5G网络共建共享安全研究

Research on Security of 5G Network Co-Construction and Sharing

谢泽铖，徐　雷，张曼君，葛　然（中国联通研究院，北京 100048）
Xie Zecheng，Xu Lei，Zhang Manjun，Ge Ran（China Unicom Research Institute，Beijing 100048，China）

摘　要：
随着5G网络建设和运营成本的不断增加，5G网络共建共享的必要性和战略意义凸显。目前国内共建共享采用5G MOCN网络架构，使得共建共享双方的移动网络由封闭转向开放，带来了开放性的安全风险。从5G共建共享网络架构出发，分析接入网、承载网、核心网、网管系统等由于共建共享带来的新的安全风险及相应的应对策略，从而保障共建共享场景下双方的网络安全。

关键词：
共建共享；网络架构；安全风险；安全策略
doi：10.12045/j.issn.1007-3043.2021.04.002
文章编号：1007-3043（2021）04-0005-05
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the increasing costs of 5G network construction and operation，the necessity and strategic significance of 5G network co-construction and sharing have gradually become prominent. At present，5G MOCN architecture is adopted in domestic，which makes the mobile network of both parties transform from closed to open，and brings open security risks. It starts from the architecture of 5G co-construction and sharing network，sorts out the new security risks brought by the co-construction and sharing，analyzes corresponding strategy for the access network，bearer network，5G core network，and network management system，so as to guarantee the security of both sides network under the co-construction and sharing scenario.

Keywords：
5G network co-construction and sharing；Network architecture；Security risks；Security strategy

引用格式：谢泽铖，徐雷，张曼君，等. 5G网络共建共享安全研究[J]. 邮电设计技术，2021（4）：5-9.

1 概述

随着5G网络的发展，网络建设投资逐步增加。由于5G单站价格高、站址密集、传输需求大，5G网络的CAPEX巨增。粗略估算，若建设70万个5G基站，投资估算约2 500亿元；若实现全国覆盖，至少需要200万个5G基站，成本将会更高。同时5G网络运营成本压力加大，单个5G有源天线的最大功耗约为1 100 W，未来有望降低至800~1 000 W，但仍远高于现网RRU（约250 W），能耗巨大。此外，5G AAU与现网2G/3G/4G无源天线需相互独立部署，天面空间更加紧张。整体来看，相同基站规模下，5G网络的OPEX也将数倍于4G网络。

因此，以扩覆盖、降成本、一张网为目标，开展5G网络共建共享，降本增效，提升资产运营效率，是大势所趋，国内外均开展了网络共建共享的多种尝试。例如，中国联通与中国电信于2019年签署《5G网络共建共享框架合作协议书》，双方划定区域，分区建设，各自负责在划定区域内的5G网络建设相关工作，谁建设、谁投资、谁维护、谁承担网络运营成本。中国移动

收稿日期：2021-02-20

与中国广电于2021年订立有关5G共建共享的具体合作协议，双方共同建设700 MHz无线网络，中国移动向中国广电有偿共享2.6 GHz网络。欧洲沃达丰将网络共享作为其整体策略，英国、西班牙、意大利、澳大利亚均在实施，共享方式也基本采用在大城市独立建设以保持网络建设和业务的独立性，在非核心区域采取网络共享，以节省成本。2020年3月，诺基亚携手Telenor和Telia在丹麦完成了5G MOCN功能的部署。

采用共建共享方式建设5G网络，可以大大节省投资成本，实现带宽翻倍、速率翻倍、覆盖翻倍。但是共建共享使得双方的移动网络由封闭转向开放，带来了开放性的安全风险。在目前共建共享条件下，存在多种边界场景，例如跨运营商场景、共享与非共享场景，客观上也使得共建共享面临诸多安全挑战。本文将从5G共建共享网络架构出发，分析接入网、承载网、核心网、网管系统等由于共建共享带来的新的安全风险及相应的应对策略，从而保障共建共享场景下双方的网络安全。

2 共建共享网络架构

根据共享方式和共享程度的不同，网络共享网络架构一般分为以下4种：站址共享、MORAN（Multi-Operator Radio Access Network）、MOCN（Multi-Operator Core Network）和GWCN（Gateway Core Network）。

a）站址共享：运营商之间只共享物理站址，包括：机房、铁塔、电源、天馈系统等。由于站址投资较大，此种方式可对站址资源共享，减少重复投资，例如中国铁塔公司负责站址基础设施的建设，由其提供给国内的运营商使用（见图1）。

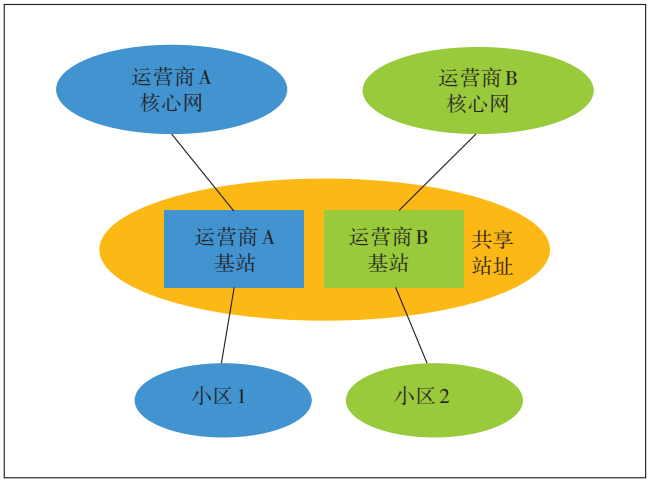

图1　站址共享示意图

b）MORAN：即分载频共享模式，仅共享基带单元和射频单元，频率资源、RRM和服务部署独立。此种共享方式在站址共享的基础上将无线接入网的主设备（即基站设备）也进行共享，不同运营商在各自所属载频上广播各自的PLMN。此种模式下，承建方和共享方共享站点的基础设施或网络设备，但是每个运营商拥有其独立的小区，这些独立的小区称为分载频共享小区，每个分载频共享小区归属于一个运营商，组网示意如图2所示。此共享方式只共享基站内部与无线接入资源无关的模块，而小区和频点不共享。对手机来说，与基站不共享是一样的，各个运营商的小区和频点独立，手机接入自己的签约网络。所以，MORAN的实现比较简单，共享不够彻底。

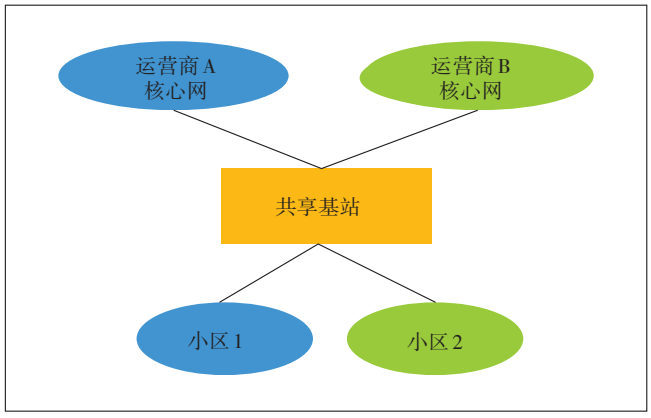

图2　MORAN组网示意图

c）MOCN：即共载频共享模式，共享基带单元和射频单元，共享频率资源，共享RRM，统一服务部署。此种共享方式在MORAN只共享基站硬件的基础上，基站内部和无线接入资源相关的最关键模块，即小区和频点也进行共享，需要在相同的载频上同时广播不同运营商的PLMN。此种模式下，承建方和共享方共享站点的基础设施或网络设备，并且也共享小区载波，这些共享的小区称为共载频共享小区，每个共载频共享小区同时归属于共建共享的双方。组网示意如图3所示，小区同时广播承建方与共享方运营商的PLMN网络号，手机按自己服务网络的PLMN接入。由于涉及同一基站内部的资源分配，因此此种共享方式比较复杂，但是共享更为深入，对于拓展用户覆盖及共享效果更为有益（见图3）。

d）GWCN，即共享RAN和部分核心网，此种共享方式在MOCN的基础上，共享部分核心网元，共享程度进一步加深。但是由于核心网侧存储着大量运营

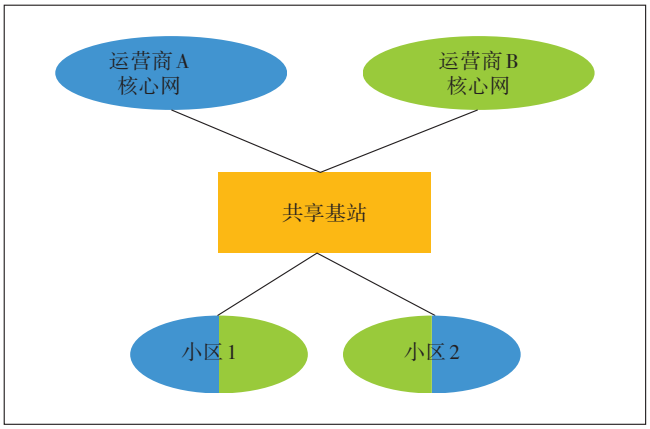

图3　MOCN组网示意图

商专有数据及用户数据，会增加运营商管理的复杂程度，同时核心网共享会带来大量网络改造和维护工作，投入产出比降低（见图4）。

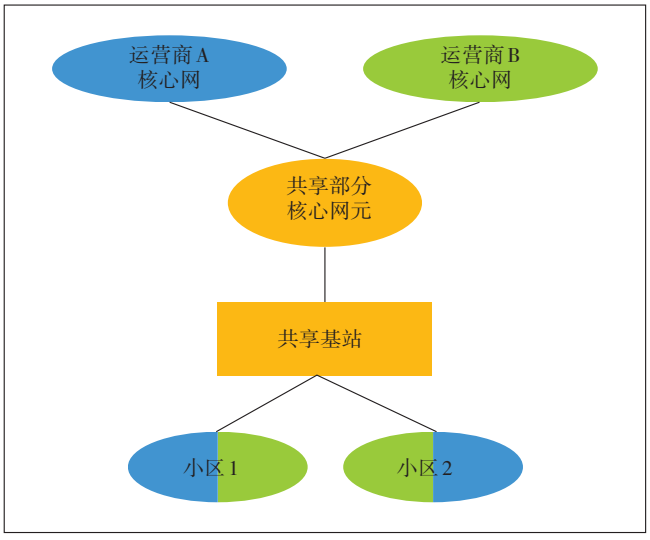

图4　GWCN组网示意图

站址共享、MORAN、MOCN和GWCN这几种网络共享方式的共享程度依次加深，涉及到容量和性能的规划、参数的修改等问题，共享难度依次加大。

目前，中国电信与中国联通5G网络共建共享采用5G MOCN共享网络架构，无线基站共建共享，核心网独立建设，多个运营商的5G核心网连接到同一个NG-RAN，共享无线接入网络，共享无线资源。

3 共建共享安全风险

共建共享双方共用的基站（不论是NSA模式还是SA模式）都通过承载网的互联链路实现互通，使双方的移动网络由封闭转向开放，带来了开放性的安全风险。在目前共建共享条件下，存在多种边界场景，例如跨运营商场景、共享与非共享场景，客观上也使得共建共享面临诸多安全挑战。由于5G网络安全涉及内容比较多，本文主要分析5G网络共建共享对接入网、承载网、核心网、网管系统等带来的影响及新的安全风险和安全需求（见图5）。

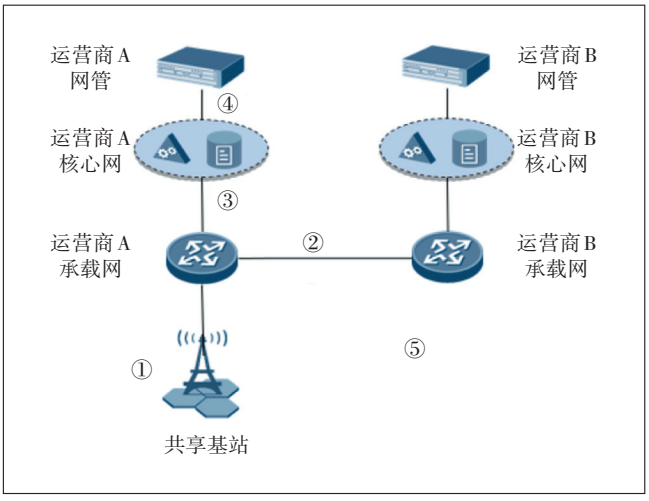

图5　共建共享安全风险示意图

3.1 接入网安全风险

MOCN模式下的共建共享，双方共享无线基站，承建方运营商的基站需要与双方的核心网相连，共享基站带来的互联互通加大了基站对外暴露的可能性，需要双方制定切实可行的措施来保障基站的系统安全、物理安全。若双方的基站的安全加固不一致、不到位，当一方基站出现安全问题时，也会影响到对方的网络。5G基站通过N2、N3接口与核心网相连，通过Xn口与其他基站相连。当基站共享后，共享基站与其他网元（如UPF、AMF、其他基站）的回传接口发生流量窃听、重放攻击的可能性加大。

3.2 承载网安全风险

共建共享双方的承载网互通是共建共享实现的基础，承载能否满足网络要求，将直接影响5G的网络质量。而承载网互通加大了与异网运营商的暴露面，对互通节点的路由设备和组件提出了更高的安全要求。

例如互联端口故障可能会引发链路异常进而导致承载的基站无法正常运行；与业务无关的、不合规的外部流量通过攻击互通节点，并以此作为跳板来实施跨网攻击；路由设备与组件漏洞可能被攻击者利用，进而对设备实施网络攻击或入侵，导致设备系统

资源的可用性下降、路由信息泄露，或者异常流量造成网络拥塞；共享互通的承载网络将面临成倍的大流量冲击，容易出现路由过载、负载不均衡的情况，导致路由节点、传输设备性能下降，路由拥塞或不可用等风险。

3.3 核心网安全风险

5G核心网采用控制转发分离架构，实现了移动性管理和会话管理的独立进行；同时存储用户的注册信息，对用户进行接入认证和移动性管理、会话管理、策略控制等。5G核心网是5G网络的大脑，负责对整个网络进行管理和控制，需要重点进行防护。传统模式下5G核心网连接自己的基站，安全性较高，而共建共享后核心网连接承建方的基站，增加了以承建方基站或者承建方承载网为跳板攻击5G核心网络的风险。需要关注由于基站共享对AMF、UPF网元带来的攻击以及5G核心网与共享基站之间回传链路的通信安全风险。

3.4 网管安全风险

为满足共享方对共享基站的访问需求，满足共建共享双方对网络的运营管理需求，可以通过反拉终端和双北向接口开放2种方式，向共享方开放网管能力。网管开放使得共建共享双方的网管互通，带来双方网管域边界隔离的安全风险和双方网管的运营维护流量传输时被窃取篡改的安全风险；增加了网管账号的开通及账号权限的分配、账号的管理的难度；同时带来非授权访问、越权访问对方网管系统的安全风险。

3.5 安全管理风险

共建共享采用双方联合运营方式管理网络，改变了传统网络各自运营的方式，若双方安全制度不完善、对接流程不清晰、安全要求不一致，当突发安全事件时可能会导致安全事件响应不及时、操作联动效率低、处置不到位的安全风险。

4 共建共享安全策略分析

共建共享涉及承建方和共享方2个主体，双方应遵循公平、公正、对等的原则，保证双方对于网络的内部操作不影响对方网络，同时双方应共同采取安全措施，保障共建共享网络的设备安全以及5G网络的共建共享持续健康运行。结合第3章分析的共建共享带来的新的安全风险，本章将从接入网、承载网、核心网、网管以及安全管理5个方面，分析共建共享场景下，应重点关注的问题及应对策略。

4.1 接入网安全策略分析

5G MOCN网络共享架构下，主要共享接入基站，因此共建共享双方应关注共享的基站网元以及共享基站与核心网络之间回传链路的安全，需要双方采取安全措施确保共享基站的安全，且安全加固要求一致。例如加强gNB与eNB/gNB的Xn接口链路以及gNB与5GC间的N2、N3等回传通信接口的安全防护，按需通过IPSec进行双向认证和加密，提升网络可靠性；从账户加固、网络加固、系统加固、日志审计、物理安全等方面对共享基站网元进行安全加固，同时双方的安全加固要求保持一致；通过建立补丁管理与更新流程、安全基线配置核查机制、新增安全防护措施等方法强化网元安全性；通过持续监测网络负载和资源、信令优化、拥塞接入控制、容灾备份与负载均衡，应对可能发生的信令风暴和流量攻击，保障接入网络的可靠性与可用性。

4.2 承载网安全策略分析

5G共建共享主要在承载网实现互联互通，根据各运营商承载网资源分布的差异，按需共享部分承载网路由。共建共享双方应加强对互通对接点的安全防护，防止业务不相关的流量未经授权访问己端网络，确保网络的安全可靠。例如，在互通对接点采用双节点口字型互联加强承载网络健壮性；通过建设不同的VPN网络、开启不同的FlexE切片等方式在承载网内提供不同运营商业务流量间的安全隔离；承载网互通节点的路由设备配置严格的访问控制策略，通过BGP路由控制与过滤、ACL访问安全策略等，强化路由的访问安全，防止泄露敏感路由信息；在承载网设备的管理平面、控制平面、转发平面，部署一定的安全策略进行安全管控，防止业务不相关的流量未经授权访问承载网，防范承载网可能遭受的攻击。

4.3 核心网安全策略分析

基站共享会导致5G核心网连接其他运营商的共享基站，5G核心网要关注与共享基站对接的AMF、UPF等核心网网元的安全防护，防止由于基站共享引起的未知接入源带来的安全风险以及承载网互通可能引发的潜在跨网攻击威胁。例如，对5G核心网中与基站对接的AMF、UPF网元，通过路由过滤策略、ACL访问策略等安全措施，防范异常流量访问核心网；共享基站与5GC之间的回传链路（N2、N3接口）按需开启IPSec，以保证通信数据不被非法篡改。

4.4 网管安全策略分析

由于共享方对于共享基站的运行情况有一定需求，从网络运营的角度考虑，共建共享双方一般通过反拉终端或开放北向接口等2种方式开放无线网管能力。其中反拉终端方式是指通过部署专线的方式将承建方OMC网管终端反拉至共享方，实现5G网管能力开放。开放北向接口方式是指承建方通过新增开放北向接口的方式，按照共享方的北向接口规范，将共享网络的配置、性能、告警等多类数据上报至共享方。

双方应加强开放能力的OMC网管的安全管理，做好网管设备、接口、终端的安全域划分，明晰安全域边界，落实各边界接入要求及安全策略。例如在网管域外部边界部署双防火墙，对安全域边界进行安全隔离，一主一备预防单点故障，并实现负载均衡；在安全域边界的防火墙上设置访问控制规则，共享方接入只能访问共享的5G网管，承建方其他网内设备共享方均不可达；根据“工作相关化和权限最小化”原则，做好无线网管分权分域的访问控制策略，基于承建方、共享方的角色管理网管账号的访问控制权限，承建方网管账号具备网管配置、操作权限，共享方网管账号仅有只读权限；同时所有网管的操作维护流量通过采取传输链路隔离、加密、容量保障等安全手段加强保护，以避免在传输过程中被篡改或泄露。

4.5 安全管理策略分析

共建共享采用双方联合运营方式管理网络，改变了传统网络各自运营的方式，对于双方的安全协作要求较高，需要具备安全事件联合处置能力。因此，需要共建共享的双方共同制定快速有效的安全协作与响应机制、安全事件处理流程等，明确各种场景下的安全职责，确保安全攻击、安全漏洞等事件信息能够及时传递共享，能够及时快速联合处置安全事件；同时能够对安全事件通告、安全事件分析、安全事件处理等进行记录，为后续审计工作提供数据，从而最大程度上保障网络安全稳定，提高协同效率。

5 结束语

5G网络共建共享，可以达到低成本高效建设5G网络的目标，是5G网络部署运营的新趋势，其必要性和战略意义逐渐凸显。共建共享过程中承建方和共享方需共同开展联合攻关，注重研究、实践和总结多种共建共享场景下的安全风险和应对策略，建立常态化的联合优化机制，确保网络健康稳定运行。后续随着共建共享合作及研究的不断加深，可在安全事件感知及告警、共享数据安全、MEC/切片等新技术新业务，在共建共享下的安全增强等层面拓宽共建共享的安全研究范围，不断探索共建共享安全合作的新模式。

参考文献：

[1] System architecture for the 5G system：3GPP TS 23.501[S/OL]. [2021-01-08]. https://www.3gpp.org/specifications/specifications.
[2] Security architecture and procedures for 5G system：3GPP TS 33.501 [S/OL]. [2021-01-08]. https://www.3gpp.org/specifications/specifications.
[3] Study on the security aspects of the next generation system：3GPP TR 33.899[S/OL]. [2021-01-08]. https://www.3gpp.org/specifications/specifications.
[4] 赵文，罗敏，田永春，等. 5G安全技术研究[J]. 通信技术，2020，53(8)：2045-2048.
[5] 曹广山，马丹，宋玉利，等. 5G共建共享基础资源择优方案探讨[J]. 邮电设计技术，2021(2)：1-5.
[6] 周滟. 5G NSA共建共享方案及边界优化策略[J]. 电子世界，2021(1)：11-12.
[7] 薛金明，赵良，张贺，等. 5G共建共享下的承载网互通链路智能预警分析和应用[J]. 通信世界，2021(1)：36-38.
[8] 佟巍，杨书宽. SA模式下5G网络共建共享技术方案研究[J]. 信息通信，2020(12)：213-215.
[9] 刘映，吴坚，彭江怀，等. 5G NSA共建共享方案实践[J]. 邮电设计技术，2020(12)：22-27.
[10] 王功朝. 电联5G网络共建共享方案[J]. 电子技术与软件工程，2020(22)：1-2.
[11] 潘磊. 浅析5G NSA网络共享模式[J]. 信息技术与信息化，2020(10)：163-165.
[12] 毕晓宇. 5G移动通信系统的安全研究[J]. 信息安全研究，2020，6(1)：52-61.
[13] 冯登国，徐静，兰晓. 5G移动通信网络安全研究[J]. 软件学报，2018，29(6)：303-315.
[14] 马宇翔. 5G无线通信系统网络安全问题的分析与探究[J]. 中国新通信，2021，23(1)：159-160.
[15] 常鹤，张强. 浅谈5G网络电联共建共享方案[J]. 中国新通信，2020，22(18)：12-13.
[16] 张志荣，李志军，陈建刚，等. 5G网络共建共享技术研究[J]. 电子技术应用，2020，502(4)：7-11.
[17] 马培勇，杨广铭，梁筱斌，等. 5G承载共建共享实践[J]. 信息通信技术与政策，2020，311(5)：21-27.

作者简介：
谢泽铖，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，教授级高级工程师，博士，主要从事网络与信息安全研究工作；张曼君，高级工程师，博士，主要从事网络与信息安全研究工作；葛然，高级工程师，主要从事网络与信息安全研究工作。