

基于5G-R的CTCS-3列控业务 接口监测系统研究

吴 宇¹, 董成文², 李 鹏²

(1. 中国铁路北京局集团有限公司, 北京 100860;

2. 中国铁道科学研究院集团有限公司, 北京 100086)

摘要: 基于 5G-R 的 CTCS-3 列控系统架构和 5G-R 接口协议栈, 研究 CTCS-3 列控业务接口监测系统架构、功能、性能以及关键技术。通过对 5G-R 信令、测量报告以及 CTCS-3 业务数据解析, 设计多种用户标识特征关联方法, 完成用户全过程数据整合与关联, 实现 CTCS-3 信令和数据跟踪、网络状况监测、查询分析、数据统计和日志图表等多种功能, 填补 5G-R 重要行车业务监测系统空白, 为 5G-R 无线网络优化提供实时、全程、多角度、多维度、图示化分析数据, 辅助 5G-R 网络下 CTCS-3 列控系统故障处理。

关键词: CTCS-3; 5G-R; 接口监测; 接口信令; 业务数据

中图分类号: U285.5

文献标志码: A

文章编号: 1673-4440(2023)06-0036-08

Research on CTCS-3 Train Control Service Interface Monitoring System Based on 5G-R

Wu Yu¹, Dong Chengwen², Li Kun²

(1. China Railway Beijing Group Co., Ltd., Beijing 100860, China)

(2. China Academy of Railway Sciences Co., Ltd., Beijing 100086, China)

Abstract: Based on 5G-R CTCS-3 train control system architecture and 5G-R interface protocol stack, this paper studies the architecture, functions, performance and key technologies of CTCS-3 train control interface monitoring system. Through the analysis of 5G-R signaling, measurement report and CTCS-3 service data, a variety of user identification feature association methods are designed to complete the user's whole process data integration and association, realize CTCS-3 signaling and data tracking, network status monitoring, query and analysis, data statistics and log chart and other functions, fill in the gaps in 5G-R important traffic service monitoring system, and provide real-time, whole-process, multi-angle, multi-dimensional graphical analysis of data for 5G-R wireless network

收稿日期: 2022-10-24; 修回日期: 2023-05-16

基金项目: 中国铁道科学研究院集团有限公司基金课题项目 (2021YJ115)

第一作者: 吴宇 (1984—), 男, 高级工程师, 硕士, 主要研究方向: 铁路通信, 邮箱: 18911889209@189.cn。

optimization to assist in troubleshooting of CTCS-3 train control system under 5G-R network.

Keywords: CTCS-3; 5G-R; interface monitoring system; interface signaling; service data

铁路将 5G-R 系统作为下一代移动通信研究方向, 成立中国铁路下一代移动通信技术研究工作组, 全面开展各相关方面技术研究。在标准制定、技术方案、系统研发、应用设计、频率特性及干扰防护研究等方面均取得一定进展。目前在监测系统研究方面仍然是空白, 缺少基于 5G-R 的 CTCS-3 (以下简称 C3) 列控业务接口监测系统, 实现对 5G-R 承载的主要行车业务进行监测, 特别是 C3 列控业务的全过程监测, 进而对监测业务的异常事件和异常状态进行预警, 辅助支撑 5G-R 网络的运营维护和 C3 列控系统故障处理。

1 概述

铁路专用移动通信是铁路信息化、数字化、智能化的重要基础设施和关键技术装备, 在支撑铁路运营、保障行车安全、提高运输效率、提升维护水平等方面发挥着重要作用。为满足铁路运输生产需要, 下一代移动通信系统推出后, 铁路 5G-R 专网取代 GSM-R 网络, 承载 C3 列控系统车-地间双向

传输。

5G-R 承载 C3 列控业务时使用现有车-地安全通信连接机制和应用消息流程, 完成行车许可、线路参数、临时限速、列车位置、列车数据等信息交互。为实现上述业务并确保 GSM-R 覆盖线路和 5G-R 覆盖线路的跨线运行, 需要对 C3 列控系统车载和地面设备及组网方式进行改进。将 ATP 的 MT 替换为 GSM-R+5G-R 双模, ATP 车载设备的 RTU 无线通信单元包含 CSD 模式和 5G-R 模式下的车-地数据传输协议, 并支持两套协议同时工作, RTU 与 MT 接口形式保持不变。RBC 设备增加 5G-R 模式的接口, 通过该接口与 5G-R 网络的 SMF 设备连接, 如图 1 所示。

2 系统组成及架构

5G-R 系统 C3 列控业务接口监测系统由数据采集单元、数据业务解析单元、信令解析单元、关联同步单元、数据存储单元、综合分析单元、网管单元、客户端、网关单元及网络安全设备组成。其

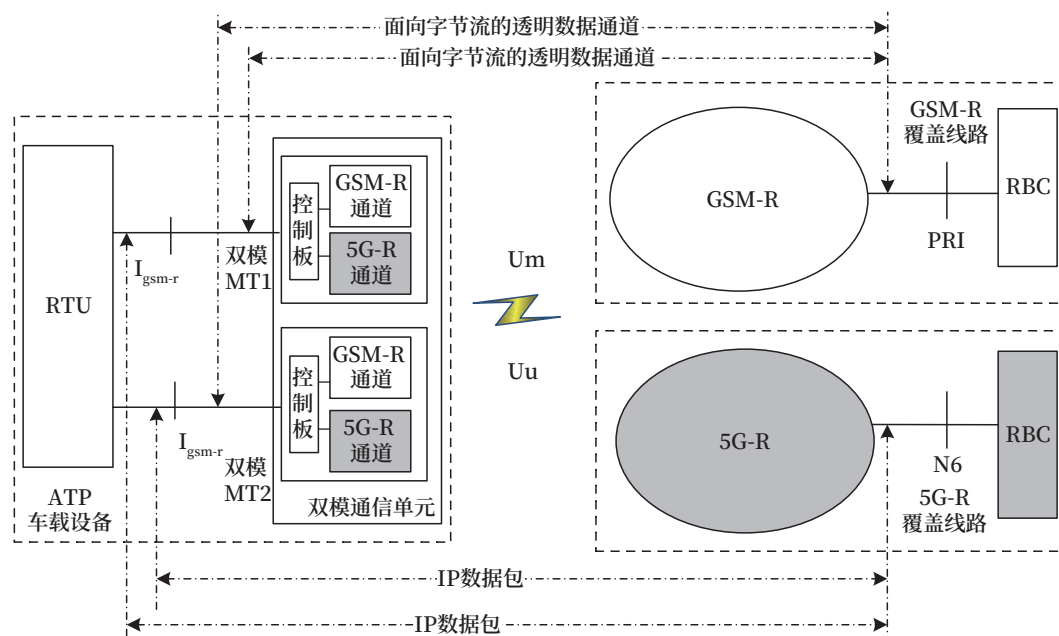


图1 5G-R承载的CTCS-3列控系统改造

Fig.1 Transformation of CTCS-3 train control system carried by 5G-R

中采集单元、数据业务解析单元、数据存储单元和信令解析单元部署在现场通信机械室机房，综合分析单元、网管单元、客户端、网关单元及网络安全

设备部署在铁路局集团公司核心网机房，现场设备与核心网设备之间通过传输或数据网互联互通。如图2所示。

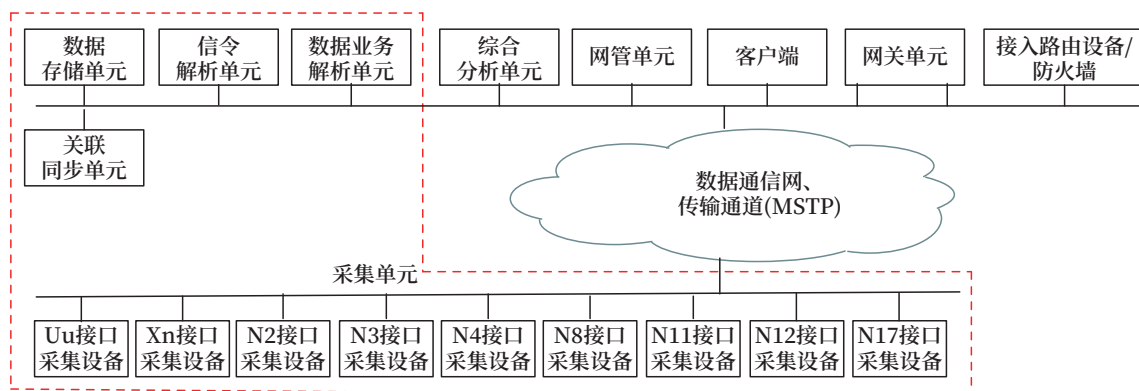


图2 基于5G-R的CTCS-3列控业务接口监测系统架构

Fig.2 Architecture of CTCS-3 train control service interface monitoring system based on 5G-R

2.1 采集单元

采集单元实现 Uu 接口 (UE 与 RAN 之间的接口)、Xn 接口 (gNB 之间的接口)、N2 接口 (RAN 与 AMF 之间的接口)、N3 接口 (RAN 与 UPF 之间的接口)、N4 接口 (SMF 与 UPF/ 边缘 UPF 之间的接口)、N8 接口 (UDM 与 AMF 之间接口)、N11 接口 (AMF 与 SMF 之间接口)、N12 接口 (AMF 至 AUSF 之间的接口)、N17 接口 (AMF 至 5G-EIR 之间的接口) 信令及业务数据进行解析。N2、N3、N4、N8、N11、N12、N17 接口以下统称 NG 接口。

Uu 接口上行通过采用功分器将基站天馈线上行信号功分一路给数据采集设备，下行通过吸盘天线采集所在基站及相邻基站的射频信号，Uu 层采集单元会对物理层信号进行解调，将 TB 传输块信息发送至信令解析单元和数据解析单元。

NG 和 Xn 接口使用 wireshark 工具等网络抓包工具实现以太网数据采集功能，网络抓包工具能解析 http 消息格式，并支持 5G-R 标准接口消息。通过配置相关协议栈，如果是信令层面，能从以太网帧数据中还原物理层、数据链路层、IP 层、SCTP 层和 NGAP 层信令；如果是用户层面，能从以太网帧数据中还原物理层、数据链路层、IP

层、UDP 层消息。通过采集单元处理后，信令解析单元仅用处理后续 NGAP 信令即可，数据解析单元仅用处理后续 GTP-U 和 C3 业务数据即可，如图3所示。

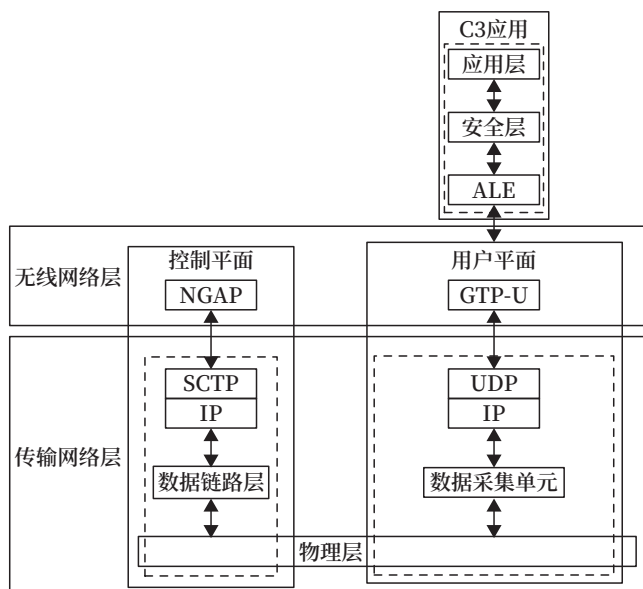


图3 NG和Xn接口解析协议栈

Fig.3 NG and Xn interfaces parse protocol stack

2.2 信令和数据解析单元

Uu 接口信令解析单元实现 MAC、RLC、PDCP、RRC 和 NAS 协议栈解析。Xn 接口和 NG 接口信令解析单元实现物理层、数据链路层、IP、SCTP、

NGAP 协议栈解析。

Uu 接口业务解析单元实现 MAC、RLC、PDCP、SDAP、ALE、安全层和应用层协议栈解析。Xn 接口和 NG 接口业务解析单元解析 IP 层、校验 IP 层, 获得传输层首部, 校验传输层, 解析 UDP 和 GTP 协议承载的应用数据, 按 C3 业务协议栈格式要求解析应用数据。

2.3 综合分析单元

综合分析单元是整个系统中枢, 根据被监测用户标识信息, 对采集原始数据进行关联、合成, 对

与被监测用户相关各接口信令和业务数据进行关联分析, 对指标统计结果进行汇总。综合分析单元汇聚 Uu、NG 和 Xn 接口信令和数业务解析系统的预处理信息, 从 5G-R 运营与支撑系统获取密钥, 从 EIR 查询用户身份信息, 与网关单元透传跨局信息, 接收网管单元配置变更和心跳包, 将解析后的信令及业务数据送到存储单元存储, 同时送到操作显示单元显示给用户。综合分析单元与其他单元间通信流程如图 4 所示。

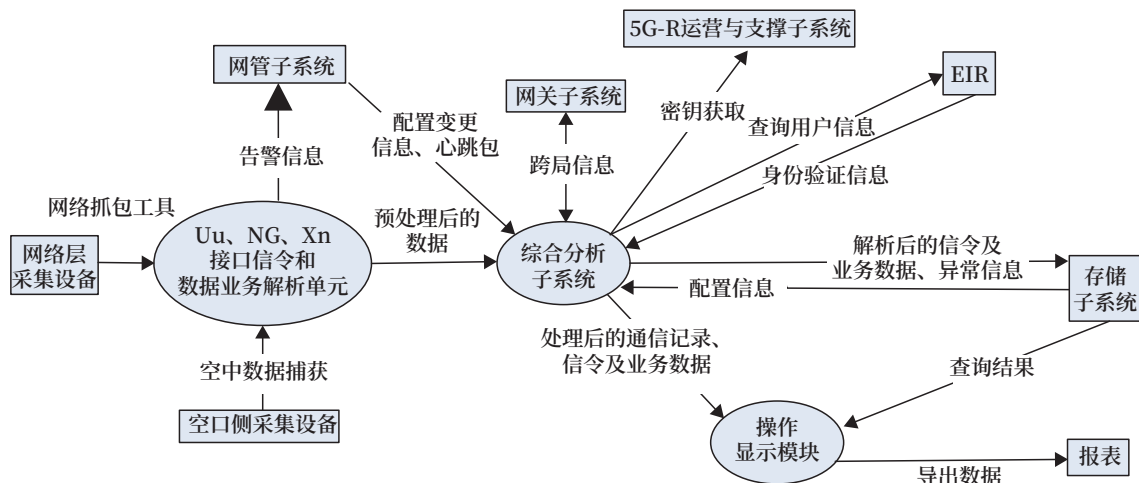


图4 综合分析单元与其他单元间通信流程

Fig.4 Communication process between integrated analysis unit and other units

3 系统功能及性能

3.1 系统功能

3.1.1 信令及业务跟踪

C3 列控业务通过 5G-R 系统承载时, 监测信令与业务流程主要包括系统消息下发、随机接入、RRC 连接管理、上下文管理、注册管理、会话管理、C3 业务数据传输和移动性管理等, 如图 5 所示。

1) 系统消息

系统消息存在 Uu 接口上, 是 UE 获得网络服务信息的第一步。通过系统消息的广播下发, UE 可以获得 AS 层和 NAS 层信息。UE 在开机选择小区驻留、重选小区、切换、以及从非覆盖区返回覆盖区时, 都会主动读取系统消息, 包括 MSI 和 OSI 系统

消息。本系统不需要获取系统消息来支持 C3 信令和业务的解析, 因此本系统不对系统消息进行处理。

2) 随机接入

随机接入过程存在 Uu 接口上, 包括基于竞争随机接入和基于非竞争随机接入过程。在初始 RRC 连接建立、RRC 连接重建、下行数据到达、上行数据发送、未激活态至连接态转换中会采用基于竞争的随机接入, 切换过程会优先采用基于非竞争的随机接入。本系统监测随机接入消息为 MSG 消息, 随机接入过程前 gNB 分配给 UE 了 C-RNTI 的动态标识, 唯一标识了一个小区空口下的 UE。

3) RRC 连接管理

RRC 连接管理存在 Uu 接口上, 包括 RRC 连接建立、RRC 连接重配、RRC 连接释放等过程。RRC 连接管理监测的信令流程包括 RRCSetupRequest,

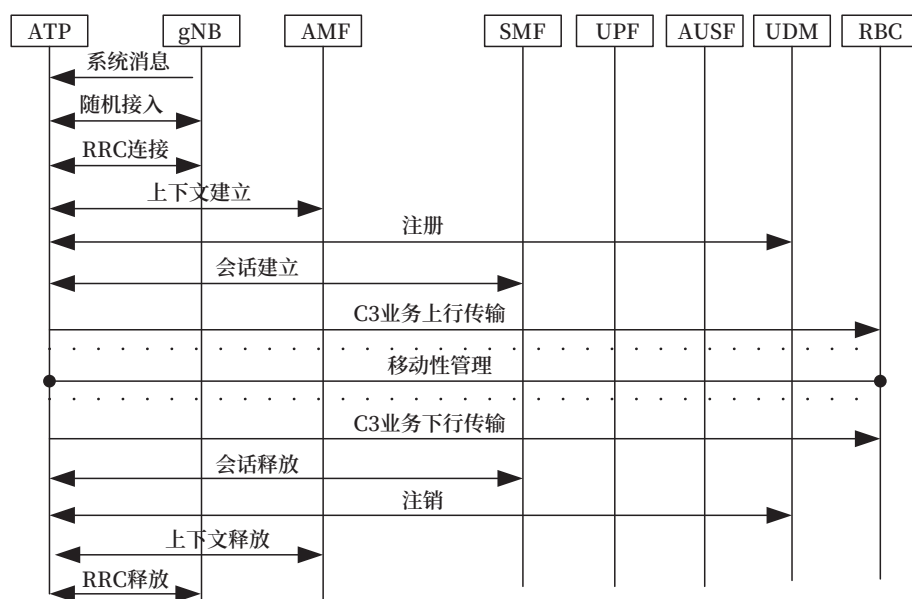


图5 基于5G-R的CTCS-3列控业务信令和数据跟踪流程
Fig.5 Signaling and data tracking process of CTCS-3 train control service based on 5G-R

RRCSetup, RRCSetupComplete, RRCReject。在RRC连接建立时会创建RRC-TransactionIdentifier标识, 该标识能够关联后续同一UE所有RRC消息。

4) 上下文管理

上下文管理存在Uu、N2、N12、N17接口上, 包括上下文建立、上下文修改和上下文释放过程。在上下文建立过程中, gNB会为UE创建专用的RAN-UE-NGAP-ID, 该标识在后续NG和XN接口消息关联中有重要作用。在上下文建立过程中, 同步完成gNodeB透传UE和AMF之间的NAS直传消息, 包括IDENTITY查询、鉴权、NAS安全模式和注册过程等。

上下文管理监测的Uu接口信令包括NAS Identity Request, NAS Identity Response, NAS Authentication request, NAS security Mode Command, AS security Mode complete, SecurityModeCommand, UECapabilityEnquiry, UECapabilityInformation, RRCReconfiguration, RRCReconfigurationComplete。

上下文管理监测的N2接口信令包括Initial Ue Message, Context Setup Request, Ue Radio Capability Info Indication, Initial Context Setup

Response, Ue Context Modification Request, Ue Context Modification Response, Ue Context Release Request, Ue Context Release Command, Ue Context Release Complete消息, 其中Initial Ue Message包含了NAS透传的注册请求, 携带了5G-S-TMSI和5G-GUTI的UE ID信息, 对实现Uu接口和NG接口用户信息关联起到重要作用。Context Setup Request包含了NAS透传的注册接受消息。

上下文管理监测的N12接口信令包括Nausf_UEAuthenticate_authenticate Request, Nausf_UEAuthenticate_authenticate Response。

上下文管理监测的N17接口信令包括N5g-eir_EquipmentIdentityCheck Request, N5g-eir_EquipmentIdentityCheck Response。N5g-eir_EquipmentIdentityCheck Request携带了UE的PEI或SUPI, 对于实现Uu接口和NG接口用户信息关联起到重要作用。

5) 注册管理

注册过程存在N2接口和N8接口上, 是穿插在上下文管理过程中完成的。注册过程监测的N2接口信令包括Registration Request, Registration

Accept, Registration Complete。N8 接口信令包括 Nudm_UEContextManagement_Registration Request, Nudm_UEContextManagement_Registration Response, Nudm_SubscriberData Management_Get Request, Nudm_SubscriberDataManagement_Get Response。

6) 会话管理

会话管理存在于 Uu、N2、N4、N11 接口, 包括 PDU 会话建立、PDU 会话修改和 PDU 会话释放过程。

会话管理监测的 N2 接口信令为 PDU Session Resource Setup Request, PDU Session Resource Setup Response, PDU Session Resource Modify Request, PDU Session Resource Modify Response, PDU Session Resource Release Command, PDU Session Resource Release Response。在 PDU 会话建立过程中会创建用户隧道 TEID 和 UE IP 地址, 该 ID 和 IP 地址将配合其他用户标识, 在进行 C3 业务数据关联中起到重要作用。

会话管理监测的 N4 接口信令为 PFCP Session Modification Request 和 PFCP Session Modification Response。

会话管理监测的 N11 接口信令为 Nsmf_PDUSession_UpdateSMContext Request 和 Nsmf_PDUSession_UpdateSMContext Request。

会话管理监测的 Uu 接口信令为 RRCReconfiguration 和 RRCReconfigurationComplete。

7) C3 数据业务传输

C3 数据业务传输为 ATP 与 RBC 之间透明传输列控业务, 存在与 ATP 与 RBC 之间的各接口。基于 5G-R 网络, RBC 向车载设备 ATP 发送位置报告参数信息和行车许可请求参数信息, 车载设备向 RBC 报告基于 LRBG 的列车位置和当前等级及模式信息。RBC 向列车发送行车许可及线路参数信息, ATP 车载设备根据这些信息实时生成目标距离模式曲线监控列车安全运行。该内容与 GSM-R

接口监测 C3 业务数据处理方式相同, 通过对链路层、传输层、安全层、应用层协议栈解析, 实现 C3 数据业务传输应用消息监测, 主要包括 Initiation of a Communication Session, Configuration Determination, Session Established, Train Position Report, General Message, Acknowledgement of Train Data, MA, MA Request, Termination of a Communication Session, Acknowledgement of Termination of a Communication Session 等。

8) 移动性管理

列车运行过程中经过不同的 gNB 或 AMF 时, 正在传输的 C3 列控业务需要完成切换过程。5G-R 切换业务包括基于 Xn 切换和 N2 切换, 本系统将对切换流程全过程进行监测。移动性管理存在于 Uu、N2、NG 接口, 以 N2 切换为例, 移动性管理监测的 Uu 接口信令包括 RRCReconfiguration, RRCReconfigurationComplete; N2 接口信令包括 Handover Required, Handover Request, Handover Command, Handover Notify, UE Context Release Command, UE Context Release Complete。

3.1.2 测量报告跟踪

GSM-R 网络中切换和小区重选等移动性管理过程是 BSC 判断实现, BSC 判断基于无线网络的场强和质量, 测量报告是通过 Abis 接口从 BTC 发送至 BSC。而 5G-R 网络中 gNB 实现了小区选择, 小区重选和切换过程, UE 需要向 gNB 发送服务小区和邻小区的测量报告, 因此 5G-R 测量报告 Uu 接口消息。通过解析 Uu 接口 Measurement Report 消息, 最终解析当前服务小区的无线场强与质量, 即 RSRP、RSRQ 以及 SINR。

测量报告跟踪原理为 Measurement Report 消息包含 MeasurementReport-IEs, Measurement Report-IEs 读取 MeasResults 内容, 当前服务小区列表包含在 MeasResults 的 MeasResultServing MOList 中, 邻小区列表在 MeasResults 的 Meas

ResultNeighCells 中。读取服务小区和邻小区后,通过 MeasResultServingCell 获取服务小区 RSRP,RSRQ 以及 SINR,通过 MeasResultNR 获取邻小区 RSRP,RSRQ 以及 SINR。

3.2 系统性能

本系统主要性能有如下要求。

- 1) 各接口数据采集设备与被监测系统完全隔离,不影响被监测系统的正常工作;
- 2) Uu 接口采集的频段范围应覆盖 5G-R 网络上/下行频段;
- 3) Uu 接口采集设备的采集灵敏度 $\leq -102\text{dBm}$;
- 4) 系统数据采集、解析准确性 $\geq 99.99\%$;
- 5) 系统数据丢包率 $< 0.01\%$;
- 6) 应同时支持对链路发送、接收方向的汇聚监听和分离监听。

4 系统关键技术

4.1 密钥管理技术

与 GSM-R 系统不同,为了确保数据传输安全性,5G-R 系统对传输的信令和数据进行密钥加密,在没有密钥情况下,难以解析各接口信令和业务数据。本系统通过与核心网网元 5G-R 运营与支撑子系统互联,从密钥管理模块获取密钥,对采集的空口、核心网各网元间的接口数据进行解码,并支持对密钥的安全保护,短期密钥使用后及时进行安全删除、长期密钥安全存储和长期密钥有效期的管理。

4.2 Uu接口关联技术

Uu 接口信令协议分为 RRC 信令和 NAS 信令。本系统实现的 RRC 信令、NAS 信令以及随机接入信令关联方案为:首先随机接入信令包含 C-RNTI 字段,该字段能够将随机接入 MSG1~MSG4 消息串联起来;其次 RRC 连接的建立信令通过 5G-S-TMSI 标识进行关联。由于随机接入的 MSG3 消息中包含 RRC 连接的建立信令的 RRCSetupRequest,因此通过 RRCSetupRequest 信令能够将随机接入与 RRC 连接的建立信令关联起来。RRC 连接的建立信令中的 RRCSetup 信

令中包含 RRC-TransactionIdentifier 用户标识,通过该用户标识能够将 Uu 接口上该用户其他 RRC 信令与测量报告信息关联起来。NAS 信令使用 RRC 信令中的 ULInformationTransfer 承载,ULInformationTransfer 包含 RRC-Transaction Identifier,通过该字段能够实现 RRC 信令和 NAS 信令关联。

4.3 NG和Xn接口关联技术

NG 和 Xn 接口关联技术包括信令关联技术和业务数据关联技术。NG 和 Xn 接口信令关联采用“源 IP 地址+源端口号+目的 IP 地址”为关联特征。以 N2 接口为例,源端口号为 RAN-UE-NGAP-ID,如基站切换或 AMF 更新后仍可继续跟踪 RAN-UE-NGAP-ID。NG 和 Xn 接口业务数据关联特征为 GTP-U 的 TEID 字段,标识数据归属隧道,每个 C3 用户有独一无二的 TEID,通过 TEID 可以关联用户业务数据。

4.4 综合分析关联技术

Uu 接口与 NG、Xn 接口数据的多接口间关联方案为:首先关键信令 NITIAL UE MESSAGEINITIAL 包含 NAS 透传的注册请求,携带了 5G-S-TMSI 和 5G-GUTI 的 UE ID 信息,进而通过 N5g-eir_EquipmentIdentityCheck Request 消息实现 gNB-S1AP-ID 与 PEI/SUPI/5G-S-TMSI 用户标识进行绑定,实现 Uu 接口与 NG、Xn 接口数据的关联。

4.5 云监测技术

除采集单元外,其他单元均可采用云平台部署方式,部署在铁路监测云上。采用云部署的优点有 3 点:一是用户可以通过软件仓库方式任意搭配需要监测的接口模块,实现用户自定义部署;二是用户可以通过云平台虚拟化系统自动化部署系统功能,提高使用效率;三是用户能够按照统一的接口调用所有 5G-R 厂家的监测信息,打破不同设备厂家间的壁垒。

5 结束语

5G-R 网络接口监测系统是对承载 C3 列控任务的 5G-R 网络中各接口进行跟踪监测, 通过采集、解析各接口的网络信令及业务数据, 采用实时关联、自动定界、深度智能 DPI 业务识别等多种技术定位用户通信异常原因, 并对无线网络性能及故障信息进行分析、统计, 为 C3 列控系统运维和故障定位提供依据。

参考文献

- [1] 葛伟涛, 冯敬然, 周敏, 等. 铁路 5G-R 无线接入网组网方案 [J]. 铁路通信信号工程技术, 2022, 19 (6): 59-63.
Ge Weitao, Feng Jingran, Zhou Min, et al. Networking Scheme of Railway 5G-R Wireless Access Network[J]. Railway Signalling & Communication Engineering, 2022, 19(6): 59-63.
- [2] 王玮. 5G-R 冗余技术方案研究 [J]. 中国铁路, 2021 (8): 13-18.
Wang Wei. Research on Redundancy Technology Scheme of 5G-R[J]. China Railway, 2021(8): 13-18.
- [3] 肖正杰, 张亮, 孙迪. 铁路 5G-R 语音调度通信系统研究 [J]. 铁路通信信号工程技术, 2022, 19 (8): 36-39, 91.
Xiao Zhengjie, Zhang Liang, Sun Di. Research on 5G-R Voice Dispatching Communication System[J]. Railway Signalling & Communication Engineering, 2022, 19(8): 36-39, 91.

- [4] 庞萌萌. 铁路 5G-R 系统核心网架构研究 [J]. 中国铁路, 2021 (8): 1-6.
Pang Mengmeng. Research on Core Network Architecture of Railway 5G-R System[J]. China Railway, 2021(8): 1-6.
- [5] 王建敏. 兼容 GSM-R 和 5G-R 互联互通的列控系统无线通信方案研究 [J]. 铁路通信信号工程技术, 2021, 18 (5): 42-46, 99.
Wang Jianmin. Research on Wireless Communication Scheme of Train Control System Compatible with 5G-R and GSM-R Interoperability[J]. Railway Signalling & Communication Engineering, 2021, 18(5): 42-46, 99.
- [6] 杨锐, 郭桂芳, 赵武元. 铁路 5G-R 运维技术方案研究 [J]. 中国铁路, 2021 (8): 19-25.
Yang Rui, Guo Guifang, Zhao Wuyuan. Research on Technical Scheme for Operation and Maintenance of 5G-R[J]. China Railway, 2021(8): 19-25.
- [7] 李雪, 许扬. 5G-R 信令组网方案研究 [J]. 铁路通信信号工程技术, 2020, 17 (10): 33-36.
Li Xue, Xu Yang. Research on 5G-R Signaling Networking Scheme[J]. Railway Signalling & Communication Engineering, 2020, 17(10): 33-36.

(上接 14 页)

- [5] 王宇. 车号识别系统在机务段的综合应用 [J]. 机车电传动, 2002 (6): 49-50.
Wang Yu. Comprehensive Application of Vehicle Number Recognition System in Locomotive Depot[J]. Electric Drive for Locomotives, 2002(6): 49-50.
- [6] 李瑞. 车号与箱号识别关联技术在铁水联运中

的应用 [J]. 铁路通信信号工程技术, 2022, 19 (5): 49-5, 67.
Li Rui. Application of Wagon and Container Numbers Identification and Correlation Technology in Railway and Waterway Multimodal Transport[J]. Railway Signalling & Communication Engineering, 2022, 19(5): 49-52, 67.