网 IDC 的趋势，成为 DDoS 攻击重灾区。5G 时代，应用和带宽的 DDoS 威胁将并存，高效抗 DDoS 成为新挑战[3]。

为应对 5G 时代的 DDoS 攻击挑战，可采用本地 MEC 智能化抗 DDoS 系统协同承载网大区清洗系统组成一体化抗 DDoS 防护方案，整体架构如图 7 所示。MEC 边界部署智能化抗 DDoS 系统，过滤带宽范围内的攻击，保障 MEC 网络基础设施可用性及 App 可用性；当检测到大流量攻击时，智能安全管理系统联动承载网抗 DDoS 系统，将攻击流量引流至承载网大区清洗，大区清洗中心完成过滤后，回注到 MEC 的流量被成功压制到带宽范围内，确保 MEC 链路带宽可用性，由 MEC 抗 DDoS 系统进一步精细化过滤会话层和应用层攻击[4]。

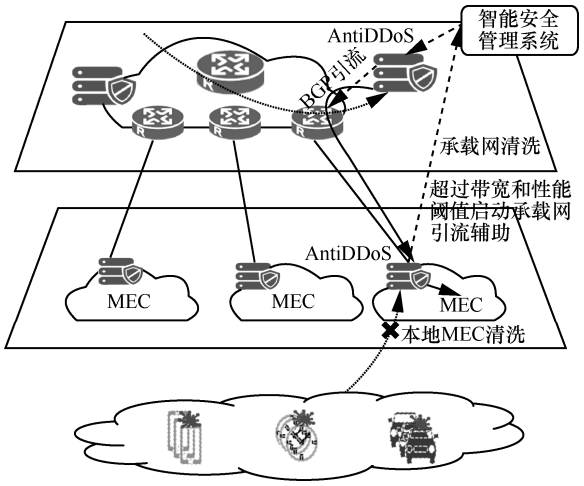

图 7　一体化抗 DDoS 防护方案架构

随着智能化技术的发展，未来一体化抗 DDoS 防护方案还可引入基于机器学习的智能化防御体系，自适应调优防御策略，提升防御精度；远程实现智能化运维，降低运维成本。

4　结束语

本文通过分析 5G 网络背景下数据采集和安全管控系统的演进思路，提出自底层数据采集至上层安全应用完整的方案建议。数据采集方面，根据 5G 时代网络和业务的变化趋势，重点提出承载网 DPI 部署方案和设备架构优化建议；安全应用方面，从内容安全和网络安全两个方面，针对 5G 新消息、不良信息和抗 DDoS 系统的建设思路提出规划建议，以应对 5G 网络带来的安全风险挑战。

参考文献：

[1] 吴迪, 李俊, 韩淑君. NFV 中的 vDPI 功能放置问题研究[J]. 科研信息化技术与应用, 2016, 7(6).
WU D, LI J, HAN S J. A research about placement of vDPI functions in NFV infrastructures[J]. E-science Technology & Application, 2016, 7(6).

[2] 张远晶, 王瑶, 谢君, 等. 5G 网络安全风险研究[J]. 信息通信技术与政策, 2020(4): 4-6.
ZHANG Y J, WANG Y, XIE J, et al. Analysis on security of 5G network and suggestions for security scheme[J]. Information and Communication Technology and Policy, 2020(4): 4-6.

[3] 何明, 沈军, 吴国威, 等. MEC 安全探讨[J]. 移动通信, 2019, 43(10): 18-21.
HE M, SHEN J, WU G W, et al. Discussions on the security of MEC[J]. Mobile Communications, 2019, 43(10): 18-21.

[4] 江伟玉, 刘冰洋, 王闯. 内生安全网络架构[J]. 电信科学, 2019, 35(9): 20-28.
JIANG W Y, LIU B Y, WANG C. Network architecture with intrinsic security [J]. Telecommunications Science, 2019, 35(9): 20-28.

[作者简介]

侯慧芳（1986− ），女，中国移动通信集团设计院有限公司工程师，主要研究方向为数据网络。

李雪芳（1984− ），女，中国移动通信集团设计院有限公司工程师，主要研究方向为通信核心网络和信息安全。

潘洁（1978− ），女，中国移动通信集团设计院有限公司高级工程师，主要研究方向为数据网络。

丁志刚（1983− ），男，中国移动通信集团设计院有限公司工程师，主要研究方向为网络与信息安全。