

嵌入式人工智能技术在IP网络的 创新应用

Innovative Application of Embedded Artificial Intelligence Technology in IP Network


薛强¹, 吴梦², 杨世标¹, 屠礼彪¹, 李伟², 廖江¹ (1. 中国联通广东分公司, 广东广州 510627; 2. 华为技术有限公司, 北京 100094)

Xue Qiang¹, Wu Meng², Yang Shibiao¹, Tu Libiao¹, Li Wei², Liao Jiang¹ (1. China Unicom Guangdong Branch, Guangzhou 510627, China; 2. Huawei Technology Co., Ltd., Beijing 100094, China)

摘要:

通过在路由器内引入全新的知识面,即嵌入式AI软硬件系统,按照既定策略(算法),对指定业务的网络数据进行极速采集、持续训练,结合在线推理及智能决策,实现对新兴及重要业务的实时感知、精准控制及快速响应,大幅提高这类业务的安全性、可靠性及承载质量,从而实现高品质IP网络,并为自动驾驶网络打造坚实的智能底座。

关键词:

嵌入式AI; 持续训练; 在线推理; 智能决策; 高品质
doi:10.12045/j.issn.1007-3043.2024.10.013
文章编号:1007-3043(2024)10-0066-07
中图分类号:TN919
文献标识码:A
开放科学(资源服务)标识码(OSID): 

Abstract:

By introducing brand-new knowledge plane within the router, namely embedded AI software and hardware system, according to the established strategy (algorithm), network data for specified services is rapidly collected and continuously trained. Combined with online reasoning and intelligent decision-making, it realizes the real-time perception, accurate control and rapid response to emerging and important business, which greatly improves the security, reliability and bearing quality of this business, so as to realize high quality IP network and creates a solid intelligent foundation for autonomous driving networks.

Keywords:

Embedded AI; Continuous training; Online reasoning; Intelligent decision-making; High-quality

引用格式:薛强,吴梦,杨世标,等. 嵌入式人工智能技术在IP网络的创新应用[J]. 邮电设计技术, 2024(10):66-72.

1 背景

随着我国“东数西算、东数西存”工程的建设以及全球AI大模型的快速发展,全社会数字化转型迈入算力时代,计算、存储、网络等基础设施的核心组成部分都融入更多的AI元素,全球领先的运营商纷纷加深云网融合,逐步构建算力网络^[1]。IP网络作为算力网络的技术底座,业务场景对它的诉求不仅仅是大带宽、大容量,还需要超高可靠性、高度智能化以及超高安全性等,如何利用AI技术实现对IP网络的升级改造,成为了一个重大的课题。

目前业界的路由器还没有推出内置AI功能,也没有相应的产品、解决方案及应用案例。某省联通组织相关专家成立IP网络智能化小组,并与华为公司联合成立攻关团队,进行软硬件系统的设计、需求研究、方案论证及实现,按计划推出相关功能及解决方案,并在现网进行测试、验证,部分已开始商用。该实践不论在生产中还是学术理论上都具有较大的意义。

2 EAI系统在路由器中的设计与实现

2.1 IP协议遇到的问题

在数字经济及新型信息基础设施高速发展的今天,IP网络是最重要的基础设施之一。以“开放与互联”为最初设计目标的IP网络,获得了巨大的成功,很

收稿日期:2024-08-02

好地满足了各类业务的发展需求。互联网经济的发展方兴未艾,新兴业务,无论是互联网短视频、直播,还是5G承载、算力互联,对IP网络的质量与性能的要求都越来越高,IP网络承载这些新兴业务仍然存在一些急需解决的问题。

一是IP网络对网络状态的感知与快速响应问题。基于xFlow等流检测技术,可以实现网络数据流量的采样和推送,但考虑到对设备性能的影响,采集比一般不超过1 000:1,不能精准反映流量状态,且推送的是原始数据,需要进行二次数据加工分析,对网络状态的感知精度较低、速度较慢。另一方面,SDN控制器的引入为IP网络带来了全局视角。控制器依据网络设备采集的流量统计、链路状态变化和异常报告等信息进行网络监控和管理,同时根据业务需求更新和调整网络策略。SDN对网络的感知,如速度最快的telemetry,采集的最高精度可达亚秒级,但要维持高精度的数据展示就需要大量的数据上报,占用网络的出口带宽,且采样周期对CPU影响较大。一个完整闭环控制耗时至少也是分钟级别的,无法做到及时响应。

二是IP网络质量的精细化要求。路由协议快速收敛,在BFD的加持下,收敛速度能达到100 ms以内,但对于数以T计的IP骨干网链路而言,出现故障时丢包数会达到几百万个,从而降低了网络质量。此外,有些业务(如算力)对网络的时延要求非常高,如算力集群的广域低时延互联,若利用现有网络协议进行部署,要使用BGP-LS采集全网拓扑,TWAMP测量时延,SDN控制器计算低时延路径,并通过NETCONF下发配置,为算力集群提供低时延的连接,但以上配置非常复杂,且动态调整较慢。

三是IP网络的业务感知问题。IP已经成为各类业务的通用承载技术,但传统的路由器是无法感知业务的,出现异常或故障时排障定位跨专业层次多,非常复杂,耗时低效。DPI可以做到局部的业务感知,但造价较高,全网部署困难。因此,网络能够便捷、经济地感知业务,对业务的正常运行提供快速及时的支持,成为了一个重要的课题。

2.2 为什么在路由器中引入EAI

传统的IP网络对业务只能提供尽力而为的服务,通过后续架构与协议的补充改善,可以对业务提供一定水平的感知与保障,但对于新兴业务的高品质要求的保障明显不足,遇到异常情况往往以牺牲质量的方式保证业务的连续性。

随着硬件芯片及AI技术的大力发展,能否在传统的IP网络设备中嵌入AI系统,引入网元级的AI计算能力?

首先,从硬件角度,随着CPU和NP芯片技术的发展,路由器的板卡上一般可以采用16核以上的多核CPU,可以借用一些CPU核的算力进行轻量化的AI建模、训练和推理。同时,路由器都是采用灵活编程的NP芯片,NP芯片本身可以进行特定行为的流识别和挖掘,因此多核CPU+可编程NP芯片的硬件能力可以实现轻量化的嵌入式AI。本方案采用某厂家的通用路由器NE5000E-20,硬件要求CPU核数量不低于16核、主频不低于2 GHz,转发芯片(NP芯片)必须支持灵活可编程能力和挖掘能力,且报文缓存能力强(缓存带宽不收敛、缓存时间不小于30 ms),单板内存不小于16 GB。未来,路由器的板卡上可以植入专用的轻量化AI芯片,既不会使路由器的功耗和成本增长太多,又可以实现更完善的AI能力。

其次,从软件角度,AI算法领域除了向超大规模方向发展提升模型的准确性与泛化能力外,模型体量的增长对算力的高要求也带来了新的技术趋势:AI模型的轻量化。随着模型蒸馏、教师-学生网络学习、强化学习等技术在模型轻量化领域的应用与发展,算法的效率得以提高,能够在设备端侧以更加灵活的方式提供低功耗的AI算法应用部署能力。

可见,内置在网络设备中的AI通用框架系统成为可能。该系统基于AI算法提供模型管理、数据获取和计算功能,将推理结果发送到网络的转发面及控制面(本机或SDN控制器),实现IP包的智能控制与快速转发,不仅能够充分利用设备的样本数据和计算能力,而且具有数据传送成本低、数据安全性高以及推理决策实时性强等优点。

2.3 主要设计思路及工作原理

基于主控、转发平面和从核CPU&AI芯片构建EAI组件系统,该系统进行流模型AI建模,系统架构及主要工作流程如图1所示。

a) 主控板。控制器全局EAI能力的使能和去使能。

b) 线卡CPU从核。它是EAI的主要部件,基于EAI算法对流进行识别、分类和排序等,与线卡NP对接,收集流数据、输出流特征信息到网管或第三方平台/软件^[2]。

c) 线卡NP。负责转发面的流特征统计和上送。

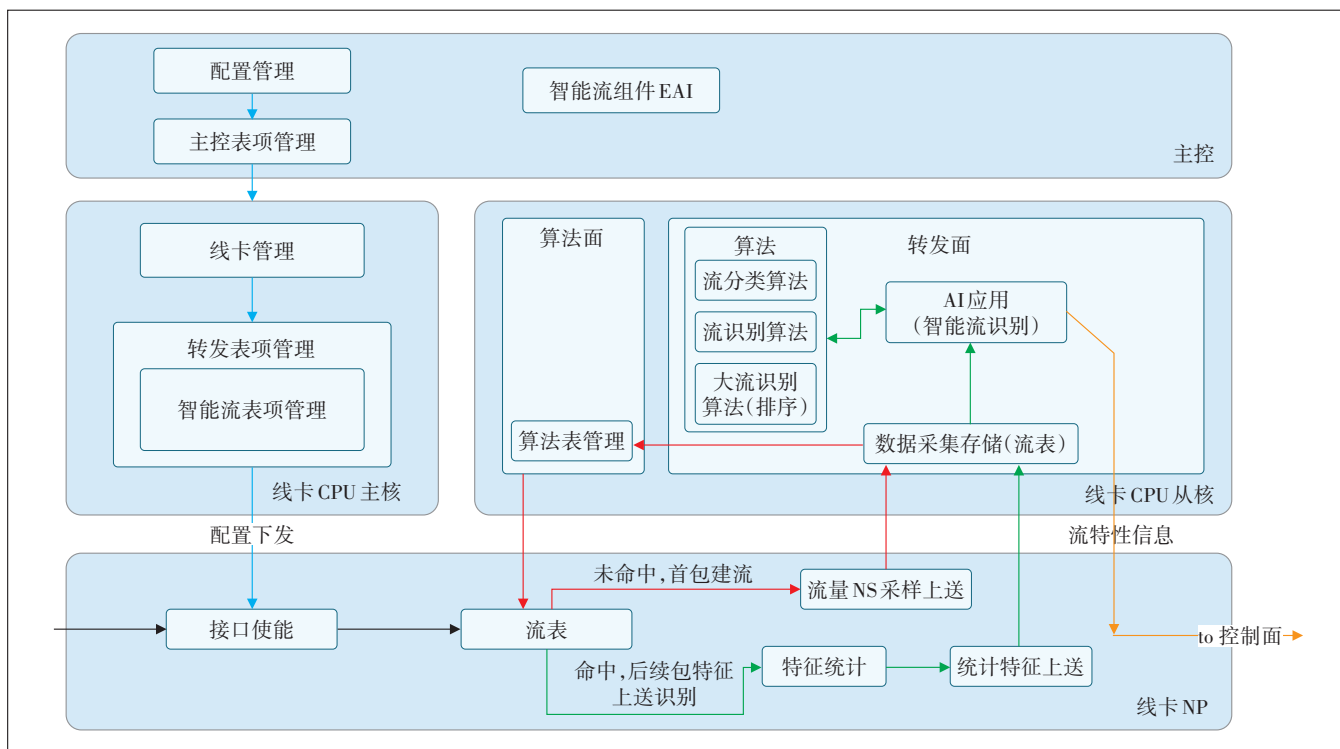


图1 EAI系统架构

系统的主要工作流程如下。

a) 全局控制EAI能力,提供人机或机机界面,通过人工或网管配置使能/去使能EAI能力,并通知到转发面CPU,转发面CPU通知转发面NP启动EAI功能。

b) 转发面启动EAI功能后实时进行流特性统计和上送。

c) 转发面未命中流表时,系统会进行首包上送并建流,建流成功后对流全量进行特征统计并上送到线卡CPU从核,转发芯片基于全流实时进行流量排序,识别TOPn流量;转发芯片基于TOPn流量实时采集上送到CPU从核或AI芯片;CPU从核或AI芯片的EAI组件通过IFC智能流识别算法,进行流量学习和建模,建立流量模型库^[3]。

d) 部署经过轻量化处理后的AI模型,可针对转发面采集的流级别微观特征进行准实时的推理。根据不同的应用场景,可以选择有监督的分类/回归或无监督的聚类模型等,并根据任务的需要融合各领域的专家知识,提升模型的识别效果。其中,对于数据相对稳定、标签难获取的场景,可使用离线训练方式;对于可自监督或由其他方式获取标注数据的场景,则可按需对模型进行增量更新或在线训练,减少概念漂移带来的精度损失。通过AI推理,新建或更新维护流量

的画像,能够由数据驱动从海量流量中自动抽取关键信息^[4-6],将识别出的符合既定策略或特征的关键信息输出到控制面,输出的控制面可以是本机的控制面或外部第三方的控制系统。

嵌入式AI系统,通过软、硬一体化设计,对指定链路或者流(五元组或其他策略)进行逐包检测,达到ms甚至 μ s级的监测能力。通过机器学习建立正常业务模型,在遇到故障或异常情况时,EAI作为转发面与控制面的桥梁,可以快速告警,当达到触发(策略)条件时,EAI可与控制面联动,实现对业务流的快速响应;或者通知到设备的转发面,实现包的备份路由转发,减少丢包;或者通知到设备控制面,实现路由的快速收敛;或者通知到集中控制面,实现基于全网的特定流量策略控制。

当然,由于从核CPU算力有限,还不能做到全业务流的监测,但利用有限的算力,可以解决有限的、紧迫的在网计算的需求,尤其在保障重要业务的安全能力方面,可大幅提升IP网络的安全性、可靠性,从而提升IP网络对业务的感知及保障能力。

2.4 特点与优势

相对传统flow的采样分析,EAI系统采用了逐包检测与分析的方式,建模准确,可实时分析与推理,智

能决策。因此,EAI系统可快速、准确地检测故障或异常,并能快速反馈至控制层,从而在局部或全局层面优化IP网的性能。

基于EAI框架,开发相应的AI网络模型及应用模块,实现局部节点的快速策略响应和网元级智能。下面将详细阐述EAI系统对IP网络的优化思路及实践。

3 EAI系统在IP网络的应用思路及实践

3.1 增强IP网络的安全性

传统DDoS攻击检测采用抽样检测的方式,耗时一般在分钟级,无法及时检测出越来越流行的“短平快”攻击(攻击流量往往在10 s内达到峰值)。通过开发的IFC智能流识别算法,进行DDoS攻击流量学习和建模,建立DDoS攻击模型库,并将识别出来的攻击关键信息输出到安全网管系统,该方法的识别时间从分钟级缩短到秒级,可有效防御传统方案无法解决的“短平快”攻击。

根据近2年中国联通云盾DDoS攻击监测平台的数据,DDoS攻击态势显示出了一些新的变化特征。一是攻击速度加快,大流量的攻击持续呈秒级加速态势,攻击峰值流量爬升至800 Gbit/s~1 Tbit/s,所需时间从2018年的50 s缩短到2022年的10 s^[7-9]。二是攻击持续时间越来越短,2022年57%的攻击持续时间小于5 min,进一步挑战防御系统的响应速度。因此,分钟级的攻击检测与攻击缓解难以满足防护需求,当前基于流的分析检测及引流清洗方案已成为防御响应的时间瓶颈。

智能流检测方案具体如下。

a) 在设备的数据面实现流级别的百毫秒时间精度1:1的统计数据采集,包括流的速率、报文长度、包含特定类型报文的速率等多种流微观特征。这些高频采集的流微观特征是支撑大规模秒级流状态监控与感知的基础(每单板可支持32K~64K IPv4 + 16K~32K IPv6地址高速监控)。报文采用的方案对比如图2所示。

b) 在设备的控制面充分利用EAI的算力,调用算法实时分析百毫秒时间精度的流微观特征。为适应不同类型目的地址的差异化流量模型,流式地学习并维护每IP粒度的正常业务流量模型参数。利用多维度特征,协同检测流速突升与报文成分、报文长度聚集突变等异常变化,滤除正常的流量偶然微突发干扰,引入时间遗忘机制应对业务流量的基线漂移现象^[10]。异常识别准确率高于95%,并能够对分片报文、TCP SYN报文突增等典型DDoS攻击现象加以提示。攻击判定门限的对比如图3所示。

c) 与现有抗DDoS清洗系统完美兼容。以Netstream V9通用模板的形式向网内指定设备进行流级别的DDoS攻击告警实时上报,容易与现有网流分析设备与清洗资源进行适配。上报内容包含流速率及其他统计增强信息,以便下游设备快速获取流信息,端到端秒级处置闭环,达到近似实时清洗的反馈闭环速度。

d) 某省联通已验证了智能DDoS秒级防御技术(“闪防”)的可行性,与传统的DDoS攻击检测对比,

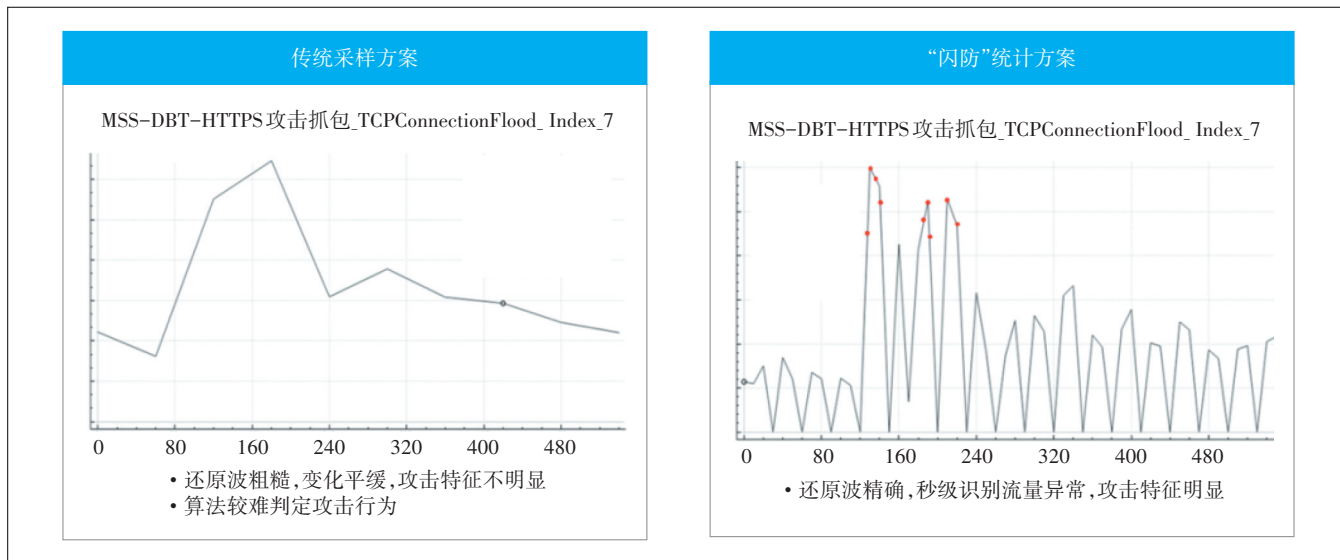


图2 报文采用的方案对比

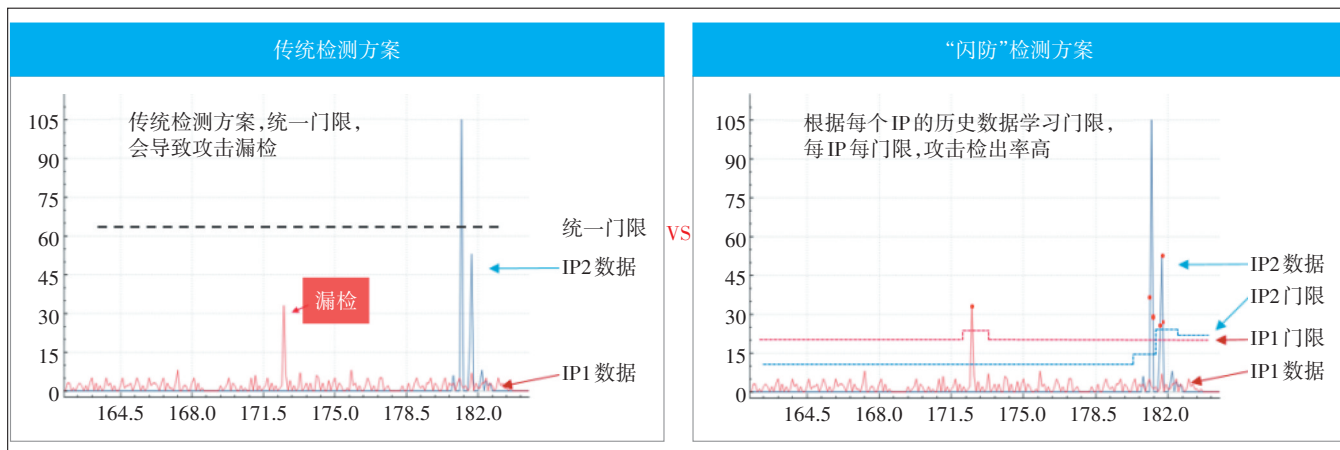


图3 攻击判定门限的对比

“闪防”具有更快更准的DDoS防御能力。传统的检测技术灵敏度较低,在遭受攻击61 s后才实现防御,业务受损时间长;而“闪防”技术实现了2 s发现攻击、5 s完成流量清洗,保障了业务的稳定运行。

3.2 增强IP网络的可靠性

光纤故障易引发网络事故和投诉,2021年某运营商的网络事故投诉中,光纤闪断问题占61.5%。光纤中断时,传统的路由协议收敛时间在分钟级,在BFD的加持下其收敛时间也需要100 ms,高速链路在这期间会丢失大量的数据包,影响业务感知。

EAI系统通过独创的带宽池化算法,从网络、网元和链路3个维度对数据流进行自检测、自感知和自调整。通过开发ARK机制(实时感知-模块隔离-自动恢复),实时检测系统各个模块对CPU、内存等系统资源的消耗,实时感知异常协议处理模块,第一时间将该模块进行资源隔离,以确保其他模块及下游设备的业

务不受影响。被隔离模块的CPU/内存资源恢复正常后,系统自动解除模块隔离状态,业务数据“0”丢失。

当出现光纤故障时,系统能自动感知光纤链路故障,自动负载分担重优化,实现拥塞毫秒级解除,使网络能够抵抗10倍BGP资源过载,预计由光纤故障引发的网络事故和投诉将减少80%以上,实现任意链路故障时业务永在线。2022年,海外运营商因BGP协议产生了重大网络事故,若采用EAI+ARK机制,则极大程度上可以避免类似事故的发生,具体方案如图4所示。

流量微秒级自动倒换基于EAI技术能力,通过快速故障感知、快速恢复和设备内快速通告等技术,实现了故障收敛由100 ms以上降低到百微秒以内,大幅减少了丢包。流量微秒级自动倒换技术只感知IP网络设备的流量变化,不需感知光纤链路物理状态变化,只切换业务流量,不对控制面产生影响,因此在切换时控制面不会跟随切换。同时,此技术支持惩罚机

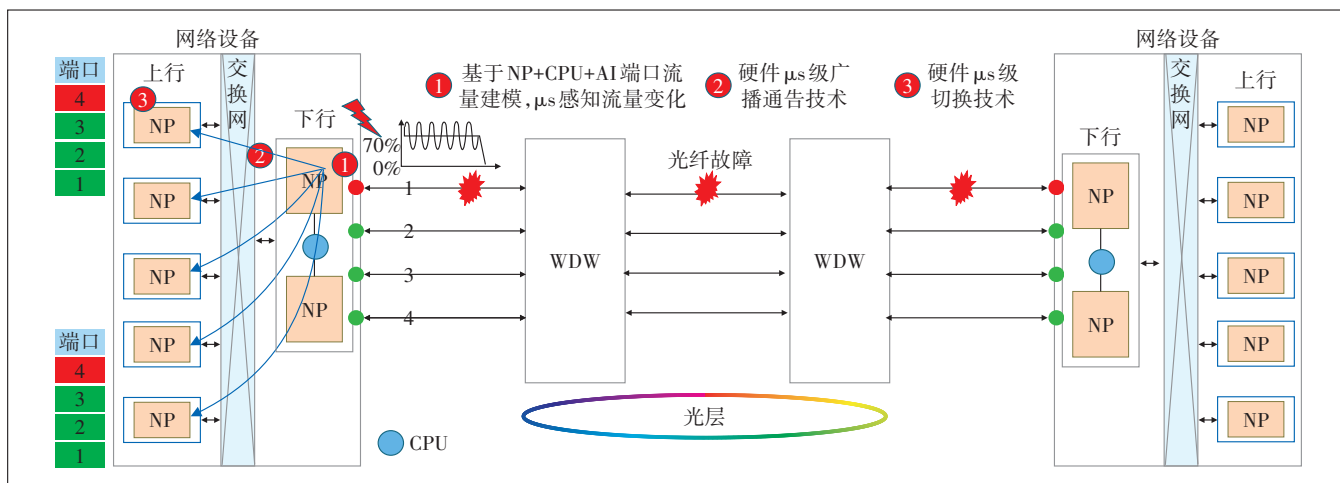


图4 模拟现网负荷分担场景下EAI的快速发现与保护

制,当一段时间内频繁发生倒换和切换时,会启动惩罚机制,在一段时间内不进行快速切换,防止业务频繁切换。

使用路由器、OTN传输设备及测试仪表在实验室搭建了测试环境。

在网络设备不使能EAI的情况下模拟OTN设备之间的光纤故障,丢包时间最大为18 634.11 μs。这个耗时是CPU感知到端口down后将中断信息上送到控制面,控制面再通知转发面切换而引起的。

在网络设备使能EAI的情况下模拟OTN设备之间的光纤故障,丢包时间最大为76.4 μs。这个耗时是转发面把流量切到正常链路的耗时,所以非常短,而正常情况下,控制面依赖端口上报中断后再进行收敛,所以耗时较长。

通过以上测试,EAI使光纤故障的切换时间从18 ms降低到了1 ms级内,大幅减少了丢包。

网络的时延、丢包、抖动是最重要的3个参数,运营商骨干IP网络的比拼目前集中在时延上。因为网络层不感知丢包,也无应对措施,所以主要靠传输层或应用层对丢包进行控制,丢包后重传是最主要的策略,重传期间用户的感知一定会下降^[11-13]。该方案的意义在于,骨干网络部署该方案后可以大大降低网络隐性(网络协议容错内)丢包的概率,大幅提升用户的应用感知,尤其是丢包敏感业务,这对于做到真正的精品IP网络具有重要意义。

3.3 增强IP对承载业务的智能感知及故障定位能力

传统的IP网络无法感知承载的业务,缺乏对关键业务流的可视化及故障定位能力。4G/5G移动业务是IP承载网最重要的业务,当业务层面出现问题时,承载网是无能为力的。对于手机客户来说,端到端的服务涉及了无线、传输、IP承载、核心网、互联网、云池,任何一个环节出现问题都有可能引起客户业务的质量下降或中断,但是因为涉及的技术环节过多且复杂,移动业务的排障是非常复杂且低效的。以往的移动业务大面积故障证明了以上结论,而如何快速发现及定位故障成为了一个重大课题。

移动业务的承载网一般采用L3 VPN over SR/SRv6来承载,在移动核心网上的P节点部署EAI系统,对5GC信令面进行AI自动感知与识别,从而实现辅助快速定位定界(见图5)。

方案的主要工作流程如下。

a) 5GC信令流识别。分析5GC信令面的重要协

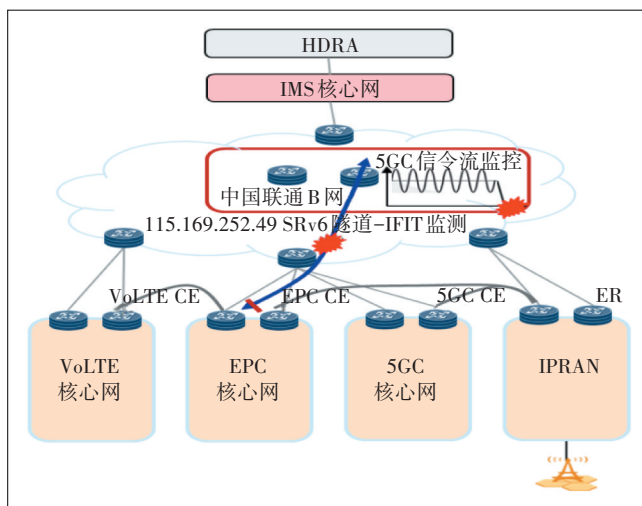


图5 EAI在移动承载网的辅助定位定界

议,如diameter、SS7、SOAP、Restfull、Nx信令等,并基于协议号/端口号对承载网内信令VPN内的流量进行识别、检测。

b) 历史基线学习。针对重要信令流,进行历史基线学习,历史流量建模,建立流量异常门限,对通信矩阵行为进行分析等操作。可以基于源+目的IP建流,最终上报信息携带协议号/端口号,同时包含源+目的IP,信息源:入(区域PE)+宿:出口(区域PE)^[14]。

c) 信令面异常告警。在历史基线学习的基础上,感知每协议每IP流量的正常潮汐变化规律,迅速感知异常的流量变化,针对1个或多个信令IP流异常进行告警,实现网络故障的感知和定界能力,比如多IP流量异常突升突降、IP通信矩阵突变等。IP通信矩阵的变化可以监控流的群体性通断状态,识别网元级的异常。

d) 快速定位定界。当有异常情况时,将告警上报SDN控制器,SDN控制器针对异常IP下发IFIT并进行telemetry上报,确定异常点,辅助快速定位。目前5GC的承载分为2段,即骨干网及本地网,基于设备能力,本方案拟部署在骨干网的P节点上,对L3 VPN/L3 EVPN承载的5GC信令流量进行监控,能定位到骨干网PE[地(市)]。由于骨干网与本地网VPN以OptionA的方式互联,P上的EAI流检测无法定位城域网的设备,但可以由城域内的控制器结合手机IP地址及SMF的地址分配信息,对基站上联承载网的第一跳进行定位,然后由控制器下发IFIT(随流检测)及telemetry上报,对该条链路进行详细的故障定位(见图6)。如果信令全程使用SRv6承载,那么故障定位将更加简化。

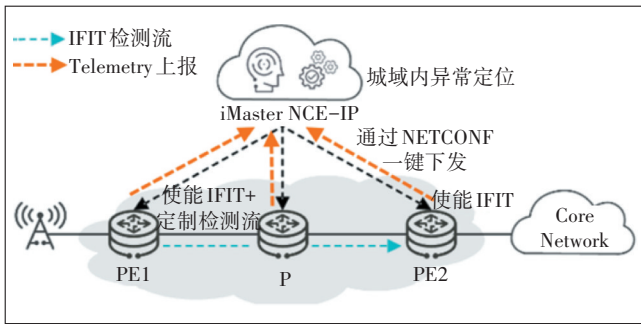


图6 城域网内的异常定位

综上,承载网通过EAI系统,开发出移动业务的画像模块,通过识别5G信令流,对移动业务进行画像,通过AI学习业务模型,在异常/故障时将故障上报SDN控制器,并能够在相关协议的配合下,迅速判断出故障来自哪个链路/网元,为移动业务的稳定可靠运行提供了重要的保障手段,具有极大的现实意义。

3.4 总结

通过EAI系统的在网计算功能,在不增加网络成本及复杂性的前提下,IP网络变得更加智慧,可及时发现承载的业务的变化及异常,为业务线及运维提供更好的服务,也为今后的大客户专线、算力专线、视频业务提供了重要的监控与服务手段,使网络的安全性、可靠性及品质得到大幅提升,给客户与业务带来了更好的体验。

4 EAI系统在IP网络中的应用展望

基于EAI系统可以开发的应用不止本文中的内容。EAI系统使得线卡天然具备了一定算力及无穷的网络数据,根据网络运维、管控、客户网络定制等需求开发相应的(算法)模块,使传统的IP网络长了智慧的翅膀。此外,EAI系统对路由器的体系架构演进、IP控制面的完备都具有重大的启发意义及探索作用。

今后还需进行深入研究,逐步引入AI专用芯片,增强算力,在架构方面,升级集中管控平台,以SDN+AI实现在全网范围内对IP网络及业务的快速、精准控制,从而实现网络级AI,为最终实现IP网的自动驾驶奠定坚实的智能底座。

参考文献:

[1] 中国联通研究院. 算力网络架构与技术体系白皮书[R/OL]. [2024-01-19]. https://www.xdyanbao.com/doc/g7mp429dj0?bd_vid=7409875353243932297.
[2] BAI W, CHEN L, CHEN K, et al. Information-agnostic flow schedul-

ing for commodity data centers[C]//Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2015:455-468.

[3] YE F, BORS A G. Lifelong teacher-student network learning[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44(10):6280-6296.
[4] HINTON G, VINYALS O, DEAN J. Distilling the knowledge in a neural network[EB/OL]. [2024-01-19]. <https://arxiv.org/abs/1503.02531>.
[5] PASSALIS N, TEFAS A. Learning deep representations with probabilistic knowledge transfer[C]//Computer Vision - ECCV 2018. Cham: Springer, 2018:283-299.
[6] HAUSKNECHT M, STONE P. Deep recurrent Q-learning for partially observable MDPs[C]//AAAI 2015 Fall Symposium. Arlington: AAAI, 2015:29-37.
[7] OSANAIYE O, CHOO K K R, DLODLO M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework[J]. Journal of Network and Computer Applications, 2016(67):147-165.
[8] VITALI D, VILLANI A, SPOGNARDI A, et al. DDoS detection with information theory metrics and netflows: a real case[EB/OL]. [2024-01-19]. https://www.researchgate.net/publication/266031486_secure_realdos.
[9] 华为, 电信安全, 联通数科, 等. 2022年全球DDoS攻击现状与趋势分析报告[EB/OL]. [2024-01-19]. <https://anquan.baidu.com/article/1790>.
[10] AL-SAAD M, KHAN A, KELEFOURAS V, et al. Unsupervised machine learning-based elephant and mice flow identification[C]//Intelligent Computing. Cham: Springer, 2021:357-370.
[11] 张彤, 冯佳琦, 马延滢, 等. 时间敏感网络流量调度综述[J]. 计算机研究与发展, 2022, 59(4):747-764.
[12] 李文信, 齐恒, 徐仁海, 等. 数据中心网络流量调度的研究进展与趋势[J]. 计算机学报, 2020, 43(4):600-617.
[13] Application-aware routing[EB/OL]. [2024-01-19]. <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/application-aware-routing.pdf>.
[14] AURELI D, CIANFRANI A, DIAMANTI A, et al. Going beyond Diff-Serv in IP traffic classification[C]//NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE, 2020:1-6.

作者简介:

薛强,毕业于中山大学,高级工程师,博士,主要从事承载网、云池等的规划、建设工作;吴梦,毕业于北京大学,工程师,博士,主要从事网络业务流量的实时状态分析及异常检测相关研发工作;杨世标,网络设计师,主要从事IP网络的维护与网络安全工作;屠礼彪,毕业于北京邮电大学,学士,主要从事IP城域网、智能城域网的规划及建设工作;李伟,毕业于武汉理工大学,工程师,学士,主要从事骨干网解决方案规划和设计工作;廖江,高级工程师,主要从事某省联通网络BG的总体工作。