BGP路由劫持检测与处置探讨

Discussion on Detection and Handling of BGP Route Hijacking

张笑颜[1]，杨艳松[2]，袁姝婕[3]，梁晓晨[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033；3. 中国铁塔股份有限公司浙江分公司，杭州 310000）

Zhang Xiaoyan[1], Yang Yansong[2], Yuan Shujie[3], Liang Xiaochen[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China; 3. China Tower Co., Ltd. Zhejiang Branch, Hangzhou 310000, China）

摘　要：

随着互联网规模的不断扩大和复杂性的增加，域间路由协议（BGP）作为互联网通信的核心组件，其稳定性和安全性变得尤为重要。基于此，提出了BGP路由劫持检测与处置的设想，通过BGP路由异常检测与处置，提升网络安全和稳定性。

关键词：

边界网关协议；域间路由；路由异常；路由安全；实时检测

doi：10.12045/j.issn.1007-3043.2025.08.013

文章编号：1007-3043（2025）08-0064-05

中图分类号：TN915

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract:

With the increasing scale and complexity of the Internet, as the core component of Internet communication, the stability and security of BGP become particularly important. On this basis, it proposes the idea of BGP route hijacking detection and handling, which enhances network security and stability through BGP route anomaly detection and handling.

Keywords:

Border gateway protocol; Inter-AS routing; Routing abnormality; Routing security; Real-time detection

引用格式：张笑颜，杨艳松，袁姝婕，等. BGP路由劫持检测与处置探讨[J]. 邮电设计技术，2025(8)：64-68.

0 引言

随着互联网的快速发展，网络攻击手段也在不断升级。边界网关协议（Border Gateway Protocol，BGP）劫持作为一种高级的网络攻击手段，其隐蔽性和危害性都相对较高。为了应对这一挑战，各个运营商或者机构都在加强BGP路由劫持的检测与处置工作。

BGP是互联网的核心路由协议，它负责在不同的自治系统（AS）之间交换路由信息，以确保数据包能够高效地从源地址传输到目的地址[1]。然而，当AS错误地宣布它们不控制的IP前缀时，就会发生BGP劫持。这种公告可能会被路由到互联网的其他路由器，导致流量错误地走向指定的AS，从而造成严重的网络安全问题。BGP劫持可能导致互联网流量出错、被监控或拦截，甚至被引导到虚假网站。这不仅会导致用户数据泄露，还会增加页面加载时间，降低用户体验。此外，垃圾邮件发送者还可以利用BGP劫持来欺骗合法IP进行垃圾邮件的发送等。因此，BGP路由劫持检测与处置尤为重要。

1 常见路由劫持异常分析

BGP路由劫持，又被称为路由注入，是指攻击者伪

收稿日期：2025-07-03

造自己的路由信息，将其发布到互联网中，从而使数据流量重定向到攻击者控制的网络中，以达到窃取客户的敏感信息数据的目的[2]。这种攻击通常会导致网络故障、服务中断和数据泄露，也存在流量侦听、中间人攻击和仿冒攻击等安全风险。

BGP路由劫持主要是攻击者通过篡改路由条目信息，使路由原有的方向发生偏离。BGP路由劫持主要有IP前缀劫持、AS路径篡改和路由数据泄露[3]。

1.1 IP前缀劫持

IP前缀劫持示意如图1所示。攻击者通常针对用户访问路径中的中间网络设备发起攻击，通过篡改设备中的IP前缀列表，破坏原有路由指引规则，导致用户访问流量的目的地指向发生变更。此过程会直接篡改用户的正常访问路径，使数据无法按预期送达目标节点，最终造成用户无法通过原路由访问目标服务[4]。

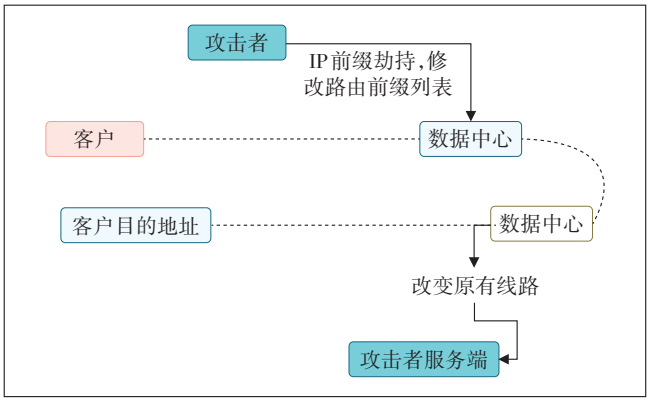

图1　IP前缀劫持示意

1.2 AS路径篡改

AS路径篡改攻击示意如图2所示。攻击者核心手段为篡改用户访问目标节点的AS路径，通过破坏原有的AS级路由转发规则，强制改变用户访问流量的

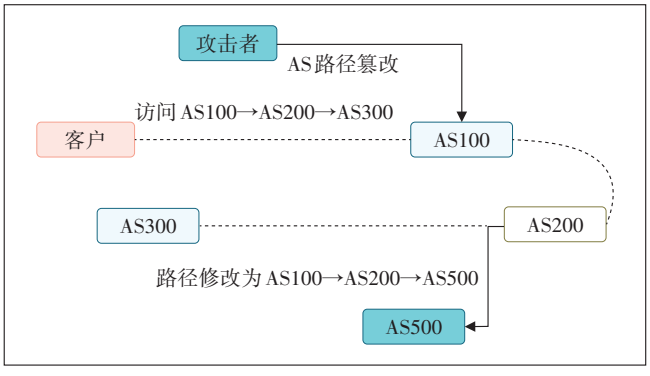

图2　AS路径篡改示意

AS传输路径，进而引发用户网络路径被篡改。该攻击可能直接导致用户网络访问目标节点不可达的故障，最终给用户造成业务或数据层面的损失[5]。

1.3 路由数据泄露

数据泄露通常是由于运维人员错误配置BGP参数导致的。以图3为例，将原本应宣告到AS300的路由错误地宣布到AS500自治系统内，使运营商的数据泄露给AS500自治系统[6]。数据泄露带来的危害涉及多个层面，比如个人隐私问题、公司商业机密曝光、遭受敲诈勒索等等。

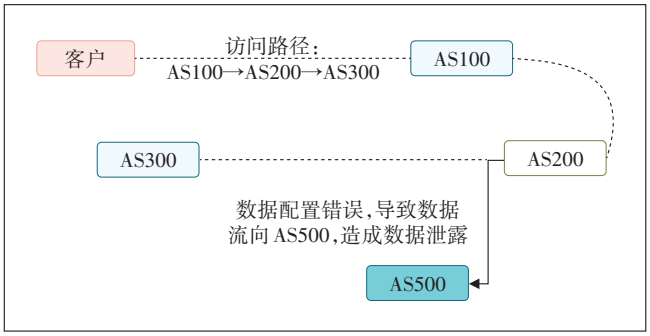

图3　路由数据泄露示意

2 BGP路由检测与处置

2.1 BGP路由发布原则

AS间一般分为Provider、Customer和Peer 3种关系。Provider为路由提供方，一般为路由的上游；Customer为路由接收方，一般为路由的下游；Peer为对等体[7]。各种角色之间遵循的BGP路由发布基本规则如下。

a）允许向Customer发送所有路由。

b）允许向Peer发送Customer和本自治系统始发的路由。

c）允许向Provider发送Customer和本自治系统始发的路由。

违反以上路由发布规则的，则判定为路由异常，需要及时发现并制止，以保障网络路由安全可信。

2.2 路由基准库构建

通过采集国内外路由标准库，构建路由检测基准库，具体如图4所示。

a）多维可信路由库。多维可信路由库通过获取ROA、IRR、地理位置、地址分配等多维信息，构建互联网路由信息库。

b）ROA路由起源认证信息库。ROA（route origin

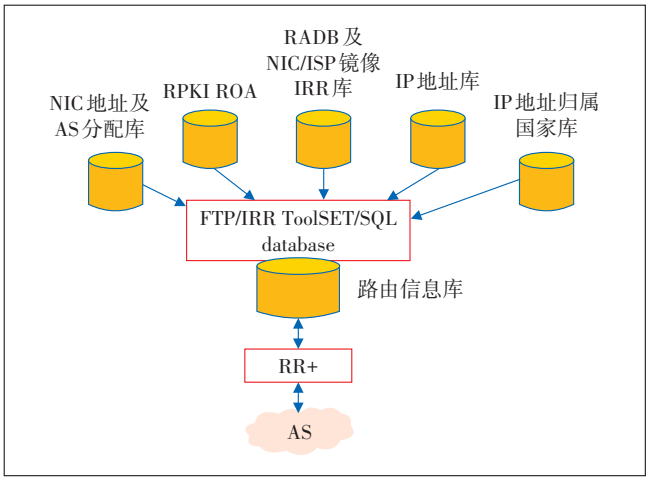

图4 路由基准库构建示意

authoriztion）路由起源认证信息库是指基于PKI公钥体系建立具有数字签名的ROA信息库，以确保数据安全可信。ROA路由起源认证信息库用于IP路由前缀Prefix与AS号的对应关系认证，注册信息包括IP前缀、归属AS号、最大掩码位数，以验证ROA路由起源信息的可信性。

c）互联网路由注册IRR信息库。互联网路由注册IRR信息库包括RADB及各大NIC/ISP的互联网路由注册数据库。其中，IRR主要包含AS、AS-SET、route/route6等object对象的路由注册信息，AS对象包括AS号与归属团体信息、AS-SET对象包括AS成员关系，route/route6对象显示了IPv4/IPv6 Prefix与ASN号之间的对应关系。

d）NIC地址及AS分配库。NIC地址及AS分配库是指建立地址分配组织已分配的IP地址及AS号码库，用于判定bogon路由。

2.3 路由劫持检测

通过与设备建立BGP邻居，实时接收更新消息，并通过与路由基准库进行比对分析，完成bogon异常检测、ROA异常检测、IRR异常检测，实现路由劫持异常的实时感知分析，保障网络路由可信。

路由劫持异常检测的整体流程如下（见图5）。

a）实时接收路由的变化消息，提取路由变化消息中prefix、peeras、originas、aspath等相关信息。

b）系统进行bogon异常检测，包含bogon as、bogon prefix检测。如果存在bogon异常，则此条路由记录为bogon异常，检测流程结束。

c）如果bogon检测不存在异常，则进行ROA检测。基于ROA库进行异常检测，如果存在异常，则此

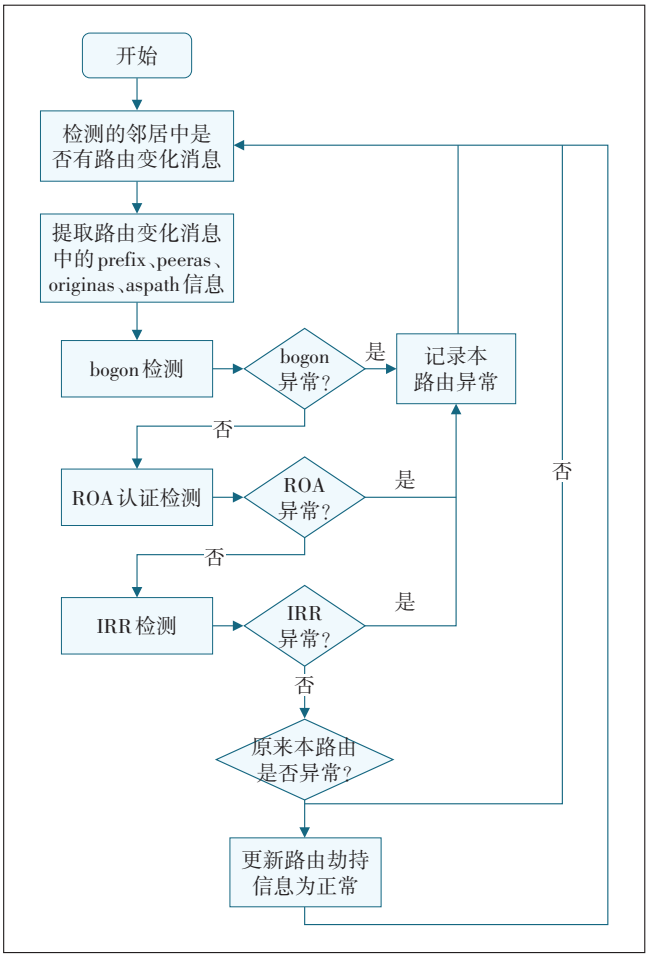

图5 路由劫持检测整体流程

条路由记录为ROA异常，检测流程结束。

d）如果ROA异常检测不存在异常，则进行IRR检测。基于IRR库进行异常检测，如果存在异常，则此条路由记录为IRR异常，检测流量结束。

e）如果IRR异常检测不存在异常，则核查此路由是否存在异常。如果存在异常，则将现有路由劫持更正常。

f）整条路由检测异常检测结束，新的路由变化消息按照现有当前流程进行检测。

下面对bogon异常检测、ROA异常检测、IRR异常检测3种检测方式进行展开说明。

2.3.1 bogon异常检测

bogon异常检测流程如下（见图6）。

a）基于系统接收的路由变化消息，通过与路由基准库的比对，判断此路由地址段是否在分配的地址范围内。如果不在地址分配范围，则记录为地址未分配异常。

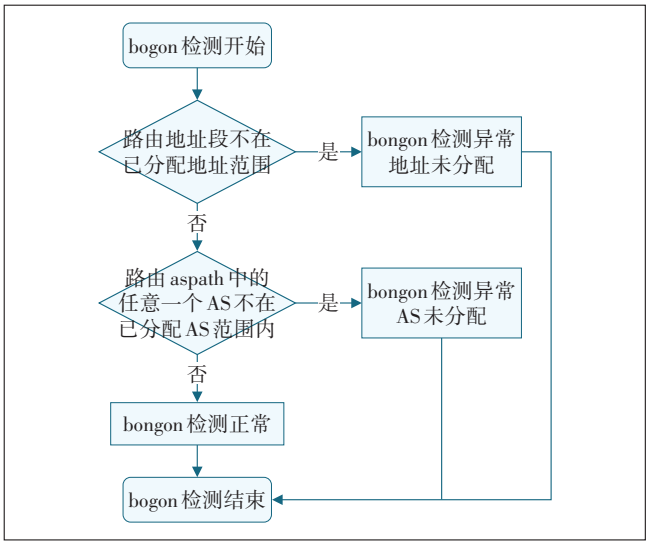

图6　bogon异常检测流程

b）地址段分配检测正常，则对应进行AS分配检测。如果对应AS不在AS分配范围，则记录为AS未分配异常。

c）AS分配检测正常，则流程结束，进入后续检测流程。

2.3.2 ROA异常检测

ROA异常检测流程如下（见图7）。

a）基于系统接收的路由变化消息，bogon检测正常后，进入ROA检测流程。

b）此路由在ROA中不存在匹配记录，则认为检测正常，流程结束。

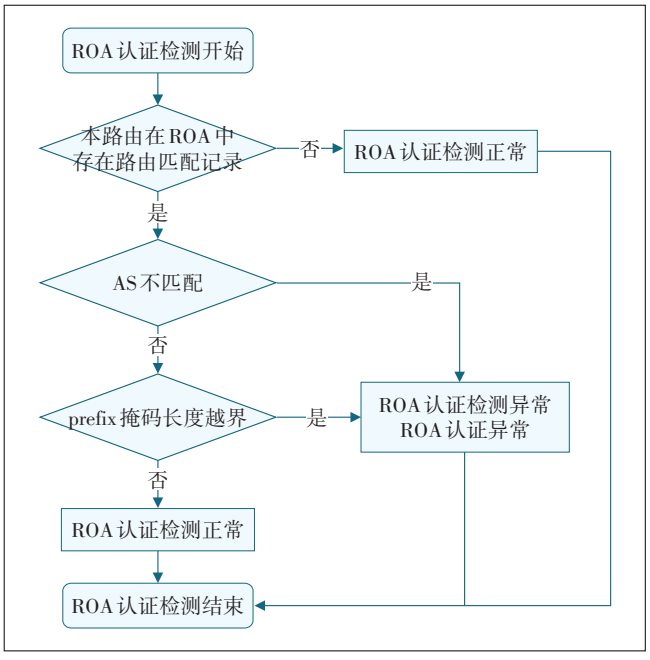

图7　ROA异常检测流程

c）此路由在ROA存在匹配记录，如果对应路由域ROA库AS不匹配，则认为异常。

d）此路由在ROA存在匹配记录，同时对应路由域ROA库AS匹配，则核查prefix长度是否越界，如果越界，则认为异常。

2.3.3 IRR异常检测

IRR异常检测流程如下（见图8）。

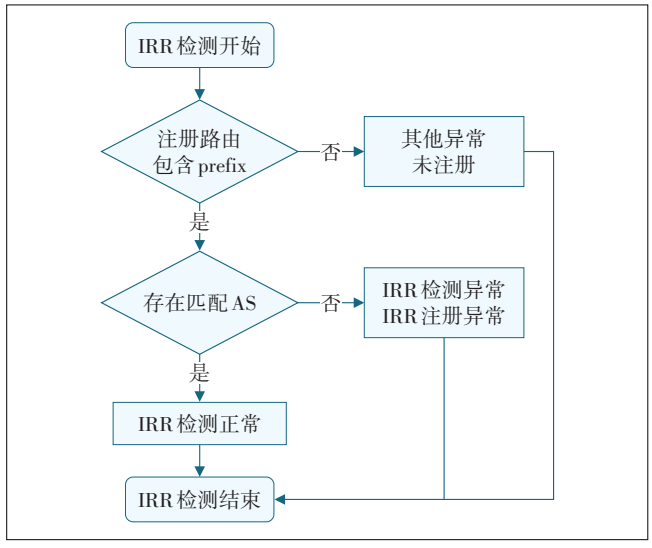

图8　IRR异常检测流程

a）基于系统接收的路由变化消息，ROA检测正常后，进入IRR检测流程。

b）注册路由是否包含此prefix，如果不包含则归为注册异常。

c）若注册路由包含此prefix，查看对应此路由AS是否能匹配，如果不匹配则认为检测异常。

d）检测正常后流程结束。

2.4 路由劫持处置

路由劫持处置流程如图9所示。

a）收到劫持封堵协同处置信息，或系统自己检测到劫持信息。

b）针对外部系统下发劫持处置信息进行判断，本网是否收到此劫持路由。

c）系统进行劫持信息、系统自身检测信息展示。

d）系统通过人工或自动进行下发劫持封堵操作。

e）判断劫持处置信息数据源系统，外部系统下发处置指令或者系统检测异常数据。

f）基于需要封堵的prefix+orgin as核查系统是否收到此路由（封堵完成继续进行监测）。

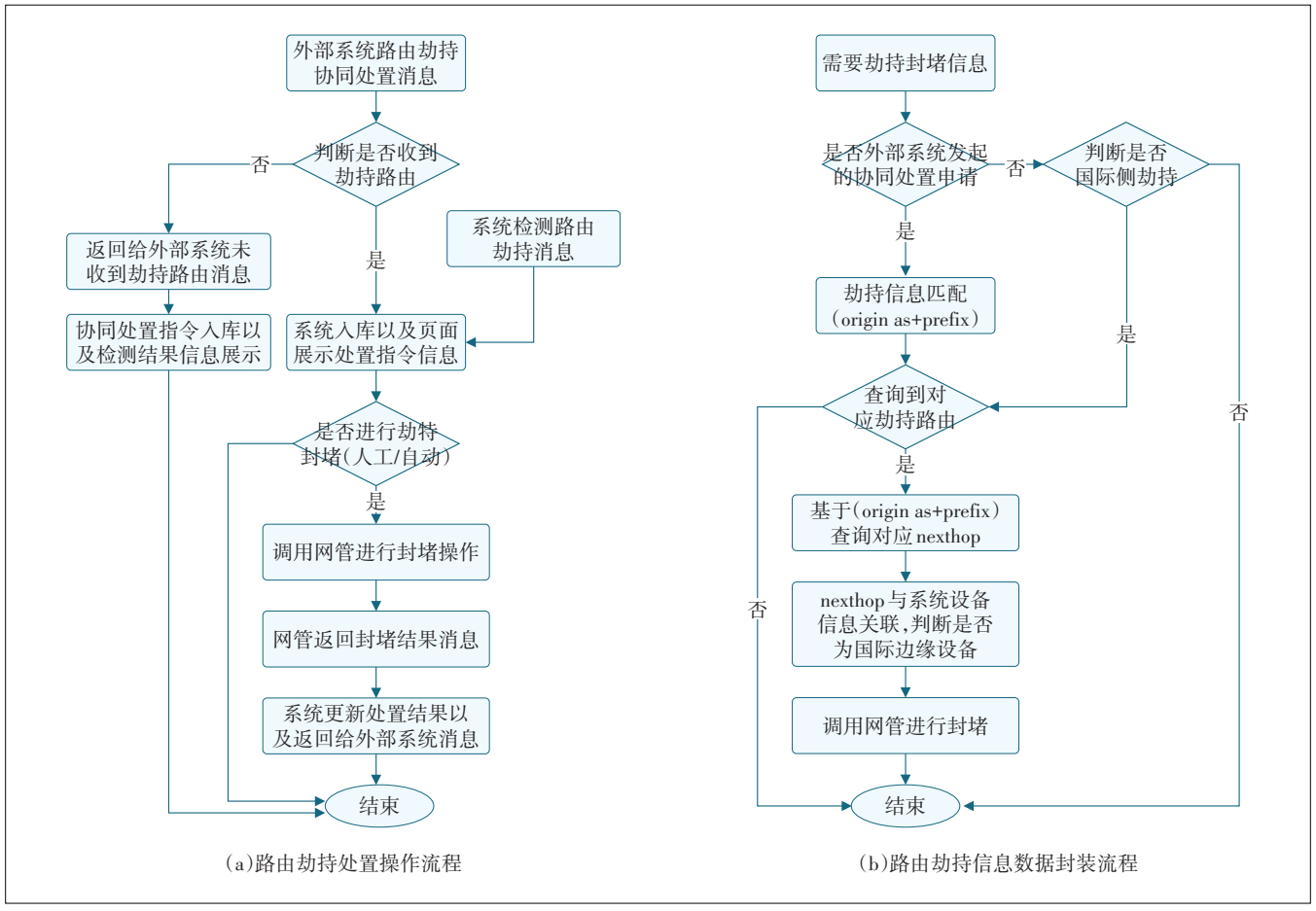

图9　路由劫持处置流程

g）基于prefix+orgin as查询对应peer as +nexthop，基于nexthop判断是否是国际设备。

h）调用能力进行封堵操作，记录封堵记录信息。

i）识别封堵结果，回填封堵结果消息。

j）系统记录处置结果信息。

3 总结

根据设想，可基于BGP协议实现路由实时采集全量路由表与路由更新数据，通过标准库路由信息数据构建了路由检测基准库，可实时检测路由劫持异常事件信息。通过对异常检测的处置，能够有效地遏制部分路由安全事件的发生，降低网络路由安全风险，保障网络的安全可信，为互联网治理和互联网安全提供坚强的护盾。

参考文献：

[1] 陈侃. 域间路由协同监测技术的研究与实现[D]. 长沙：国防科学技术大学，2009.
[2] 邱菡，李玉峰，兰巨龙，等. 域间路由系统的级联失效攻击及检测研究[J]. 中国科学（信息科学），2017，47(12)：1715-1729.
[3] 刘欣. 互联网域间路由安全监测技术研究[D]. 长沙：国防科学技术大学，2008.
[4] 赵鹏. 国家级互联网域间路由安全监测系统的设计与优化[D]. 长沙：国防科学技术大学，2010.
[5] 郑皓，陈石，梁友. 关于“数字大炮”网络攻击方式及其防御措施的探讨[J]. 计算机研究与发展，2012(S2)：69-73.
[6] 王小强，朱培栋，卢锡城. 防范路由劫持的协同监测方法[J]. 软件学报，2014，25(3)：642-661.
[7] 邹慧，马迪，邵晴，等. 互联网码号资源公钥基础设施（RPKI）研究综述[J]. 计算机学报，2022，45(5)：1100-1132.

作者简介：
张笑颜，毕业于悉尼大学，助理工程师，主要从事智能云网相关专业规划、研发、技术创新等工作；杨艳松，毕业于西安邮电学院，高级工程师，主要从事智慧云网相关产品及系统研发工作；袁姝婕，毕业于日本梅花女子大学，助理工程师，主要研究方向为5G通信基础设施通信塔、室内分布系统和无线综合解决方案及技术演进、通信网络工程建设规划、通信工程建设项目管理、客户服务能力建设等；梁晓晨，毕业于北京邮电大学，高级工程师，主要从事智能云网相关专业规划、研发、技术创新等工作。