语音中继业务安全运营解决方案与关键技术浅析

Security Operation Solutions and Analysis of Key Technologies for Telephone Trunk Service

赵晨斌[1]，符　刚[2]，陈浩然[2]（1. 中国联合网络通信集团有限公司，北京，100033；2. 中讯邮电咨询设计院有限公司，北京 100048）

Zhao Chenbin[1]，Fu Gang[2]，Chen Haoran[2]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：

描述了语音业务涉诈涉扰现状和科学管控的需求痛点。介绍了固网语音中继业务安全的解决方案，详细阐述了固网语音中继信令拦截技术、基于大数据的异常呼叫行为分析、基于AI语义理解的涉诈内容分析等三大关键技术。最后，对语音中继业务的安全前景进行了展望。

关键词：

语音中继；信令拦截；异常呼叫行为；意图识别

doi：10.12045/j.issn.1007-3043.2024.11.011

文章编号：1007-3043（2024）11-0063-07

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：

It describes the current situation of fraud and nuisance call，the sore points of scientific management and control of telephone services. Then it explains the solving schemes for the security of telephone trunk services. Itelaborates on three key technologies：telephone trunk signaling interception technology，abnormal call behavior analysis based on big data，and fraud content analysis based on AI semantic understanding. Finally，the security prospects of telephone trunk services are discussed.

Keywords：

Telephone trunk；Signaling interception；Abnormal calling behavior；AI intention recognition

引用格式：赵晨斌，符刚，陈浩然. 语音中继业务安全运营解决方案与关键技术浅析[J]. 邮电设计技术，2024（11）：63-69.

0 前言

近些年来，电信网络诈骗问题日益突显，严重影响社会秩序，损害人民群众利益，是当前发案量最高、损失最大、人民反应最强烈的犯罪行为之一[1]。同时，因其参与主体多、产业链条长、技术对抗强、打击难度大，是一项系统复杂的社会治理难题[2]。诈骗电话作为整个诈骗流程的起始及引流环节，是源头治理的关键一环。同时，非应邀商业电话作为违背用户意愿的有害行为，与以人民为中心、高质量发展的理念背道而驰，需统筹考虑，以系统观念综合治理。除移动网异常电话卡治理外，固定网语音业务涉诈涉扰问题日趋严峻，运营商语音通信资源被非法利用、违规滥用的风险日益突出，固网语音业务安全运营成为运营商联网通信业务发展面临的新挑战。

收稿日期：2024-09-05

1 语音中继业务安全现状痛点

1.1 当前现状

电话、短信等联网通信业务是助推数字经济发展的必备基础能力，强触达、低成本、广连接的基础通信业务是促进市场繁荣发展、推动数字经济和实体经济融合发展的重要利器，尤其是在政府公众服务、商业

营销推广、企业客户服务、企业数字化转型方面释放其巨大的助推能量。但在基础语音业务高速发展的同时，政企固话、语音专线的涉案问题、骚扰投诉问题出现抬头，2023年酒店固话涉案成为典型案例，线路资源转租转售现象时有发生。在不断增加的考核压力与缺乏有效管控技术手段的条件下，运营商选择暂缓发展固网语音业务，亟需科学的技术手段精准施策，以有效的业务安全治理举措突破语音业务发展障碍。

1.2 主管部门要求

语音中继主要业务形式是提供政企单位固话及语音呼叫服务，为了规范语音呼叫服务行为，维护用户的合法权益，促进语音呼叫服务市场的健康发展，工业和信息化部根据《中华人民共和国反电信网络诈骗法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国电信条例》等相关法律法规制定并颁布了一系列管理规定。《通信短信息和语音呼叫服务管理规定（工业和信息化部令第31号）》中对信令与录音数据留存以及研判分析做了要求，要求基础电信业务经营者以及语音呼叫服务提供者应当在其服务系统中记录语音呼叫的发送端和接收端电话号码以及平台类电话录音。信令数据至少保存1个月，上述信息除信令数据外至少保存5个月。基础电信业务经营者应当建立预警监测、大数据研判等机制，通过合同约定和技术手段等措施，防范未经用户同意或者请求发送的商业性短信息或拨打的商业性电话。

《工业和信息化部关于加强呼叫中心业务管理的通知（工信部信管〔2020〕81号）》中对经营行为提出了管理要求。呼叫中心业务经营者确因用户同意的即时回访或信息咨询等实施呼出的，应当留存不少于30日的通话录音、相应的主被叫号码和拨打时间、用户同意的相关凭证等信息，并要求建立健全技术防范手段禁止客户使用呼叫中心系统违规拨打骚扰电话。

1.3 需求痛点

前期调研显示，语音中继业务安全发展的主要痛点如下。

a）基于固话的异常呼叫行为监测与处置技术手段不足。缺少针对固定电话、语音中继异常呼叫行为的精准建模能力，现有模型难以及时有效地针对涉诈涉扰号码进行差异化管控。

b）缺少通话语音质检能力。对于语音呼叫服务提供商，仅仅依靠呼叫行为分析，无法鉴别企业用户外呼的实际情况，尤其是难以及时发现不法分子利用SIP协议漏洞获取系统管理权限，拨打诈骗电话，以及利用设备间、酒店房间私接设备实施诈骗的行为。

c）缺少用户画像分析与外部信息联动。缺少对企业用户及使用中号码的信用评分、健康度评估策略，难以有效区分问题用户和普通用户，无法针对不同用户制定有效策略。缺少与行业主管机构、第三方平台的联动能力，无法及时获取涉案号码、号码投诉或号码标记等数据。

如需解决上述痛点，需统筹考虑语音中继业务发展及业务安全痛点。从业务经营维度来看，首先，需要增强语音中继业务发展运营分析手段，实现对企业客户号码使用状态、接通率、投诉率等的一点看全能力。其次，对于语音中继外呼业务，需要对客户侧来电意愿等综合特征进行分析，改变接通率低、投诉率高的现象。最后，在号码管理、投诉处置、工单处理等方面，需要采取集约化管理手段，实现业务发展和安全管理的有效联动。通过业务收入、成本、投诉层面的经营模型，能更好掌控业务发展的“健康度”情况。

从安全监管维度，首先，需要增强语音中继业务安全管控手段，及时精准处置涉诈号码，实现一网统管一键关停能力。其次，需要增加对语音中继使用用户呼叫行为的风险控制能力，并且根据用户类型、业务场景、呼叫行为的突变实施有效的呼叫行为控制。再次，需要增加语音识别、语义理解等智能化质检手段，对超范围经营、涉诈涉扰等呼叫行为进行有效的监测及处置。最后，需要具备语音业务平台盗打识别能力。移动云坐席、云固话等“公有云+互联网”的通信资源访问方式存在业务安全风险。

2 运营体系与业务架构

2.1 解决思路

语音中继业务管控依赖于一套完整的运营体系和一系列技术手段，包括事前的源头治理、事中的监测处置、事后的核验预警等全方位举措，从而实现业务安全发展与高效运营。在集约化方面，可构建两级架构运营体系，即集团管理平台对全国31省省级管控平台进行数据拉通并进行业务管理，省级管控平台对语音专线网元层面实施具体管控，并对异常话务进行分析，实现业务接入的统一管理。同时，实时监控异常现象和数据，对违规业务进行“一键关停”，实现业

务风险的统一监测。集团管理平台可以配置管理风控策略、质检模型，一点开启全国生效，实现管控策略的统一配置。省级管控平台执行集团管理平台下发的风控策略、质检模型，发现异常自动预警上报，由反诈专员或业务运营人员统一审核，实现涉诈告警的统一稽核。

2.2 运营体系

从运营体系来看，集团管理平台面向集团决策人员，侧重于集中运营管理分析、态势感知研判与模型策略运营，具体包括租户管理、AI质检能力管控、处置指令下发、投诉管理、取证管理、录音存储管理、异常行为告警管理、预警信息推送、报表统计管理等面向全国语音中继业务的统一策略管理与统一业务运营数据分析。省级管控平台面向生产运营人员，侧重于模型策略的执行与话务控制，既包括对集团下发策略的配置、限制号码呼叫、分析呼叫行为、管理黑白名单，又包括对话务进行数据分析和人工检查稽核，对涉诈涉扰行为的快速发现、认定和处理。省级管控平台系统层面需对接各省通信网，进行信令采集、录音数据下载，同时对相关网元下发拦截和放行指令，实现对各类型中继话务的有效管控。语音中继安全运营体系如图1所示。

2.3 业务架构

为适配语音中继业务安全运营体系，围绕AI语音质检、呼叫行为风险控制、集中管理及运营分析等核心技术能力，通过构建安全治理+运营管理一体化平台，实现语音业务安全可管可控、运营数据一点看全。

整体业务架构分为数据采集层、业务执行层与业务应用层。数据采集层主要采集话单数据、呼叫信令数据与语音媒体数据，对接B域、O域、M域数据信息，同时与内部其他反诈类平台数据系统以及外部数据系统进行对接或联动。业务执行层包括分析处理模块与工单管理模块。分析处理子系统包含基于AI基础能力、大数据分析基础能力的语音转写与内容质检、异常呼叫行为判别、企业码号使用情况分析等功能，以及采集后数据的集中存储、敏感词库、风控策略库、异常呼叫行为模型库、质检模型库的持久化存储。工单管理模块包括工单的生成、派送、流转及流程自动化，以及报表统计、数据可视化、态势感知等业务管理类功能。业务应用层提供面向集团决策者的全国语音中继业务运营分析决策以及安全趋势研判的数据结果呈现，面向运营支撑人员的话术审核、模型训练、人工复检、核验救济的功能界面，同时面向省分工作人员提供本省中继业务发展情况、业务安全情况、策略执行情况的功能界面。该架构可实现事前-事中-事后端到端业务运营管理与安全治理。

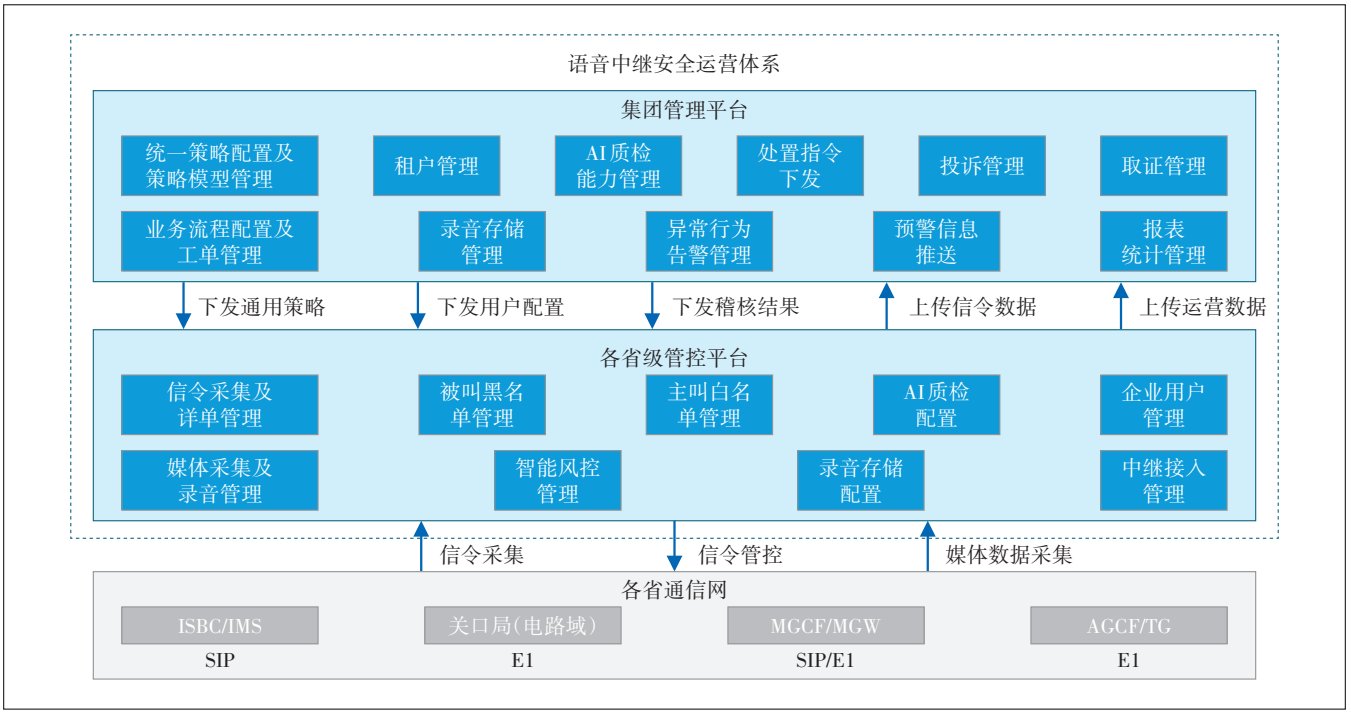

图1　语音中继安全运营体系

3 关键技术

语音中继业务安全运营涉及监测识别和预警处置两大环节，其中监测识别环节包括大数据异常呼叫行为分析以及AI质检关键技术，预警处置环节包括信令拦截关键技术。

3.1 基于大数据的异常呼叫行为分析

基于大数据的语音异常行为分析主要利用机器学习、模式识别、知识图谱等技术手段，以企业信息数据、话单数据、信令路由数据、监管平台投诉数据、互联网公司号码标记为数据来源，以数据挖掘行为分析结果为驱动，识别电信网络中的异常呼叫，进而对诈骗电话、非应邀商业电话进行准确预警。该技术通常用于事中识别监测及事后准实时处理，实时程度取决于模型准确率和人工复核能力[3]。

3.1.1 异常呼叫行为分析流程

大数据异常呼叫行为分析通常包括训练流程与预测流程（prediction）。训练流程包括数据样本采集、特征提取、数据分析、模型评估、模型上线5个环节；应用流程包括数据采集、通用规则比对（通用规则包含黑白名单管控、时间段管控、服务签约评判、呼叫阈值、按键DTMF事件、号码禁显、境外号码、静音识别）、模型比对、模型后评估4个环节。

3.1.2 异常呼叫行为关键技术

大数据异常呼叫行为常用算法包括分类算法、聚类算法与知识图谱。分类算法通过已知的诈骗样本、骚扰样本、投诉与标记数据进行模型训练，并利用训练好的模型对新的行为时间进行涉诈涉扰风险分析预测。

3.1.2.1 分类算法分析模型

根据话单数据计算每一个号码的通话特征，结合企业使用属性的一些规律特征（如外呼号码每天话务量和呼叫时段较固定、客服号码或企业固话无明显特征），使用决策树、朴素贝叶斯等相关机器算法训练多棵树模型，最终结合多棵树的预测结果判断高危号码。具体来说，基于企业信息、话单与信令日志，构建数据仓库并得到描述号码行为的各类特征表，根据不同诈骗电话、非应邀商业电话场景，利用特征工程理论进行特征选择，将特征向量作为多类型机器学习的输入，并通过Xgboost、随机森林将弱分类器组合成强分类器，进行结果组合得到最终判定结果。还可以基于号码的话单数据构建深度学习时序模型（如RNN、LSTM）来识别可疑号码，将基于时序的输入向量经过循环神经网络后，通过Attention机制让系统更专注于找到输入数据中明显与当前输出相关的有用信息。

3.1.2.2 聚类算法分析模型

聚类算法涉诈异常呼叫模型通常提取主叫号码原始信令数据集合x_1~x_n的相关属性，如振铃时长、拨打时间、呼叫间隔、被叫号码特征、呼叫频次、通话时长等指标，从中提取质心，并计算各主叫号码属性相异度，重复该步骤直至聚类结果不再发生变化。例如基于该方法提取某一个时间段全量疑似诈骗电话的信令数据，计算诈骗呼叫区别于其他呼叫的行为特征，包括振铃时间长，部分通话时长大于a秒，甚至大于b秒，拨打时间集中在c~d之间，被叫号码离散度高于e。通过全局分析和高维空间聚类，在少量样本数据或特征不明显的情况下找出数据中隐含的共同特征，完成关联涉诈号码的自动发现。

分类与聚类算法可以相互结合，进而提升发现识别技术能力。根据异常呼叫行为在多维空间向量上距离相近的特征，通过构建多维空间向量，利用聚类算法将疑似涉诈涉扰行为抽取共性信息生成训练数据。基于聚类算法生成的训练数据，分类算法能够在此基础上进行模型训练并进一步发现共性样本之外的异常呼叫行为，增强了反诈防扰监测研判与风险预警能力。

3.1.2.3 知识图谱

基于关系型数据库进行关联分析的传统大数据反诈风控模型在数据处理分析速度上存在一定局限性，知识图谱以图数据库为工具，聚合关联多种数据源，通过点和边的形式呈现企业、号码、主叫源地址信息等数据的关联性，对呼叫行为模式进行匹配分析，精准判断用户是否存在诈骗的可能性，是解决涉诈号码风险评估、企业平台号码盗打研判、异常行为分析的实际问题的重要技术。

3.2 基于AI质检的涉诈内容分析

AI质检技术利用运营商多类型语音涉诈样本，明确典型的高危诈骗场景，提供基于LLM模型的辅助数据标注以及预处理，选择如BERT、GPT等预训练语言模型作为反诈场景识别的基础，设计有效的文本特征提取方法，配合关键要素信息抽取与规则文法逻辑判断的综合研判模型，实现高准确度的意图理解与电话诈骗精准识别[4]。

3.2.1 AI质检分析流程

AI质检通过对网络侧政企语音的内容转写、关键要素提取、要素识别、意图分类，实现金融贷款、身份仿冒等电信诈骗场景内容识别模型的构建，对海量通话中涉诈涉扰电话进行准实时预警和处置，提升风险语音的监测识别能力[5]。

AI质检技术关键环节是智能语音识别与智能语义理解。智能语音识别通过语音分割、前端特征提取、区分性特征提取、特征规整、多遍解码、声学模型训练、语言模型训练、置信度判决，完成语音数据向文字的转换[6]。基于业务落地场景，收集大规模的语音数据，该数据为涵盖不同场景、不同说话人和不同语音特点的数据，并对相关数据进行音频信号降噪以及语音段的分割和标注等预处理。对于语音识别后的文本，智能语义理解基于传统深度神经网络（RNN、LSTM）或基于BERT等预训练模型，将语义相似的词映射为距离相近的词向量来进行关联，为诈骗通话文本意图标签分类提供精准的语义表达[7]。

3.2.2 AI语义理解关键技术

AI语义理解可对文本进行语义分析，作为AI质检底层能力，该技术能够用于理解语音转写的文本，为电信诈骗场景的内容识别模型提供更多判断特征[8]。AI语义理解主要包括内容要素抽取、文本分词与语义向量表征、意图理解三大环节。

内容要素抽取是基于NLU的分词分析和关键要素抽取能力，可自动对语音识别结果（文本）进行多类别的实体抽取（如人名、地名、机构、日期、证件号码、互联网账号、手机号以及行为、群体、宗教等敏感词汇）。实体抽取的重点在于需从文本中识别出具有特定意义的实体，如诈骗场景中的涉及银行卡、转账等敏感词，并考虑其在上下文语境的真实含义，判断文本是否为有效敏感词。

文本分词与语义向量表征通过词法分析、句法分析快速有效地分析句子中的短语、从句和句子成分，从而在无标注的情况下理解文本的词性和句子结构，将文本转换为多个关键词，同时利用文本向量表征，将语义分析问题转换为由一组词向量构成的语义空间[9]。

意图理解通过关键词正则匹配、规则文法、深度神经网络等方式进行通话内容的意图识别，将语音识别结果（文本）与各类诈骗模型进行比对并计算相关度，从而实现诈骗电话的检测。结合情感分析可更好地理解用户意图并进行反馈，为场景识别提供有效信息。在涉及诈骗骚扰的场景下，需要根据具体的业务需求与数据，定义合理的意图分类体系以及与诈骗场景的匹配关系。例如用户的违规意图，如冒充公检法、冒充金融客服贷款等，将直接触发诈骗预警，抑或用户实际使用号段意图与报备号段意图用途不一致，若其关键要素提取出违规内容，将间接触发诈骗预警[10]。

3.3 语音中继业务信令拦截技术

语音中继客户的接入方式分为IMS域接入和电路域2种类型，其中IMS域接入有MGCF、AGCF、ISBC 3种形式。语音中继省级管控平台在部署上并联跨接在ISBC/AGCF/MGCF关口局上，逻辑上串接在中继线路上，话务入网之前可以进行拦截与放通[11]。

对于AGCF/MGCF中继形式，省级管控平台对IMS域E1专线的管控对接方式、信令流程以及判断呼叫不合法时信令的拒绝流程分别如图2、3、4所示。

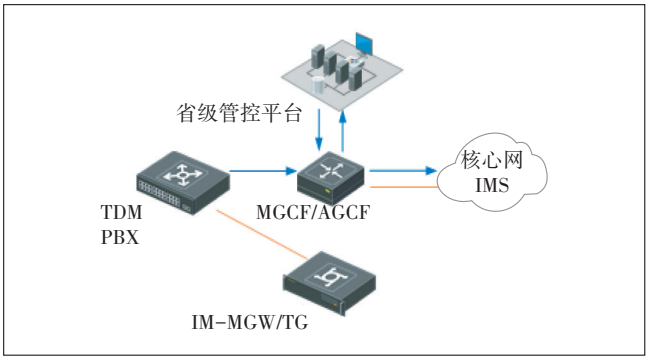

图2　AGCF/MGCF对接方式

对于ISBC中继形式，省级管控平台对IMS域E1专线的管控对接方式、信令流程以及判断呼叫不合法时信令的拒绝流程分别如图5、6、7所示。

电路域通过关口局的对接方式、信令流程及判断呼叫不合法时信令的拒绝流程分别如图8、9、10所示。

4 总结和展望

基于语音中继的呼叫中心、客服中心、企业总机业务可以通过低成本帮助企业快速和用户建立沟通桥梁，高效完成服务通知、产品推广、电话回访等政企需求，但一旦被滥用、盗用就会严重影响人民群众的正常生活，甚至遭受经济损失[12]。运营商需统筹业务发展和业务安全，应通过更全面、精准、有效的技术手段，并采取坚决果断的措施遏制电信网络诈骗、建立完善非应邀商业电话治理长效机制，精准施策[13]。一

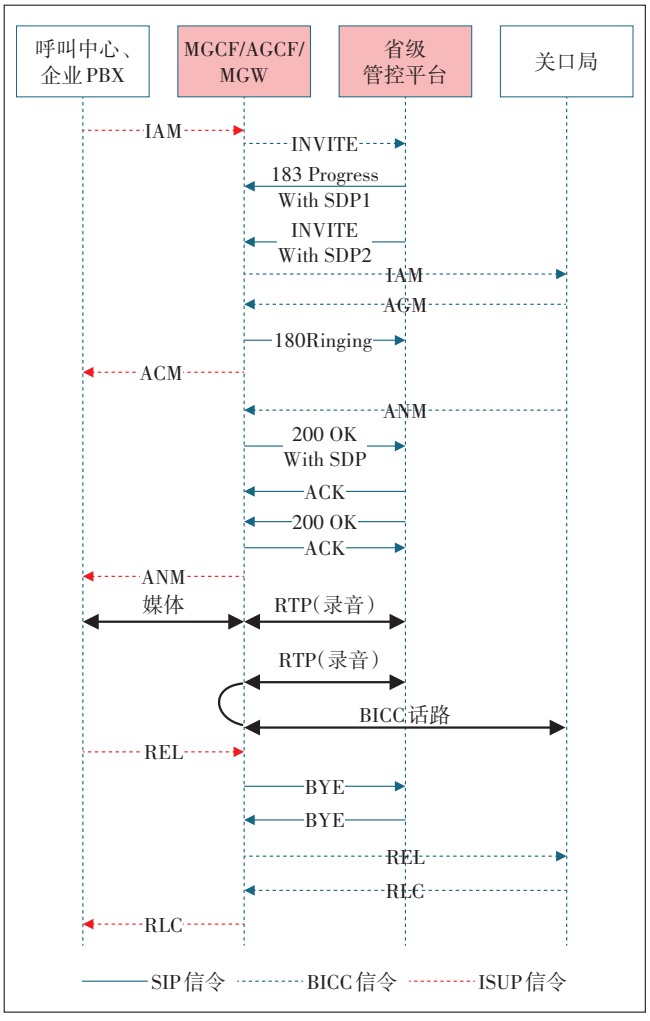

图3　AGCF/MGCF呼叫流程

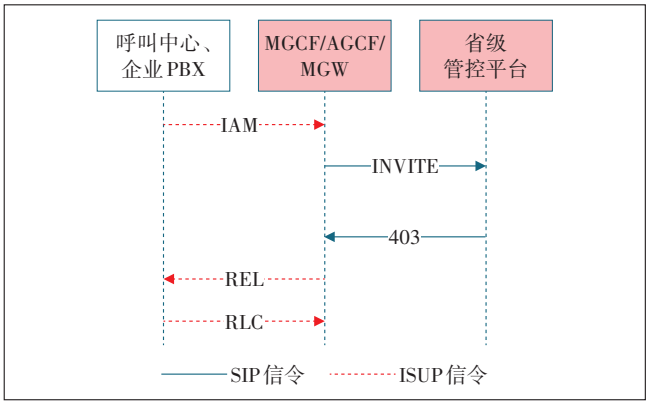

图4　AGCF/MGCF拦截流程

方面监测识别转租盗打等引发电信诈骗潜在行为，同时遏制违规领域推销，还群众“耳根清净”；另一方面切实满足政企客户面向真实需求用户群体信息精准触达的诉求，进而促进基础语音业务高质量发展[14]。

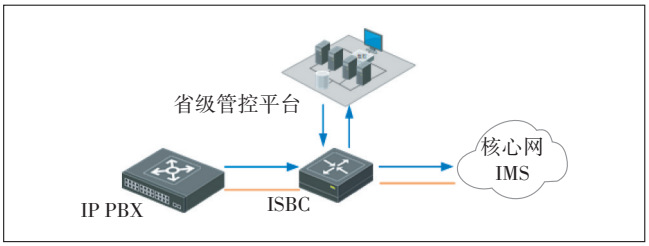

图5　SIP专线对接方式

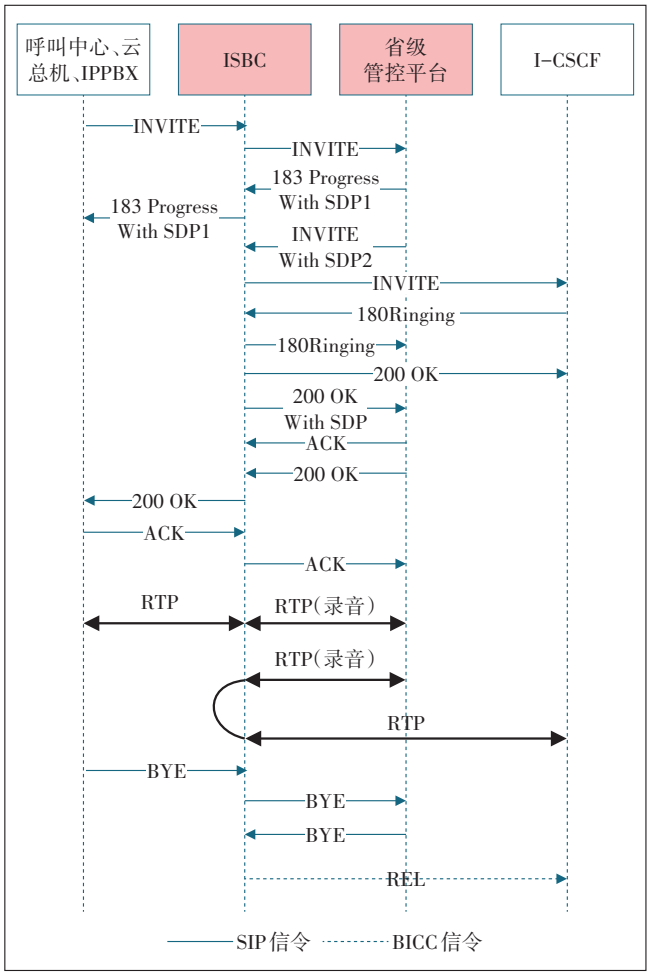

图6　SIP专线呼叫流程

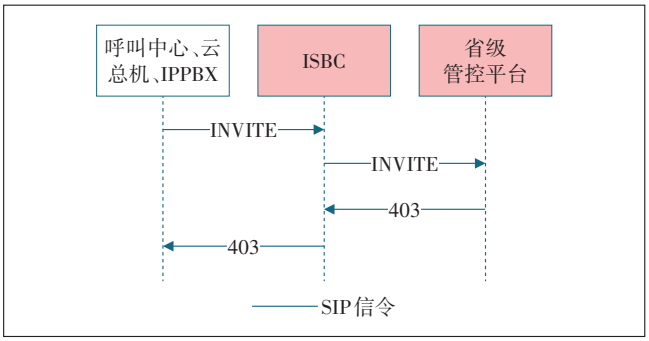

图7　SIP专线拦截流程

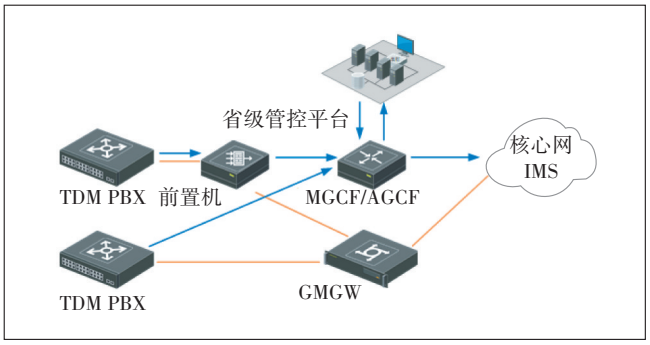

图8　关口局专线对接方式

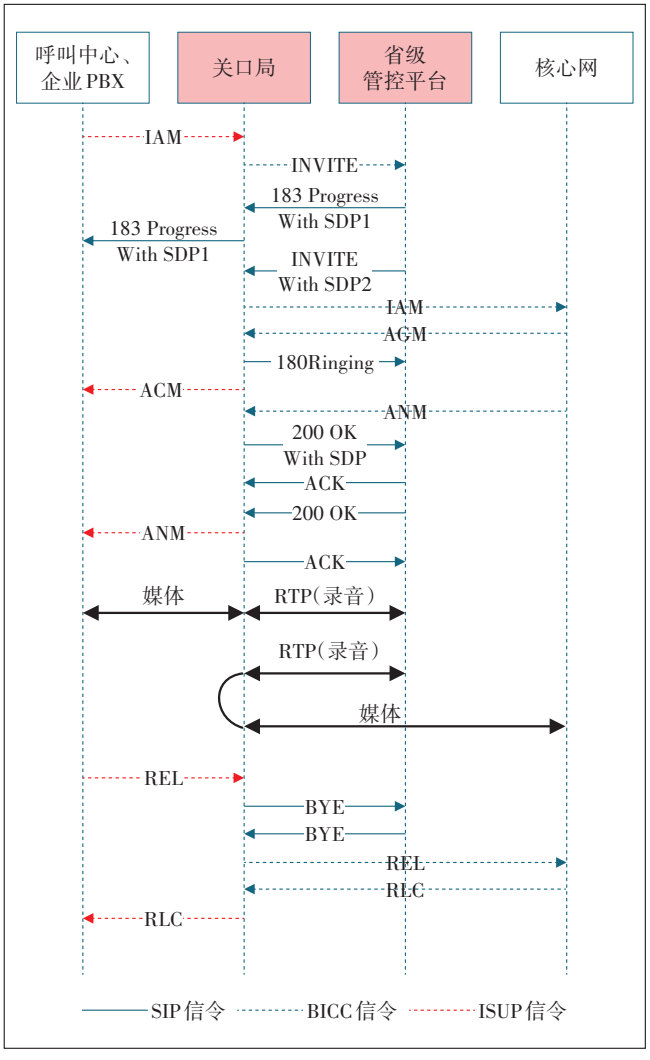

图9　关口局呼叫流程

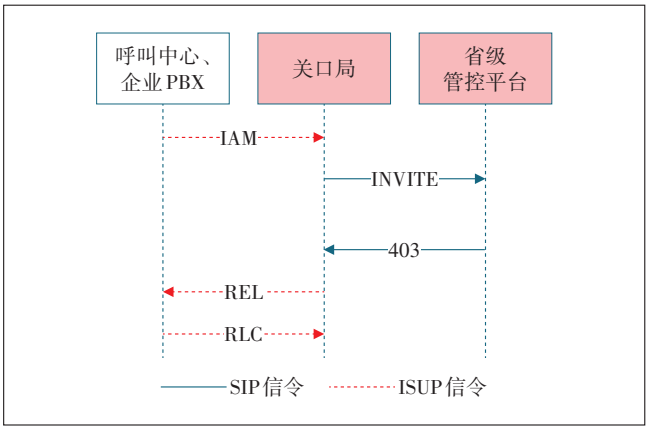

图10　关口局拦截流程

参考文献：

[1] 中国信息通信研究院安全研究所. 电信网络诈骗治理与人工智能应用白皮书(2019年)[R/OL]. [2024-01-29]. https://www.docin.com/p-2291103065.html.

[2] 中国信息通信研究院安全研究所. 新形势下电信网络诈骗治理研究报告(2020年)[R/OL]. [2024-01-29]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201218393889946295.pdf.

[3] 唐琦，杨光. 加强模式识别和机器学习技术在电信网络诈骗治理中的运用[J]. 人工智能，2022(1)：82-88.

[4] 刘红星，刘山葆. 声纹识别和意图理解技术在电信诈骗检测中的应用研究[J]. 广东通信技术，2020，40(7)：33-39.

[5] 付立挺，董德武，夏利松. 自然语言理解技术在电话诈骗识别预警领域的应用[J]. 警察技术，2021(5)：19-23.

[6] 陆文红，刘剑. 基于大数据+AI机器学习的反诈模型研究[J]. 邮电设计技术，2022(9)：59-64.

[7] 林宇俊. 5G时代下基于大数据AI的全周期反通信信息诈骗方案研究[J]. 电信工程技术与标准化，2019(11)：47-54.

[8] 蒲黎明. 电信诈骗语义分类系统的设计与实现[D]. 北京：北京邮电大学，2019.

[9] 刘黎辉，董倩，宋原. 基于互联网安全对诈骗、骚扰电话异常呼叫的拦截处置方案[J]. 信息与电脑，2019，31(23)：165-167，170.

[10] 纪润博，许子先. 构建立体防控体系治理电信诈骗[J]. 现代电信科技，2017，47(1)：18-23.

[11] 杜刚，朱艳云，张晨，等. 运营商反电信诈骗技术手段研究[J]. 电信工程技术与标准化，2021，34(3)：70-74.

[12] 黎宏. 电信诈骗中的若干难点问题解析[J]. 法学，2017(5)：166-180.

[13] 司徒德耀，林洁群，蔡培雄. 基于大数据分析的防电信诈骗呼叫建模[J]. 信息通信技术与政策，2018(1)：89-93.

[14] 中国信息通信研究院安全研究所. 信息通信行业防范打击通讯信息诈骗白皮书(2018年)[R/OL]. [2024-01-29]. https://www.doc88.com/p-6186489177590.html.

作者简介：
赵晨斌，工程师，学士，主要从事电信反诈、商用密码、信息安全领域政策研究与技术研究工作；符刚，高级工程师，硕士，主要从事信息安全、移动核心网、通信能力开放和新通信创新业务等研究工作；陈浩然，高级工程师，硕士，主要从事电信反诈、核心网音视频技术研究工作。