

基于VPP的SRv6增强型网络安全机制实现

Implementation of SRv6 Enhanced Network Security Mechanism Based on VPP

汤泳¹,由志远¹,张珂珂²,高允翔³,陈亚峰¹(1. 中讯邮电咨询设计院有限公司,北京 100048;2. 中国联通小沃科技有限公司,上海 200082;3. 中国联合网络通信集团有限公司,北京 100033)

Tang Yong¹,You Zhiyuan¹,Zhang Keke²,Gao Yunxiang³,Chen Yafeng¹(1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 10048, China; 2. China Unicom Xiaowo Technology Co., Ltd., Shanghai 200082, China; 3. China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘要:

分析了SRv6协议面临的安全威胁,介绍了通过HMAC方式增强SRv6网络安全的方案及原理。说明了SRv6 HMAC封包及校验算法的相关流程和细节,并详细分析了基于VPP的SRv6 HMAC增强安全方案的具体实现过程及方法。最后,对在VPP中开启HMAC增强安全方案带来的性能损失进行了对比测试。

关键词:

SRv6;网络安全;VPP;HMAC;RFC 8754

doi:10.12045/j.issn.1007-3043.2026.09.015

文章编号:1007-3043(2026)09-0079-05

中图分类号:TN918

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

The security threats faced by the SRv6 protocol are analyzed, and the solution and principles of enhancing SRv6 network security through HMAC are introduced. Then the process and details of SRv6 HMAC packet encapsulation and verification algorithms are outlined. Furthermore, a detailed explanation of the specific implementation process and methods of SRv6 HMAC enhancement security scheme based on VPP (Vector Packet Processing) is provided. Finally, comparative tests are conducted to evaluate the performance impact of enabling HMAC enhancement security scheme in VPP.

Keywords:

SRv6; Network security; VPP; HMAC; RFC 8754

引用格式:汤泳,由志远,张珂珂,等. 基于VPP的SRv6增强型网络安全机制实现[J]. 邮电设计技术,2026(9): 79-83.

1 背景

全球信息化的不断推进使互联网应用得到了迅速而蓬勃的发展,随着网络规模的扩大以及云时代的到来,网络业务种类越来越多,不同业务对网络的要求不尽相同,传统IP/MPLS网络遇到不少挑战。基于IPv6转发平面的段路由(Segment Routing IPv6, SRv6)^[1]是新一代IP承载协议,其结合了SR源路由优势和IPv6简洁易扩展的特质,具有独特的优势。SRv6具有强大的可编程能力^[2],它具有网络路径、业务、转

发行为三层可编程空间,能支撑大量不同业务的不同需求,契合业务驱动网络的潮流^[3]。

SRv6的可编程特性也使其面临与传统IPv6网络不同的安全威胁。攻击者可以通过修改SRH头部信息在SRv6网络中实施攻击^[4-5]。如图1所示,SRv6网络攻击者主要通过伪造、修改SRv6报文的SRH头信息^[6],引导网络流量偏离正常路径,如将流量导入到非法网络设备(如图1中路由器PX)中进行网络流量的窃取、修改、丢弃等操作^[7]。

目前,SRv6网络安全方案主要分为基础方案和增强方案。基础方案主要通过ACL进行流量过滤,丢弃非法访问内部信息的流量;增强方案则通过对通信源

收稿日期:2026-08-03

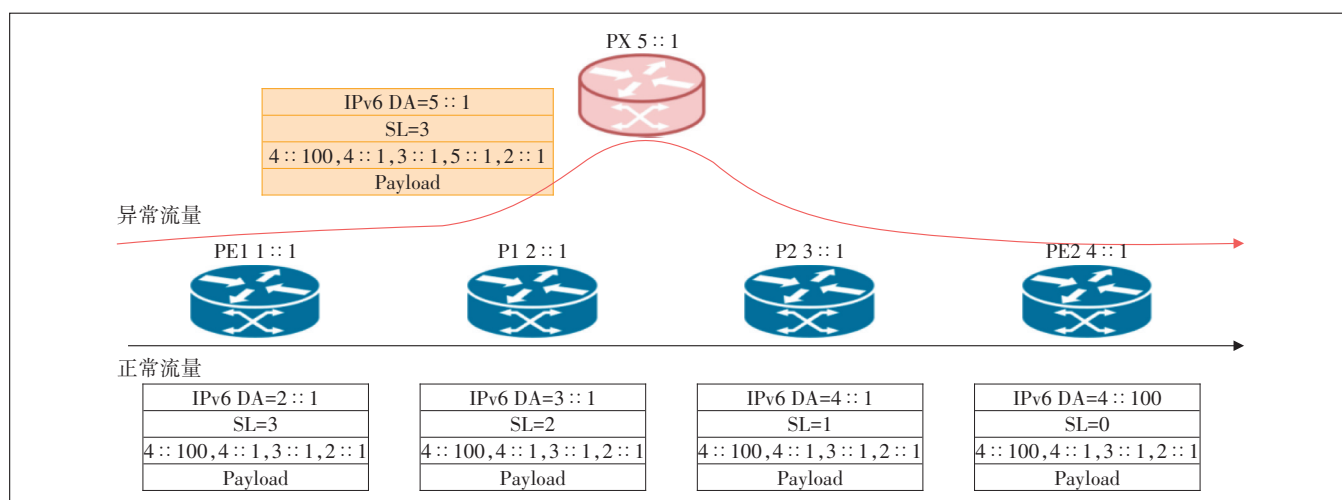


图1 修改SRv6 SRH方式网络攻击示意

进行身份验证,对SRv6进行报文级检验防止SRv6网络受到攻击。

SRv6网络安全基础方案^[8-9]主要通过部署网络ACL策略对可信域外进入的报文进行防范,通过对外连接接口及网络内部接口上配置ACL规则,对报文源地址及目的地址进行合法性校验,丢弃不合法的报文。

a) 外连接口上需配置ACL规则。若收到的SRv6报文的源地址或目的地址来自分配SID的地址块,则丢弃报文。这是因为正常情况下不应该将内部SID泄露到域外,若被域外获取,则认定携带该地址的报文为攻击报文。

b) 网络内部接口上也需配置ACL规则。当SRv6报文的目的地址为本地SID,且源地址不是内部SID或内部接口地址,或不在SID空间范围内时,则将报文丢弃。这是因为只有可信域内部的设备才能进行SRv6报文封装,所以当目的地址是SID时,源地址必须是内部的SID或者内部接口地址。

上述基础方案可在一定程度上防止SRv6网络受到攻击,然而如果SRv6可信域网络内部存在具有漏洞的设备,或者具备封包能力的外部设备恶意进行SRv6报文SRH头的封装行为,则会导致上述基础网络安全方案失效^[10]。通过基于HMAC机制的SRv6增强网络安全方案,可以确保网络设备对SRv6报文中的SRH头进行高强度的合法性校验,从而解决通过篡改SRH方式进行SRv6攻击的网络安全风险。

VPP(Vector Packet Processing)^[11]是由Linux基金会的FD.IO组织开源的高性能、可扩展的用户空间数据平面软件框架,目前广泛应用于构建网络功能虚拟

化(NFV)和中小型网络设备的转发面解决方案。在VPP开源框架中实现SRv6 HMAC安全具有较强的工程应用意义。

2 HMAC网络安全方案概述

2.1 报文格式

RFC 8754^[12]标准文稿定义了SRH报文及其中的HMAC TLV字段^[13]的具体内容,其结构如图2所示。

IPv6报文符合RFC 8200文稿所规定的IPv6报文格式,因而可被普通IPv6路由器转发;SRH头数据跟在普通的IPv6基本头之后,其中较重要的内容如下。

a) Next Header: 8 bit,用来标识下一个报文的类型。

b) Hdr Ext Len: 8 bit,表示以8个字节为单位的SRH头的长度,不包括首8字节。

c) Routing Type: 8 bit,路由类型字段,取值为4,表示携带的是SRH。

d) Segments Left: 8 bit,标识需要查看的下一个SID的编号,初始取值为 $n-1$ (n 表示路由扩展头中SID的数目),每经过一个节点减1。

e) Last Entry: 8 bit,SRH头中报文实际转发路径的第一个SID的编号。

f) Segment List: SID列表。按照报文转发路径上节点从远到近的顺序进行排列,即Segment List[0]表示路径的最后一个SID,Segment List[1]表示路径的倒数第二个SID,以此类推。

HMAC TLV为SRH头中的可选字段内容,其格式内容如下。

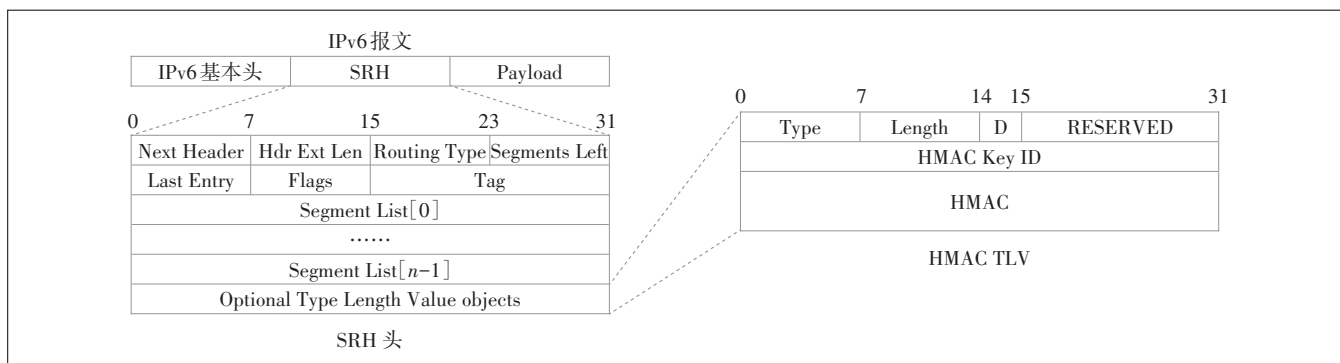


图2 SRv6 HMAC报文结构

- a) Type: 8 bit, 取值为5。
- b) Length: 7 bit, 可变长度数据的长度, 以字节为单位。
- c) D: 1 bit。1表示使用了缩减的Segment List, 此时不进行IPv6目标地址的检查。
- d) RESERVED: 15 bit。须为0。
- e) HMAC Key ID: 4 B, 唯一标识用于生成HMAC的预共享密钥和算法。
- f) HMAC: 报文HMAC计算结果, 以8个字节的倍数为单位, 最多为32 B。

2.2 HMAC 校验流程

在网络设备中进行SRv6 HMAC校验的主要流程如图3所示。

- a) 设备接收并存储预共享密钥。
- b) 检查报文中HMAC是否存在, 如不存在则直接丢弃。
- c) 检查报文SL(Segments Left)是否大于Last Entry, 如大于且HMAC TLV D标志位为1, 则认为是正常报文; 如小于或等于, 则判定报文IPv6目的地址(DA)是否与SL指向的地址相同, 如相同则认为是正常报文。如不满足上述2个条件, 则认为是异常报文并丢弃。该步骤的目标为判定目标地址与当前报文SL指向的地址是否一致。

d) 如通过前述检查, 则根据RFC 8754计算报文的HMAC值。对比该HMAC值与报文携带HMAC值是否相同, 如相同则认为是正常报文, 否则生成ICMP错误信息并记录, 同时丢弃该报文。

2.3 报文HMAC计算方法

SRv6报文HMAC TLV中的HMAC字段根据RFC 2104中定义的方法进行计算, HMAC计算由3个要素构成, 具体如下。

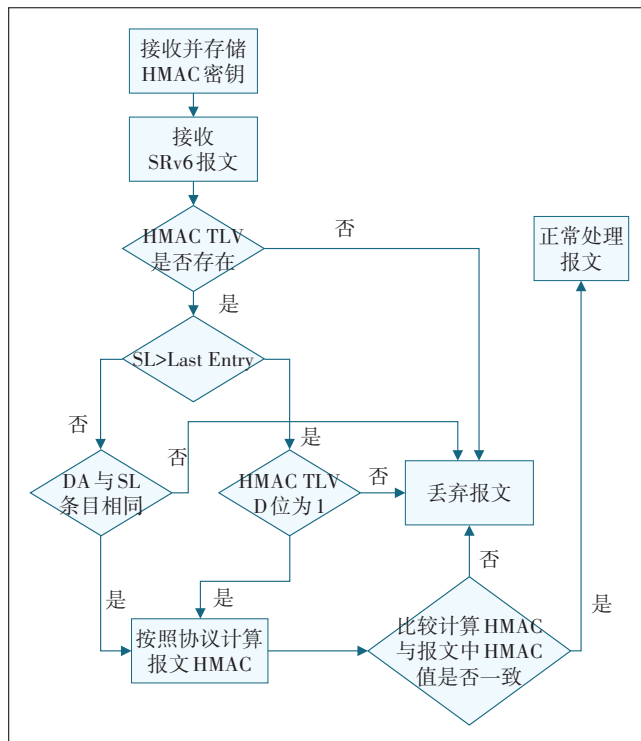


图3 SRv6 HMAC校验流程

- a) 密钥(Key): 预共享密钥, 由HMAC密钥ID标识。
 - b) HMAC算法: 由HMAC密钥ID标识。
 - c) 文本(Text): 通过IPv6标准头部和SRH的部分字段的连接形成, 具体如下。
 - (a) IPv6 Header: 源地址(16 B)。
 - (b) SRH: Last Entry(1 B)。
 - (c) SRH: Flags(1 B)。
 - (d) SRH: HMAC长度后16位(2 B)。
 - (e) SRH: HMAC Key ID(4 B)。
 - (f) SRH: 段列表中的所有地址(可变字节)。
- HMAC摘要被截断为32 B, 并放置在HMAC TLV

的HMAC字段中。对于产生长度少于32 B的HMAC算法,需将HMAC摘要放置在HMAC字段低位,并以0补齐,使HMAC长度为8 B的倍数。

从以上流程及算法可以看出,在保障预分配密钥安全的情况下,任何对SRv6报文与网络传输相关部分内容的修改都会导致后续网络节点HMAC校验失败,从而保障了SRv6网络的安全。

3 SRv6 HMAC安全在VPP开源框架中的实现

3.1 VPP简介及其数据包处理流程

VPP库是Linux基金会FD.io的核心组件,该组件是思科矢量包处理技术(Vector Packet Processing)的开源版本。由于其在数据包软转发(利用CPU转发数据包而非网络处理器)的高性能特性,本身已具备丰富的网络功能集及便于扩展自研网络功能等特性,在NFV及中小型网络设备领域有着广泛的应用。

VPP库基于数据平面开发包(DPDK)开发^[14],除利用DPDK的轮询模式驱动程序(PMD)和环形缓冲区支持以提高数据转发性能以外,VPP主要的特性是采用矢量包处理机制。该机制将一批底层硬件队列收到的数据包,组成一个数据包矢量(Packet Vector),然后借助报文处理图以矢量方式处理报文。

采用矢量报文处理方式处理一批报文时,如果指令Cache命中,则这一批报文都命中;否则这一批报文都未命中。未命中时,使用矢量报文中的第一个数据包来加热高速缓存,后续数据包重复执行缓存中所得到的指令,以在整个报文分组中分摊一个报文的高速缓存未命中时间。该方式利用了数据报文流时间局限性的特点,大大提高了CPU指令Cache在处理网络报文时的命中率,并且利用一次性读取多个报文,缓解报文读时延问题,从而提升了网络报文的处理效

率,具备较好的性能。

VPP采用节点图方式组织矢量报文的处理流程,通过研发自定义的图节点并将其插入到VPP运行节点图当中,或者在相应的图节点中注册外部回调函数等方式,实现VPP库功能的拓展。

3.2 SRv6 HMAC在VPP中的实现方案

SRv6 HMAC功能在VPP中的实现^[15]如图4所示。

a) 数据包通过DPDK从网卡接收数据进入以太网2层数据包输入处理(12-input)节点。

b) 在VPP框架中注册路由DPO(Data Path Object,在VPP中用来确定数据包路由的自定义数据结构)对象,将数据包引流到不同的节点处理,分别进行HMAC封包或HMAC校验。

c) 本方案不添加新的矢量数据图处理节点,而采用在原有VPP库的SRv6处理节点(sl-pl-rewrite-encaps、sr-localsid)添加外部回调函数的方式实现SRv6 HMAC相关处理逻辑。在SRv6封装HMAC时,根据前述算法进行HMAC TLV的生成,并加入SRH头中;在校验时,对SRH头中包含的HMAC TLV数据进行校验。上述回调函数如失败则丢弃报文。

d) 如封装或校验行为成功,则将矢量数据包重新传递给IPv6路由查找节点(ip6-lookup)和IPv6数据发送节点(ip6-rewrite)进行矢量数据包的转发任务。

3.3 主要代码处理流程

3.3.1 封装HMAC TLV流程

该流程需要在VPP框架中的“SID列表重写封包”节点(sl-pl-rewrite-encaps)挂载回调函数,VPP封装HMAC TLV伪代码如图5所示。

3.3.2 解封装侧验证HMAC流程

该流程需在VPP框架的“SRv6本地SID处理”节点(sr-localsid)挂载回调处理函数,该函数的主要处理

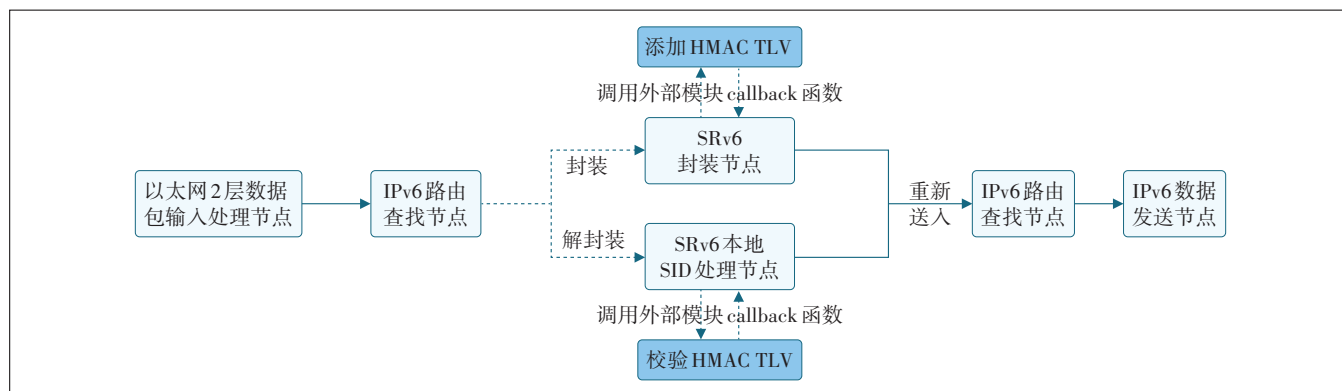


图4 VPP实现SRv6 HMAC示意图

```
Require: 输入数据包缓冲区b, HMAC参数(哈希长度、密钥ID等)
Ensure: 修改后的数据包包含 HMAC TLV
1: 提取IPv6头部ip和SRH头部srh
2: 计算HMAC 可变长度 hmac_var_len:
3: if 哈希长度<32 then
4:   计算填充长度 padding←(8-(hash_len mod 8))mod 8
5:   hmac_var_len←hash_len+padding
6: else
7:   hmac_var_len←32           ▷ 截断至32字节
8: end if
9: 验证缓冲区预留空间 assert(b.current_data≥hmac_len)
10: 调整缓冲区指针:
11: 前移hmac_len字节
12: 复制原始头部数据到新位置
13: 更新SRH头部:
14: 设置HMAC标志位 srh.flags←srh.flags V 0x01
15: 定位HMAC TLV 位置 hmac←srh+srh.length×8+8
16: 填充TLV元数据:
17: hmac.type←SRV6_HMAC_TYPE
18: hmac.length←hmac_var_len
19: 设置密钥ID hmac.key_id←shm.key_id
20: 更新SRH长度 srh.length←srh.length+hmac_len/8
21: 构建HMAC输入数据:
22: 复制源地址src_addr到输入缓存
23: 添加SRH元数据: last_entry.flags, hmac.flags
24: 添加段列表segments[0..last_entry]
25: 计算HMAC:
26: 初始化加密操作 op←HMAC_SHA1()
27: 执行加密 vnet_crypto_process_ops(op)
28: if 哈希长度<32 then
29:   复制结果 hmac.hmac←op.digest[0..hash_len-1]
30:   填充零 hmac.hmac[hash_len..hmac_var_len-1]←0
31: else
32:   截断结果 hmac.hmac←op.digest[0..31]
33: end if
34: return 0           ▷ 处理成功
```

图5 VPP封装HMAC TLV伪代码流程

逻辑与封装HMAC流程类似,较封装过程增加的代码处理逻辑如下。

a) 检查报文是否包含HMAC TLV。

b) 判断报文目标地址与当前报文SL指向的地址是否一致,不一致则丢弃。

c) 采用前文所述的办法计算该报文的HMAC值,并与报文中携带的HMAC值进行比对,如果相同则通过校验,否则不通过,并丢弃报文。

3.4 性能对比测试

以上述方式在VPP中实现HMAC机制后,开启HMAC与关闭HMAC网络转发性能对比如表1所示。

4 结语

新一代IP承载协议SRv6由于其可编程、扩展灵活以及支持多种新业务等优势,在数通网络中得到了广泛的应用,同时也带来了新的安全威胁。针对SRv6网络特有的SRv6 SRH修改的攻击方式,本文介绍了

表1 开启与关闭HMAC网络转发性能对比(单位:Gbit/s)

序号	场景	1 024 B 报文	512 B 报文	256 B 报文	64 B 报文
1	不开启 HMAC	10	10	8.2	3.6
2	开启 HMAC	9.1	8.71	6.81	1.43

测试环境:CPU为Intel(R) Atom(TM) CPU C3558 @ 2.20 GHz;RAM为2 133 MHz,8 GB;网卡为Intel X553 10 GbE SFP+。

基于HMAC机制的SRv6增强网络安全方案,并探讨了其在VPP开源框架中的详细实现方案。由于VPP框架目前被广泛应用于NFV网元及中小型网络设备中,且VPP框架原生无对SRv6 HMAC机制的支持,本文的研究对相应工程领域的研发具有一定的参考意义。

参考文献:

- [1] IETF RFC 8402 Segment routing architecture[S].
- [2] 王君健. SRv6技术探讨[J]. 邮电设计技术, 2020(1): 59-63.
- [3] 张帅, 曹畅, 唐雄燕. 基于SRv6的算力网络技术体系研究[J]. 中兴通讯技术, 2022, 28(1): 11-15.
- [4] 鲁冬杰, 杨凯, 庄小君, 等. 基于SRv6的网络安全技术研究[J]. 电信工程技术与标准化, 2022, 35(12): 27-33.
- [5] 王伟闯. 基于SRv6协议的对称密钥生成与身份认证机制研究[J]. 无线互联科技, 2023, 20(5): 146-150.
- [6] IETF RFC 8200 Internet protocol, version 6 (IPv6) specification[S].
- [7] 杨振东, 陈善杰. 面向安全场景的服务链技术研究和实践[J]. 邮电设计技术, 2023(8): 42-47.
- [8] 杨波, 徐胜超. 基于SRv6服务链的云网专线场景安全防护方法[J]. 计算机与现代化, 2023(8): 107-111.
- [9] 陈广强. 城域网5G业务端到端安全研究和提升[J]. 长江信息通信, 2022, 35(12): 177-179.
- [10] 余启明, 吴爽, 黄帅, 等. 云网融合下的安全能力池关键技术与应用[J]. 中兴通信技术, 2023, 29(1): 20-25.
- [11] 张宇巍, 曾一, 杨燕宁. 基于VPP的虚拟路由器数据平面加速方法[J]. 计算机系统应用, 2017, 26(10): 276-280.
- [12] IETF RFC 8754 IPv6 segment routing header (SRH)[S].
- [13] IETF RFC 2104 HMAC: keyed-hashing for message authentication[S].
- [14] 朱宜斌. 用DPDK和VPP优化5G网络用户面数据报文转发[J]. 数据通信, 2023(4): 43-46.
- [15] 艾雪瑞, 许放, 张涛, 等. 基于HMAC算法的网络通信安全数据传输系统设计[J]. 电子设计工程, 2024, 32(6): 175-179.

作者简介:

汤泳, 高级工程师, 硕士, 主要从事数据通信网络工程咨询设计、SDN系统研发、NFV网元研发等相关工作; 由志远, 高级工程师, 硕士, 主要从事网络软件研发工作; 张珂珂, 高级工程师, 硕士, 主要从事IT系统研发及支撑工作; 高允翔, 高级工程师, 博士, 主要从事网络数智运营研发及技术标准研究工作; 陈亚峰, 高级工程师, 学士, 主要从事数据通信网络工程咨询设计及NFV、SDN相关的研发工作。