专栏

基于SRv6+ARN的算力网络安全编排调度技术研究

郗卓宁[1]，侯慧芳[2]，潘洁[2]，赵占军[2]，卜忠贵[2]，叶兰[1]，陈曦[2]，薛嬰[2]
（1. 中国移动通信集团有限公司，北京 100032；
2. 中国移动通信集团设计院有限公司，北京 100080）

摘　要：针对当前算力网络安全服务发展中存在的资源池编排调度效率低下、云网安技术融合不足等关键问题，以运营商在安全服务市场面临的云网安协同创新与运营压力为研究背景，提出基于IPv6转发平面的段路由（segment routing over IPv6，SRv6）+应用响应网络（application responsive network，ARN）的算力网络安全排调度技术策略。该策略通过深度融合SRv6协议实现网络与业务端到端贯通，运用ARN提升数据面标识的简洁性和动态调度能力，构建具备高效编排调度能力的网络数据平面，支持安全业务的灵活组合和快速部署。研究成果主要包含SRv6+ARN编排调度技术架构、关键技术和可靠性保障，为运营商构建云网安协同的算力网络安全资源池提供技术支撑。

关键词：安全编排调度；SRv6；ARN；算力网络；安全资源池
中图分类号：TP393.08
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025170

Research on the security orchestration and scheduling technology of the computing power network based on SRv6 + ARN

XI Zhuoning[1], HOU Huifang[2], PAN Jie[2], ZHAO Zhanjun[2],
BU Zhonggui[2], YE Lan[1], CHEN Xi[2], XUE Zhao[2]
1. China Mobile Communications Group Co., Ltd., Beijing 100032, China
2. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstract: Addressing key issues such as low efficiency of resource pool orchestration and scheduling, insufficient integration of cloud-network-security technologies in the current development of computing network security services, against the research background of the cloud-network-security collaborative innovation and operation pressure faced by operators in the security service market, a computing network security resource pool orchestration and scheduling technology system based on segment routing over IPv6 (SRv6)+ application responsive network (ARN）was proposed. Through in-depth integration of the SRv6 protocol, the research realizes end-to-end connectivity between the network and the service, and through ARN, it improved the simplicity of data plane identification and dynamic scheduling capabilities, constructing a network data plane with intelligent orchestration and scheduling capabilities to support the flexible combination and rapid deployment of security services. The research results mainly include the

收稿日期：2025−03−26；修回日期：2025−07−14

SRv6+ARN orchestration and scheduling technology architecture, key technologies, and reliability guarantees, providing technical support for operators to build a cloud-network-security collaborative computing network security resource pool.

Key words: security orchestration and scheduling, SRv6, ARN, computing power network, security resource pool

0 引言

目前，全球范围内安全访问服务边缘（secure access service edge，SASE）市场趋势迅猛，SASE专注于提供高效敏捷的安全服务，整合了安全Web网关、零信任网络访问、防火墙即服务等能力。国际数据公司（International Data Corporation，IDC）2024年9月发布的*Revelations in the Global DataSphere, 2024: Key Trends and Takeaways*（Doc# US52269924）估计，中国SASE市场规模2024年上半年达4.1亿元（约5 700万美元），全年预计突破10亿元。IDC预测2024—2029年中国SASE市场的复合增长率将达到28.6%，市场处于蓬勃发展阶段。在中国，大型企业和政府客户网络安全等级保护需求旺盛，但多数政企客户安全预算有限、安全能力储备不足，面对不断增加的新型安全攻击，部署单一安全产品难以有效应对复杂的网络安全形势，而采购整套安全解决方案的需求很旺盛。

电信服务运营商基于自身算力网络调度的技术优势、网络覆盖优势和辐射全国省市县的庞大营销团队，积极抢占企业安全服务市场，提升政企客户安全服务能力和开拓相关产品。通过整合全集团云网、安全、运营等优势资源和能力建设算力网络安全资源池，拓展多项安全服务能力，覆盖地市区（县）下沉市场，向党政军客户、小微企业等提供差异化、弹性扩缩容、高可靠的一站式软件即服务（software as a service，SaaS）化安全云防服务，在提升算力网络安全可信服务效能、推动业务转型增值创收的同时，进一步彰显运营商社会责任，为各行各业网络安全赋能。

算力网络安全资源池根据客户订购信息进行安全能力业务链编排，并将客户流量调度到安全资源池进行安全服务。传统的编排调度技术存在业务链编排复杂、虚拟局域网（virtual local area network，VLAN）占用多、流量来回绕行等问题[1]，路径调整和扩展需要逐节点配置，业务灵活性较差；基于IP地址的用户标识方式使服务范围限制在专线用户，难以拓展市场空间。运营商需要将云设施、网络技术、安全能力深度融合[2]，通过差异化服务、优质的技术支持和灵活的商业模式来提升市场竞争力[3]。基于IPv6转发平面的段路由（segment routing over IPv6，SRv6）+应用响应网络（application responsive network，ARN）编排调度技术的算力网络安全资源池，以SRv6协议打通网络、业务互联通道，结合ARN提升数据面标识的简洁度和灵活性[4]，可为客户提供自定义安全服务组合，一站式满足客户安全需求。与此同时，针对不同客户、业务、应用，其可以提供差异化的服务水平协议（service level agreement，SLA）质量保障，全面推动运营商在安全服务市场的快速开拓。

本文旨在解决算力网络安全资源池编排调度效率低、云网安融合不充分等影响算力网络安全服务发展的问题，研究基于SRv6+ARN的算力网络安全编排调度技术，为云网安深度融合的算力网络安全资源池建设部署提供技术架构参考。

1 传统安全编排调度技术分析

1.1 算力网络安全资源池总体架构

算力网络安全资源池总体技术架构由运营层、编排调度层和基础设施层组成[5]，如图1所示。

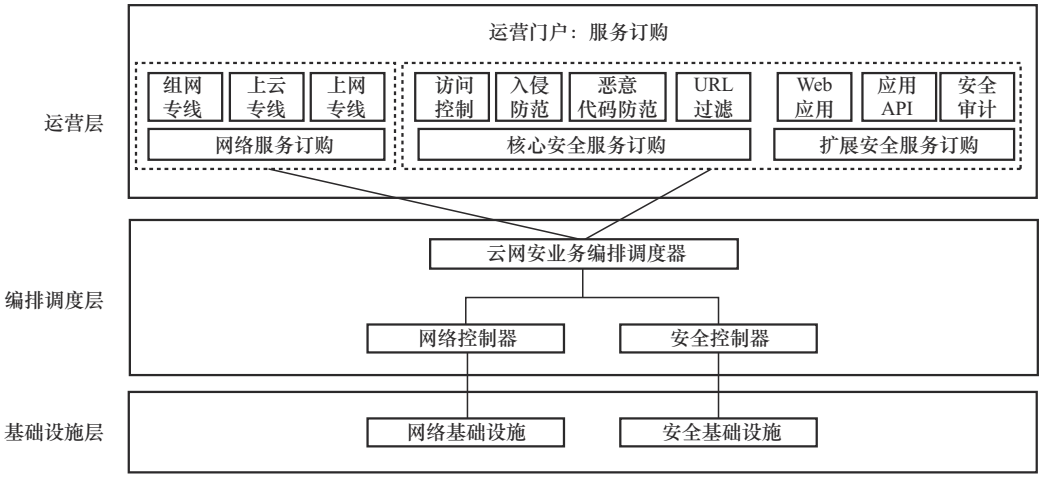

图1　算力网络安全资源池总体技术架构

运营层通过运营门户提供面向企业用户的网络及云化安全原子能力资源池的一体化服务能力。运营门户与云网安业务编排调度器对接，发布客户安全服务订购信息。

编排调度层通过云网安业务编排调度器、网络控制器及安全控制器实现整体业务编排调度功能。编排调度器对接运营门户，接收客户的网络和安全服务订购请求，进行网络和安全资源的调度；对接网络控制器和安全控制器，将资源调度结果发送至网络控制器和安全控制器。网络控制器负责端到端SRv6[6-7]流量工程策略（SRv6 TE Policy）业务链路径编排，并下发给网络基础设施。安全控制器负责用户安全资源分配，并下发给安全基础设施。

基础设施层包括网络基础设施和安全基础设施。网络基础设施指承载网网络设备，对接网络控制器，上报网络拓扑，接收上层路径编排结果；安全基础设施指安全能力资源池，对接安全控制器，接收其下发的安全资源创建要求及用户安全服务映射表，为用户生成对应安全资源。

1.2　传统安全编排调度技术问题

算力网络安全资源池可为客户提供等保合规、数据安全、增强安全、密码安全等多种安全服务能力，并根据市场需求和安全技术发展持续迭代优化[8]。对于防护和检测类安全服务，需将客户流量引流至安全资源池内部进行安全服务，涉及客户流量的网络调度和业务链编排；对于扫描类、运维审计类安全服务，网络可达即可进行服务；对于主机安全类安全服务，用户通过安装客户端网络可达即可进行服务，这类非流量型安全服务不需引流客户流量，但也需编排调度层对订购业务进行业务链编排。因此，编排调度层是算力网络安全资源池的“大脑”，负责网络调度、业务链编排、安全资源管理等安全服务核心能力的实现。

运营商在建设安全资源池时，传统的实现方案是基于策略路由（policy-based routing，PBR）的安全编排调度技术。客户流量在网络中通过匹配PBR进行流量转发，流量牵引至安全资源池内后，需要静态配置安全原子能力逐跳访问策略，按PBR逐项进行安全服务，服务完成后再按PBR将用户流量转发回大网继续进行目的地访问[9]。

基于PBR的安全编排调度，需对客户流量在安全资源池内的逐跳访问策略进行配置，编排策略复杂。配置策略包括安全能力网关融合传输与安全网关（integrated transport and security gateway，ITSG）和各安全原子能力之间逐跳访问的子接口信息、对应的IP地址，并在交换机网络建

立ITSG到各安全网元的业务虚拟可扩展局域网（virtual extensible LAN，VxLAN）转发隧道，通过VLAN-ID标识。以某基于PBR实现安全编排调度的安全资源池为例，订购客户的流量引流至安全资源池后，将在ITSG和各项安全原子能力之间以“打乒乓”的方式进行安全服务，匹配PBR进行转发。

以用户订购安全原子能力1和安全原子能力2为例，基于PBR的安全服务链编排流程如图2所示。

（1）在ITSG IF0（流量入接口）配置PBR策略，ITSG IF1子接口通过匹配访问控制列表（access control list，ACL）重定向策略将流量转发至安全原子能力1-IF3子接口，用户流量在Leaf封装VxLAN隧道进行转发。

（2）安全原子能力1对应的Leaf交换机接收到VxLAN报文后，解封装VxLAN报文进行IP转发，进入安全原子能力1进行服务。

（3）安全原子能力1服务完成后，通过配置默认路由按相同的VxLAN封装、解封流程将流量从安全原子能力1-IF4转发回ITSG IF2。

（4）ITSG IF2配置PBR策略，通过匹配重定向策略按上述相同的转发流程将流量转发到安全原子能力2-IF5子接口，进行安全原子能力2服务。

（5）用户流量完成安全服务后，ITSG按PBR将用户流量转发至网关、城域核心路由器，用户流量回到网络继续转发至访问目的地。

总体来说，传统的编排调度技术存在诸多弊端：流量需经过多次编排，编排效率很低；涉及大量静态规则配置和协议支持，路径调整和扩展需要逐节点配置，难以快速响应市场业务需求；缺乏应用感知能力，无法细颗粒度感知业务需求；在用户标识方面，采用传统基于用户IP地址的标识方式，流量转发和业务识别复杂性高，且仅支持专线等IP地址固定的用户类型，导致安全服务的市场局限性很大[1]。因此，亟须引入高效编排调度技术架构，将网络和安全深度融合，突破传统技术瓶颈，满足多元化安全服务市场和精细化安全防护需求。

2　基于SRv6+ARN的算力网络编排调度技术分析

基于SRv6+ARN的算力网络编排调度技术采用SRv6灵活转发，结合ARN技术提升流量识别效率。该技术将每个安全资源池节点作为段标识符（segment identifier，SID）节点插入SRv6业务链，网络和安全基础设施节点会维护SID列表，根据SID映射表将用户流量转发到下一跳接口，中间节点无须维护任何状态，便可实现高效流量转发；ARN利用IPv6报文的可编程空间，引入应用标识符（ARN ID）进入网络，提供更

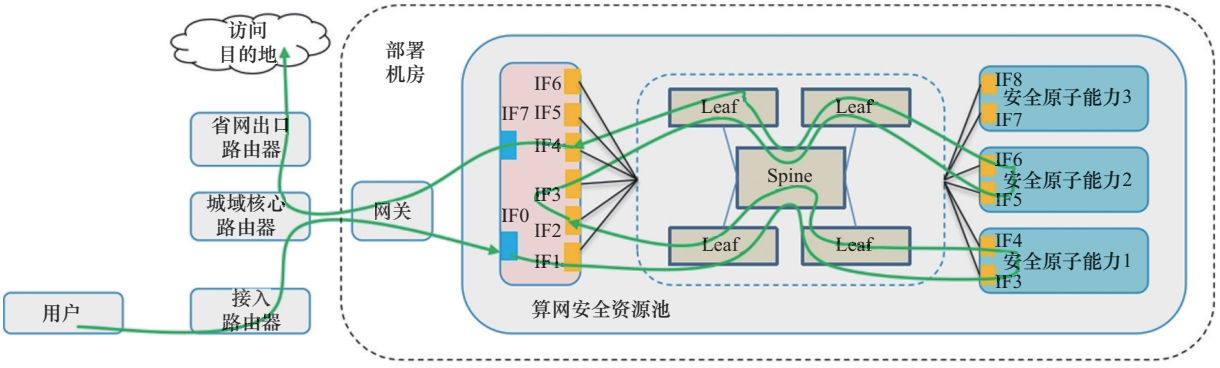

图2　基于PBR的安全编排调度流程图

便捷、精细化的网络服务[10]。

以 SRv6 源路由技术为代表的网络灵活可编程技术[11-12]，使基础承载网络更加弹性和智能，网络服务能力更加丰富和精细化[13]。将应用、业务和基础网络能力进行高效整合，既是 5G/后 5G 时代新型应用和业务的必然需求，也是基础承载网络服务能力延伸和演进的行业趋势。ARN 提供基于数据面进行网络能力开放编程的模型，让应用像调用操作系统一样调用网络资源。例如，上层软件通常在调用操作系统资源时首先需要进行申请，以获取资源句柄及调用权限，然后再以该句柄为应用程序接口（application program interface，API）参数完成处理。在 ARN 的场景中，如果把用户应用看作上层软件，网络能力看作被封装好的操作系统资源，则 ARN ID 就类似资源句柄，用户通过申请一个 ARN ID 获取调用权限后，在报文中携带该 ARN ID 就可以实现对网络能力的调用。ARN 为目前相对分离的业务和网络系统提供了一种创新且平滑兼容的融合架构，为业务和应用侧提供了简明而高效的网络能力接口，为基础网络提供了应用级颗粒度的资源视图和调度能力[10]。

2.1　SRv6+ARN 设计理念

运用 SRv6+ARN 进行网络、安全、算力的融合编排，并将业务、路由、应用各层解耦，有效提升算力网络安全资源池服务灵活性和高效性。SRv6+ARN 的设计理念如下。

（1）基于数据面进行网络能力开放可编程。以软件编程的方式在数据面开放编程接口，让应用像调用操作系统一样调用网络资源。在当今数字化的世界中，用户对网络的需求远远超出了简单的连接功能，用户希望网络能够提供稳定、高速的连接，满足多样化的应用需求。即便是同一类型的应用，不同行业、不同场景中的使用需求也可能各不相同。让应用通过数据面编程来调用网络能力，为不同需求的报文提供相应保障。

（2）将地址和服务解耦。传统的网络设计是基于地址的，即根据目的地址进行管理和路由，确定网络对报文所提供的转发服务。但是，用户应用种类日渐增加，依靠地址携带服务等级使网络管理逐渐复杂。因此，需要根据用户应用的特征和需求来对网络进行管理和优化，将地址和服务分离开来，提供多维度立体的转发服务。

（3）将网络和应用解耦。在网络和应用之间增加 ARN 层，网络不需要直接感知应用，屏蔽了应用的多样性，同时也防止应用直接访问网络能力。通过 ARN 对网络和应用各自进行封装，实现应用隐私及网络内部信息的隐藏。基于该封装，还可实现应用调用网络过程中的访问控制，实现类似软件编程中令牌的授权调用机制。

（4）多种网络资源统一抽象。随着网络服务的个性化和多样化发展，网络在转发用户报文的过程中所使用的网络资源也越来越丰富，如算力、网络切片、服务链等。在使用这些网络资源的过程中，往往需要在报文中携带额外标识来确定用户或应用与网络资源的映射关系，或者使用 ACL 来解析和匹配报文的特征信息，以确定所关联的网络资源。在 ARN 中，多种网络资源可以用 ARN ID 来统一表示，降低了数据面标识的复杂性，简化了运维部署。

2.2　总体技术架构

基于 SRv6+ARN 的算力网络编排调度技术架构如图 3 所示，其由云网安业务编排器、网络控制器和安全控制器组成。云网安业务编排器接收安全业务订购信息并实现 SRv6 业务链编排，采用安全资源池、安全服务能力分层业务链架构实现网络和安全业务解耦。网络控制器、安全控制器实现总体调度，其中网络控制器负责网络流量引流调度，安全控制器 ITSG 负责整体安全资源池业务链的编排引流，安全控制器增值业务服务

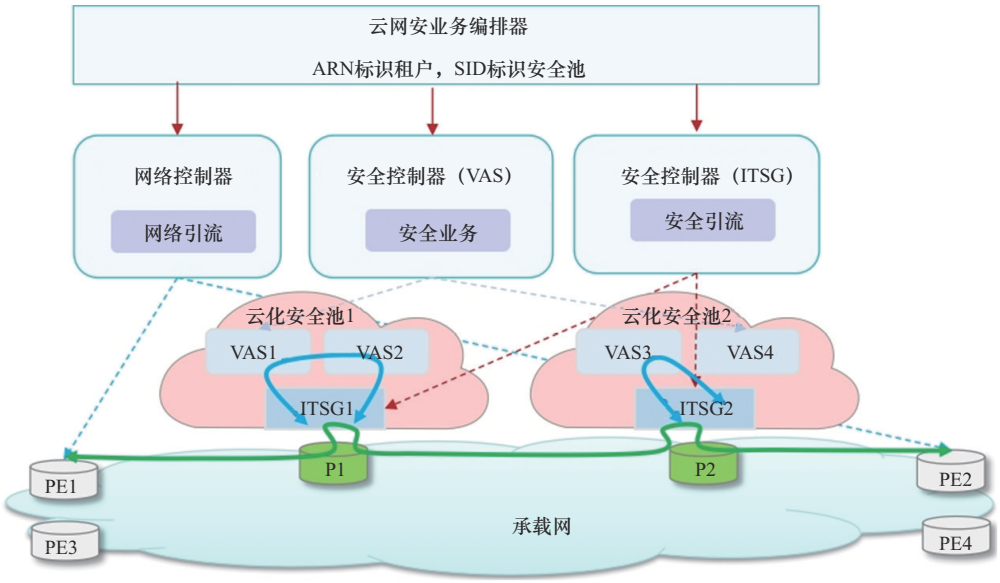

图3　基于SRv6+ARN的算力网络安全编排调度技术架构

（value-added service，VAS）负责具体安全服务子业务链的编排引流。

2.3　数据面格式

SRv6采用IPv6转发技术，通过在IPv6报文中封装段路由报头（segment routing header，SRH）扩展头，在SRH扩展头中定义Segment List（即SID）实现灵活的路由转发，将每个安全资源池节点作为SID节点插入SRv6业务链，无须在网络中间节点维护逐流的转发状态，这种方式极大地简化了路径编排的复杂性，同时提供了更高的灵活性和可扩展性。

在SRH扩展头之后封装目的选项报文头（destination options header，DOH）扩展报文头，可携带ARN ID等信息。该信息仅能被目的节点解析，转发路径上的其他节点不能读取分析该DOH扩展头。利用网络封装业务标识和服务信息，略微增加了数据面的复杂性，但大为简化了控制面。IPv6扩展头格式如图4所示。

传统的网络设计是基于地址的，即根据目的地址确定网络对报文所提供的转发服务，在ARN中，用户可以用ARN ID来统一标识，降低了数据面标识的复杂性，实现网络和应用解耦、地址和服务解耦。ARN报文格式定义ARN ID为32 bit无符号整形，ARN ID可根据业务场景封装为3种类型：仅携带网络标签、仅携带资源标签、同时携带网络及资源标签，满足网络服务保障和增值服务需求。

SRv6+ARN报文数据面格式如图5所示。基于SRv6+ARN报文数据面全面开放网络可编程能力，利用SID编排实现业务路径可编程，通过Segment编排实现安全资源池服务能力可编程；利用DOH扩展头实现客户流量标识即业务可编程，实现网络和业务深度融合，为算力网络安全服务编排调度能力的提升提供了重要的网络技术保障。

2.4　关键技术

网络基础设施和安全资源池支持SRv6基本转发能力，可在算力网络安全资源池建设中全面应用端到端基于SRv6+ARN的算力网络安全编排调度技术。

2.4.1　策略设计

基于SRv6+ARN的业务链编排调度策略由两层业务链构成。客户流量在网络转发时，需要按照业务逻辑依次经过各个网络服务节点，这些

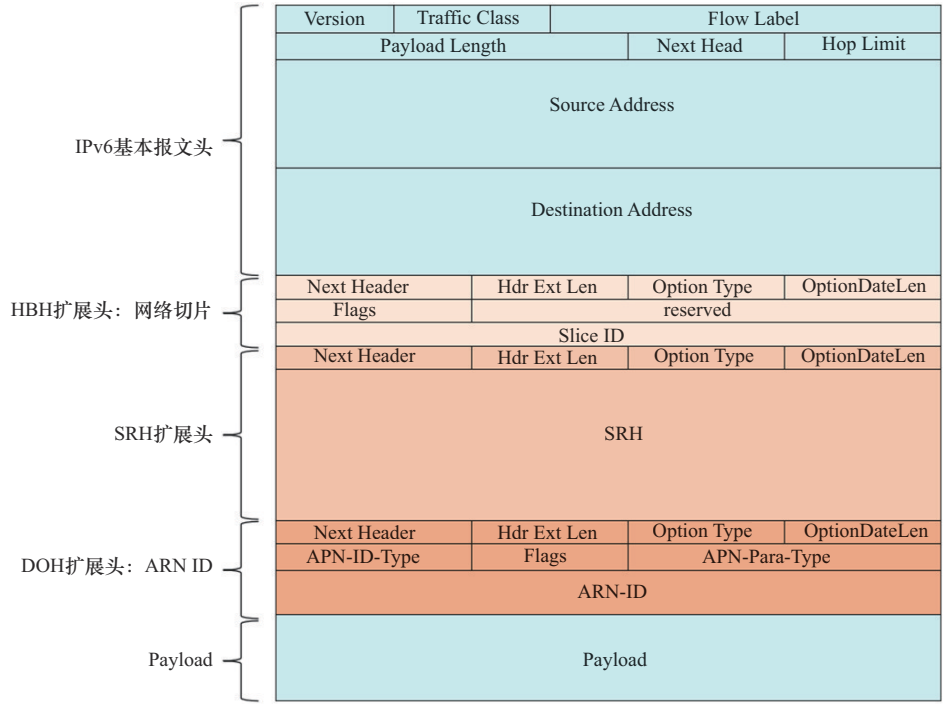

图4　IPv6扩展头格式

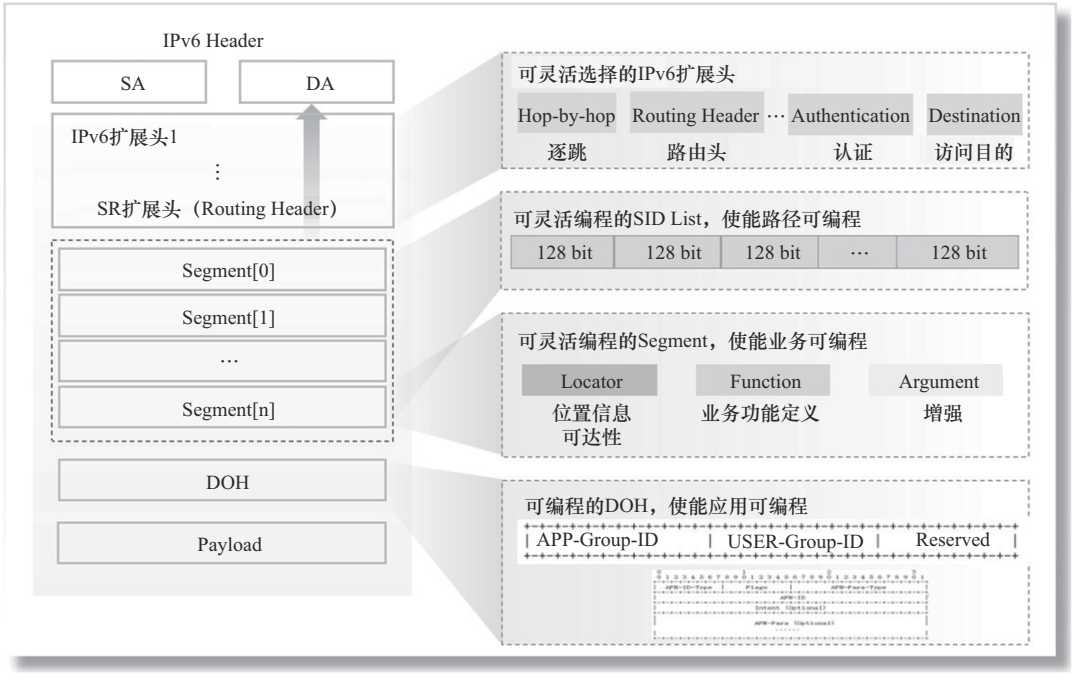

图5　SRv6+ARN报文数据面格式

网络服务节点按顺序组合起来就构成了一个业务链。在安全资源池服务中，主业务链被封装为启动标识符（bootstrap identifier，BSID）；流量进入安全资源池内部后，会依次经过各项安全原子能力进行安全服务，这些安全服务按顺序组合起来就构成了子业务链。两层业务链实现了网络与安全业务解耦，网络不感知具体业务，主业务链主要实现网络编排，子业务链主要实现业务编

排，两层业务链均结合ARN实现客户识别[14]。

客户订购安全服务后，算力网络安全资源池编排调度层需为后续编排调度定义执行策略。SRv6+ARN业务链编排策略根据订购信息为客户分配安全资源池VAS SID（以下简写为vSID）、安全能力资源vSYS、客户标识ARN ID和主业务链BSID等信息，其中每个客户配置唯一ARN ID。假设某客户订购安全能力A+B+C，其中安全能力A、B部署于同一安全资源池VAS1，安全能力C部署于另一安全资源池VAS2，两个安全资源池均部署于同一云设施内。SRv6+ARN业务链编排为客户生成客户标识ARNID1、主业务链BSID1，进入安全资源池VAS后分解为两个子业务链VAS1和VAS2，VAS1提供原子能力A、B对应标识为vSID1，VAS2提供原子能力C对应标识为vSID2，业务流顺序为vSID1→vSID2，从而为该客户依次实现A、B、C 3种原子能力。

2.4.2 业务流程

云网安业务编排器为整个资源池ITSG规划一个BSID，网络控制器编排资源池ITSG BSID到SRv6 Policy，实现第一层业务链编排；资源池ITSG根据ARN ID识别客户映射安全子业务链，展开VSID，VAS内通过ARN ID识别客户映射安全能力资源vSYS，实现第二层业务链编排，进行安全服务。

基于SRv6+ARN的业务链编排调度策略配置流程如图6所示。

（1）运营平台接收客户订单，下发客户订购信息和安全业务配置信息至云网安业务编排器。

（2）云网安业务编排器根据客户订购信息进

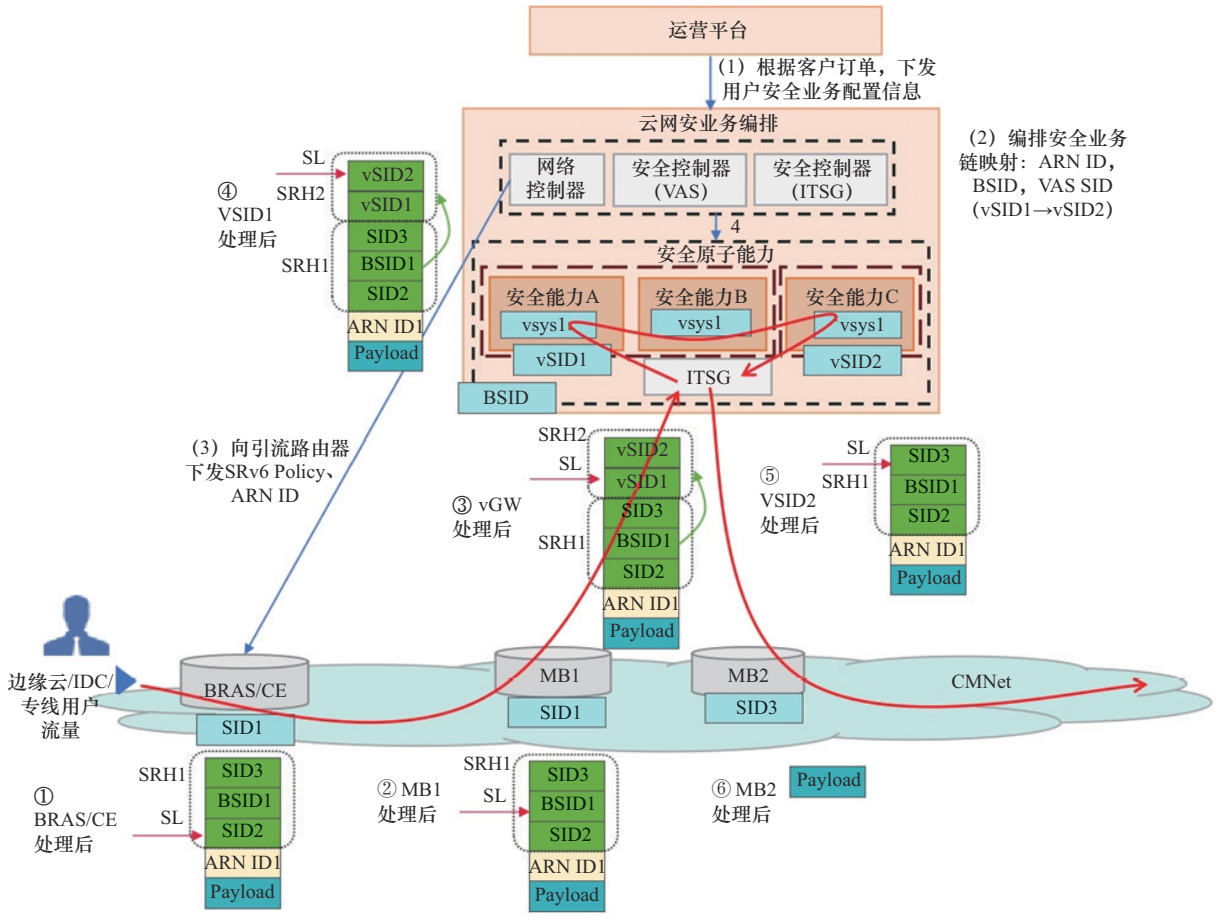

图6 基于SRv6+ARN的业务链编排调度配置策略流程

行网络和安全业务链编排，生成编排策略（包含ARN ID、BSID、VSID等）下发至网络控制器和安全控制器。

（3）网络控制器将BSID插入SRv6业务链中，向网络基础设施下发引流策略（SRv6 Policy、ARN ID等信息）。

（4）安全控制器（ITSG）向安全资源池ITSG下发安全业务链编排策略，安全控制器（VAS）向安全原子能力下发安全服务子业务链的编排。

安全编排策略配置后，基于SRv6+ARN的业务链编排调度流程具体展开如下。

（1）客户侧接入路由器接收到SRv6 Policy后，将用户流量进行SRv6封装，在SRH扩展头中定义路由信息，并加入ARN ID1用于标识用户。以图5为示例，定义BRAS/CE路由器为SID1，MB1路由器为SID2，MB2路由器为SID3，该客户安全资源池服务主业务链为BSID1，扩展头SRH转发路径定义为SID2→BSID1→SID3，用户流量引流到对应的SRv6隧道。

（2）MB1路由器收到目的地址是自己的SRv6报文，将SRH1头的同步层级（synchronization level，SL）偏移至下一个地址，并按该地址将客户流量转发至安全资源池。

（3）安全资源池ITSG展开BSID1，通过ARN ID匹配客户，通过查询业务链策略确定该客户BSID1在安全资源池服务顺序展开为vSID1→vSID2。客户流量封装SRv6外层隧道，外层隧道写入二层业务链编排信息，客户流量可根据外层隧道的路由策略依次经过安全能力进行服务。

（4）安全能力通过ARN ID识别客户，客户流量在vSID1依次经过安全能力A（vsys1）→安全能力B（vsys1）进行安全服务，并通过SRH2转发路径转发至vSID2-安全能力C（vsys1）进行安全服务。

（5）客户流量在vSID2结束安全服务后，在最后一跳解封装外层SRv6隧道，并按照内层SRv6隧道编排将客户流量转发至MB2路由器。

（6）客户流量到达MB2路由器，MB2解封装SRv6隧道，客户流量按照正常路由转发至目的地址。

基于SRv6+ARN的业务链编排调度策略将SRv6技术与ARN结合，极大地丰富了云网安服务的维度和精细度。它不仅包含选路的基本信息，还可携带业务类型、业务优先级等业务关键特征，加载客户行业属性、地域分布、个性化需求等客户信息，实现网络和业务的快速响应和高效服务。相比传统PRB编排调度技术，基于SRv6+ARN的业务链编排调度技术具有多方面的优势，二者的关键技术对比见表1。

2.5　可靠性保障

算力网络安全编排调度的可靠性至关重要，它是保障安全服务稳定运行的基石。可靠性方案主要考虑ITSG可靠性和安全原子能力可靠性，需充分考虑容错和自动恢复机制，这两项保障机制相辅相成，共同为安全编排调度提供坚实支撑，为安全服务保驾护航。

2.5.1　ITSG可靠性保障机制

算力网络安全资源池ITSG负责整个安全资源池流量调度和业务链编排。为保障ITSG可靠性，建议双机或者多虚拟机部署。虚拟机间实现协议表项同步（虚拟机之间表项同步可使用现有技术方案，如共享存储、消息队列、数据库外置、边界网关协议、协议备份等，本文不再累述此技术），每个虚拟机提供不同的网络地址用于L3交换机（SW）做探测，各VAS配置到L3交换机的IPv6默认路由，交换机上配置并发布VAS和ITSG的Locator路由，VAS做完安全服务后，更新SRv6报文目的IPv6地址，发往L3交换机，交换机根据目的IPv6地址选择发往下一个VAS处理

表1　SRv6+ARN与PBR编排技术对比

对比维度	SRv6+ARN	PRB策略路由
路径编排灵活性	SRv6通过在IPv6报文中新增SRH扩展头，支持在入节点显式编程数据报文的转发路径，无须在网络中间节点维护逐流的转发状态。这种方式极大地简化了路径编排的复杂性，且提供了更高的灵活性和可扩展性	PRB通常依赖于静态配置和复杂的协议支持，路径调整和扩展需要逐节点配置，灵活性较差
网络可编程能力	SRv6具备强大的网络可编程能力，支持三级编程模型：SID列表用于路径规划，SID中的三字段（定位器、功能、参数）用于业务功能实现，以及通过TLV携带应用信息。结合ARN，SRv6能够直接在IPv6报文中携带应用信息（如ARN ID和应用需求参数），实现应用级别的流量编排和网络服务	PRB主要依赖于传统的网络协议和静态配置，缺乏动态编程能力
扩展性和兼容性	SRv6基于IPv6的原生属性，具有天然的可扩展性，支持大规模网络部署。同时，SRv6与现有的IPv6+技术（如网络切片、iFIT等）完全兼容，能够实现更精细化的网络服务	PRB在大规模网络中扩展性较差，通常需要逐节点配置和维护
应用感知能力	通过ARN技术，SRv6能够在IPv6报文中直接携带应用信息（如ARN ID和应用需求参数），使网络设备能够感知应用需求并提供差异化的服务。这种方式简化了应用识别流程，减少了对深度报文检测（deep packet inspection，DPI）的依赖	PRB缺乏应用感知能力，通常需要额外的DPI或ACL规则来识别应用
运维复杂性	SRv6简化了网络协议，减少了对复杂协议（如LDP、RSVP-TE等）的依赖。结合ARN，网络设备可以直接通过IPv6扩展头获取应用信息，减少了ACL资源消耗	PRB编排依赖于复杂的协议和静态配置，运维复杂性较高
安全性	SRv6结合ARN能够实现应用级别的流量隔离和加密传输。同时，SRv6的SID可以携带安全策略信息，进一步增强网络的安全性	PRB的安全性主要依赖于传统的网络隔离技术，缺乏应用级别的安全策略支持

或者返回ITSG。当ITSG虚拟机故障时，L3交换机探测到ITSG虚拟机不可达，对于回程路由会自动将流量切换到ITSG的其他虚拟机，保障不影响用户流量正常流转。ITSG可靠性保障机制示意图如图7所示。

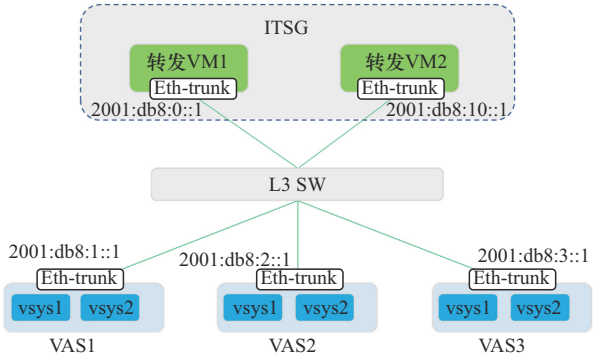

图7　ITSG可靠性保障机制示意图

2.5.2　安全原子能力可靠性保障机制

算力网络安全资源池整体架构设计需充分考虑安全原子能力可靠性。若运营商未进行VAS主备部署，在设计安全服务的可靠性时，应以不影响用户流量正常流转为首要前提。当ITSG收到业务报文后，识别租户ARN ID，根据租户订购的安全服务映射安全业务子链，封装VAS SID列表。此时部署基于TE的快速重路由技术（traffic engineering fast reroute，TE FRR），当ITSG检测其中某个VAS SID不可达后，目的IPv6地址自动更新为下一个VAS SID，绕开该安全网元，将流量引流到下一个VAS。单VAS部署可靠性保障机制示意图如图8所示。

步骤1　定义SRv6 Policy。在ITSG上定义

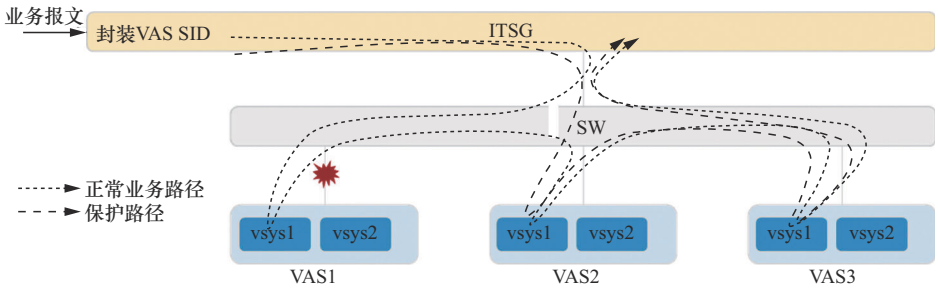

图8　单VAS部署可靠性保障机制示意图

SRv6 Policy，指定头端为ITSG，尾端为各VAS的SID，为每个VAS配置对应的SRv6路径。例如，对于VAS1、VAS2等，分别定义不同的SID，每个SID包含到达相应VAS的SID序列。

步骤2　关联应用流量。将需要经过VAS处理的应用流量与相应的SRv6 Policy关联。通过在ITSG上配置流分类和策略路由，将特定的流量匹配到相应的SRv6 Policy，使流量按照指定的路径转发到对应的VAS进行处理。

当安全原子能力建设时进行了安全网元主备部署，主备安全网元应配置不同的IP地址，且具备自提供热备份能力。ITSG根据SRv6报文中的ARN ID识别租户，同时根据租户订购的安全服务对BSID进行展开，封装VAS SID列表。ITSG安全控制器下发SRv6 TE Policy，包含主备2条候选路径，部署单臂双向转发侦测（bidirectional forwarding detection，BFD）对主备路径进行检测。当主路径中出现任意故障时能快速切到备路径，主备场景整体编排方案如图9所示。

步骤1　配置FRR保护。在ITSG上为每个SRv6 Policy配置TE FRR保护。TE FRR通过计算备份路径来实现故障保护。当检测到当前路径上的某个VAS SID不可达时，能够快速切换到备份路径。备份路径可以是预先计算好的另一条SRv6路径，其尾端为下一个可用的VAS SID。

步骤2　BFD联动检测。部署BFD与TE FRR联动，以实现快速故障检测。在ITSG与各个VAS之间建立BFD会话，当某个VAS出现故障时，BFD能够快速检测到并通知ITSG。ITSG随即触发TE FRR机制，将流量切换到备份路径，从而实现对故障VAS的快速切换。

2.6　基于SRv6+ARN的编排调度技术设计实例

基于SRv6+ARN的编排调度案例设计，可以根据不同行业的具体合规要求，通过合理分配ARN标签、精心设计SRv6策略路径，以及利用SRv6的网络编程和监控能力，实现定制化的安全业务链，有效满足客户的行业属性和地域合规要求。

以医疗行业数据隐私保护与共享场景需求为例，某大型医疗集团旗下多家医院分布在不同地区，需要共享患者医疗数据以实现远程会诊和联合科研，但必须严格遵守美国健康保险流通与责任法案（HIPAA）等医疗数据隐私法规[15]，确保患者数据不被非法访问和泄露。

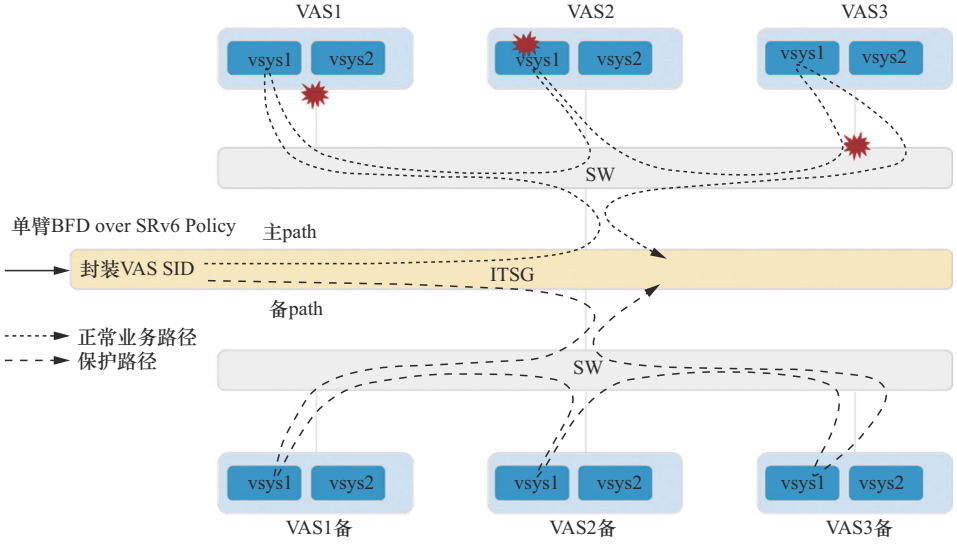

图9　主备场景整体编排方案

SRv6+ARN适配设计如下。

（1）ARN精细分类。为不同医院的网络出口设备分配“Hospital_A_Network”“Hospital_B_Network”等ARN ID，为医疗数据存储服务器分配“HIPAA_Compliant_Storage” ARN ID，为各类安全服务设备（如防火墙、加密网关）分配对应的“Medical_Data_Firewall”“Medical_Data_Encryption”ARN ID。

（2）定制化SRv6业务链。当Hospital A的医生发起远程会诊请求，并将涉及的患者数据发送给Hospital B时，SRv6策略路径为Hospital A医疗终端→带“Hospital_A_Network”标签的出口设备→ITSG→带“Medical_Data_Firewall”标签的VAS（进行深度数据检查和访问控制）→带“Medical_Data_Encryption”标签的VAS（对数据加密）→带“SRv6_Secure_Path”标签的加密链路→带“Hospital_B_Network”标签的接收设备→带“HIPAA_Compliant_Storage”标签的存储服务器。在整个过程中，通过SRv6 Policy确保数据只在授权的合规节点间传输和处理，并且每个环节都根据ARN ID进行严格的标签匹配和策略执行。

（3）审计与溯源。利用SRv6网络编程的可编程性，记录每个数据包在SRv6网络中的流转路径和经过的安全服务节点，以及每个节点的处理动作和时间戳。结合ARN ID标签信息，形成详细的审计记录，以便在发生数据泄露或其他安全事件时，能够快速溯源，确定问题环节和责任主体，同时也有助于定期的合规审计工作的顺利开展。

3 结束语

基于SRv6+ARN的算力网络安全编排调度技术以高效编排调度、云网安深度融合为算力网络安全资源池服务注入强大竞争力，使得网络能够深度感知业务与客户的双重需求，进而实现网络和业务的快速响应与高效服务。

未来，该技术的应用还可为安全服务拓展更多的市场空间。在面对突发的业务流量高峰时，SRv6技术灵活的选路能力，结合ARN对云资源的精准定位，使算力网络安全系统能够迅速调配合适的网络带宽资源，优先保障高优先级业务的流畅运行，避免因网络拥塞导致业务卡顿甚至中断；根据客户的行业属性要求，基于SRv6技术构建定制化的安全业务链，通过精确的选路将数据包引导至相应的安全检测节点，如针对医疗行业客户重点强化数据加密与防篡改检测，实现全方位、精细化的安全防护，提升客户满意度与忠诚度，全面推动算力网络安全资源池服务迈向更新的发展高度。

参考文献：

[1] 何涛, 杨振东, 曹畅, 等. 算力网络发展中的若干关键技术问题分析[J]. 电信科学, 2022, 38(6): 62-70.
HE T, YANG Z D, CAO C, et al. Analysis of some key technical problems in the development of computing power network[J]. Telecommunications Science, 2022, 38(6): 62-70.

[2] 贾庆民, 郭凯, 周晓茂, 等. 新型算力网络架构设计与探讨[J]. 信息通信技术与政策, 2022(11): 18-23.
JIA Q M, GUO K, ZHOU X M, et al. Design and discussion on novel computing power network architecture[J]. Information and Communications Technology and Policy, 2022(11): 18-23.

[3] 朱文阅, 董江帆, 李玉华, 等. 算力网络安全与数据安全治理技术研究[J]. 电信工程技术与标准化, 2024, 37(1): 12-17.
ZHU W Y, DONG J F, LI Y H, et al. Research on computing power network security and data security governance technologies[J]. Telecom Engineering Technics and Standardization, 2024, 37(1): 12-17.

[4] 韩婷婷, 杨锋, 姜文颖, 等. 基于IPv6的应用响应网络技术创新与实践[J]. 通信世界, 2024(19): 46-48.
HAN T T, YANG F, JIANG W Y, et al. Technical innovation and practice of application response network based on IPv6[J]. Communications World, 2024(19): 46-48.

[5] 邱勤, 徐天妮, 于乐, 等. 算力网络安全架构与数据安全治理技术[J]. 信息安全研究, 2022, 8(4): 340-350.

QIU Q, XU T N, YU L, et al. Security architecture of computing power network and data security governance technologies[J]. Information Security Research, 2022, 8(4): 340-350.

[6] 李硕朋, 方娟, 陈肯. 基于SRv6的确定性网络服务共享保护方案[J]. 通信学报, 2021, 42(10): 32-42.
LI S P, F J, CHEN K. DetNet service share protection scheme based on SRv6[J]. Journal on Communications, 2021, 42(10): 32-42.

[7] 黄光平, 史伟强, 谭斌. 基于SRv6的算力网络资源和服务编排调度[J]. 中兴通讯技术, 2021, 27(3): 23-28.
HUANG G P, SHI W Q, TAN B. Orchestration and scheduling of computing power network resources and services based on SRv6[J]. ZTE Communications, 2021, 27(3): 23-28.

[8] 王泽南, 李佳浩, 檀朝红, 等. 面向网络安全资源池的智能服务链系统设计与分析[J]. 网络与信息安全学报, 2022, 8(4): 175-181.
WANG Z N, LI J H, TAN Z H, et al. Design and analysis of intelligent service chain system for network security resource pool[J]. Journal of Network and Information Security, 2022, 8(4): 175-181.

[9] 马记, 刘刚. 浅谈策略路由与路由策略[J]. 网络安全和信息化, 2021(7): 78-80.
MA J, LIU G. A brief discussion on strategic routing and routing strategies[J]. Cybersecurity & Informatization, 2021(7): 78-80.

[10] 中华人民共和国工业和信息化部. 基于SRv6的安全能力调度技术要求: YD/T 6023—2024[S]. 2024.
Ministry of Industry and Information of the People's Republic of China. Safety capability scheduling technology requirements based on SRv6: YD/T 6023—2024[S]. 2024.

[11] 曹畅, 张帅, 刘莹, 等. 基于通信云和承载网协同的算力网络编排技术[J]. 电信科学, 2020,36(7):55-62.
CAO C, ZHANG S, LIU Y, et al. Convergence of telco cloud and bearer network based computing power network orchestration[J]. Telecommunications Science, 2020, 36(7): 55-62.

[12] 庞冉, 易昕昕, 辛亮, 等. 算力网络路由调度技术研究[J]. 电信科学, 2023, 39(8): 149-156.
PANG R, YI X X, XIN L, et al. Research on routing scheduling technology of computing power network[J]. Telecommunications Science, 2023, 39(8): 149-156.

[13] 王鹏睿, 胡宇翔, 崔鹏帅, 等. 基于可编程数据平面的SRv6功能一致性验证机制[J]. 计算机科学, 2024: 1-12.
WANG P R, HU Y X, CUI P S, et al. SRv6 functional conformance verification mechanism based on the programmable data plane [J]. Computer Science, 2024: 1-12.

[14] 中华人民共和国工业和信息化部. 基于SRv6的业务链技术要求: YD/T 4784—2024[S].2024.
Ministry of Industry and Information of the People's Republic of China. Technical requirements for service chains based on SRv6: YD/T 4784—2024[S]. 2024.

[15] 曾益康. 数据时代健康信息交换中的隐私保护: 以美国《HIPAA法案》为例[J]. 中国数字医学, 2022, 17(3): 6-10.
ZENG Y K. Privacy protection in health information exchange in the data era: A case study of the U.S. HIPAA Act[J]. China Digital Medicine, 2022, 17(3): 6-10.

[作者简介]

郗卓宁（1980– ），男，中国移动通信集团有限公司高级工程师，主要研究方向为IT信创技术、云计算及人工智能技术等。

侯慧芳（1986– ），女，中国移动通信集团设计院有限公司高级工程师，主要从事基于算力网络的新一代网络安全关键技术方面的研究工作。

潘洁（1978– ），女，中国移动通信集团设计院有限公司高级工程师，主要研究方向为算力网络安全和信息安全。

赵占军（1972– ），男，中国移动通信集团设计院有限公司网络所所长，主要研究方向为移动通信核心网、云计算及人工智能技术、算网安全等。

卜忠贵（1976– ），男，中国移动通信集团设计院有限公司正高级工程师，主要研究方向为移动通信核心网、云计算及人工智能技术、算网安全等。

叶兰（1979– ），女，中国移动通信集团有限公司高级工程师，主要研究方向计算机科学技术网络及数据安全。

陈曦（1989– ），男，现就职于中国移动通信集团设计院有限公司，主要从事网络与数据安全方面的研究工作。

薛曌（1992– ），女，现就职于中国移动通信集团设计院有限公司，主要从事网络安全监测、算力网络安全、商用密码的研究工作。