5G网络信令流量安全监测研究

Research on Security Monitoring of 5G Network Signaling Traffics

郑　涛[1]，谢泽铖[2,3]，张曼君[2,3]，陆　勰[2,3]，王姗姗[2,3]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中国联通研究院，北京 100048；3. 下一代互联网宽带业务应用国家工程研究中心，北京 100048）

Zheng Tao[1]，Xie Zecheng[2,3]，Zhang Manjun[2,3]，Lu Xie[2,3]，Wang Shanshan[2,3]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. China Unicom Research Institute，Beijing 100048，China；3. Next Generation Internet Broadband Service Application National Engineering Research Center，Beijing 100048，China）

摘　要：

5G与垂直行业的深度融合使得攻击者更易利用网络的暴露面发起攻击，而网络流量正是攻击行为的载体，各企业防护的难度也越来越高。在此背景下，除了传统的安全防护手段之外，运营商和5G行业客户均希望能够对5G流量进行安全分析监测，弥补其他安全工具的不足之处。通过主动监测5G信令交互异常行为，对可能遭受的信令攻击和终端异常等事件进行预警，有助于全面掌握5G网络的安全态势，打造更加安全的5G网络。

关键词：

5G；信令流量；安全；监测

doi：10.12045/j.issn.1007-3043.2023.09.014

文章编号：1007-3043（2023）09-0075-04

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：

The deep integration of 5G and vertical industries makes it easier for attackers to launch attacks on networks by taking advantage of network exposure，and network traffics are the carriers，which makes it increasingly difficult for enterprises to defend the attacks. In addition to traditional security protection methods，both operators and 5G industry customers hope to conduct security analysis and monitoring of 5G traffics and make up for the shortcomings of other security tools. By actively monitoring the abnormal interaction of 5G signaling，it gives early warning to the possible signaling attacks and terminal anomalies，so as to grasp the security situation of 5G network and build a more secure 5G network.

Keywords：

5G；Signaling traffics；Security；Monitoring

引用格式：郑涛，谢泽铖，张曼君，等. 5G网络信令流量安全监测研究[J]. 邮电设计技术，2023（9）：75-78.

0 引言

自2019年商用以来，5G网络已经迈入高速发展期，各种现象级应用层出不穷，5G用户的单用户流量跟4G用户的单用户流量相比有了极大的提升[1]。目前，5G网络的接入流量、业务流量仍在持续大规模增加中。5G网络与各种垂直行业的融合在深度和广度上也都得到了大幅提升，这种深度融合使得原来封闭的园区网络和运营商网络向着纵深开放转变，攻击者更易利用网络的暴露面发起攻击，而网络流量正是攻击行为的载体，使得各企业进行安全防护的难度越来越高。

在此背景下，除了传统的安全防护手段之外，运营商和5G垂直行业客户均希望能够通过有效的流量监测技术手段，对5G专网流量进行安全分析监测，以便更加快速地发现安全事件并进行威胁溯源，弥补其他安全工具的不足之处。

1 传统流量监测技术简介

网络流量分析技术（Network Traffic Analysis，NTA）于2013年被首次提出，并且在2016年逐渐兴起。2017年，NTA被Gartner评选为2017年十一大信息安

收稿日期：2023-07-28

全新兴技术之一,同时也被认为是5种检测高级威胁的手段之一。在Gartner的定义里,NTA是以网络流量为基础,应用人工智能、大数据处理等先进技术,基于流量行为进行实时分析并展示异常事件的客观事实[2]。后来,随着技术的发展,在NTA基础上逐渐增加了检测和响应的功能,Gartner于2020年提出了NDR(Network Detection and Response)的概念,成为业界的主流。文献[3]提出对无线网络流量的分析和准确预测是无线网络管理与安全领域的重要研究内容之一,在网络规划、网络监控、流量趋势分析、网络优化以及入侵检测和异常检测等方面发挥着重要作用,并介绍了DPI(Deep Packet Inspection)、DFI(Deep / Dynamic Flow Inspection)等典型的无线网络流量分析的模型与常用流量分析方法。文献[4]介绍了将DPI技术与DPF技术结合进行全流量分析的方法。文献[5]介绍了NetStream、Netflow、sFlow等基于端口的分析技术和基于DPI网络探针等网络流量的分析技术。文献[6]介绍了5G场景下的全流量安全检测与分析技术,采集5G全流量、资产信息、漏洞信息、设备日志、安全事件等信息,进行全网5G安全事件监测分析、5G终端资产管理、漏洞管理、原始攻击报文存储、5G安全事件溯源及处置、5G安全威胁态势感知等。

目前国内外安全企业已经提供了多款网络流量安全分析监测类系统,用于监测和解决企业互联网场景下IT网络所面临的安全问题。同时,NTA技术在移动通信网络中也有应用,一般用于分析基于HTTP(Hyper Text Transfer Protocol)、FTP(File Transfer Protocol)等传统传输协议的用户流量,进行Web(World Wide Web)应用攻击、数据库攻击、网络恶意程序等安全攻击事件的监测和识别,适用于日常异常流量监测、攻防演练等场景,如图1所示,缺乏根据网络流量特点及5G网络业务特点进行分析的信令流量监测技术。

随着5G网络应用场景的不断扩展以及5G网络个性化安全需求的不断增加,现有NTA技术和流量安全分析监测类系统无法实现针对5G网络特有的交互流量协议,如PFCP(Packet Forwarding Control Protocol)、NGAP(Protocol for NG Interface)等协议的识别、解析和威胁发现,缺少针对5G网络场景类交互异常和威胁感知的能力,无法满足5G网络场景的流量监测需求。目前业内多将信令消息用于DPI话单回填,对于基于5G特有的业务流程交互、5G信令特点进行流量监测的研究较少。因此,研究5G网络场景下的信令流量监测,对发现5G网络威胁及进行威胁溯源,提高5G网络全网安全态势感知能力,有着重要的意义。

2 5G信令流量安全监测技术

不同于传统的NTA流量分析技术,5G信令流量安全监测技术更多基于5G网络的业务特点和5G网络的协议特点去做分析,例如5G网络中N1/N2接口的NGAP协议、N3接口的GTP-U(GPRS Tunnelling Protocol for the User plane)协议、N4接口的PFCP协议等,并根据5G网络用户的特点和业务特点构建流量分析模型,对5G网络的安全监测更有针对性。通过采集5G网络N1(UE-AMF之间接口)、N2(RAN-AMF之间接口)、N4(UPF-SMF之间接口)、N8(AMF-UDM之间接口)、N10(SMF-UDM之间接口)、N11(AMF-SMF之间接口)、N12(AMF-AUSF之间接口)、N14(AMF-AMF之间接口)、N15(AMF-PCF之间接口)、N16(SMF-SMF之间接口)、N22(AMF-NSSF之间接口)、N26(AMF-MME之间接口)、N28(PCF-CHF之间接口)、N29(SMF-NEF之间接口)、N32(SEPP-SEPP之间接口)、N33(AF-NEF之间接口)、N40(SMF-CHF之间接口)等信令交互接口的原始流量,运用大数据、机器学习

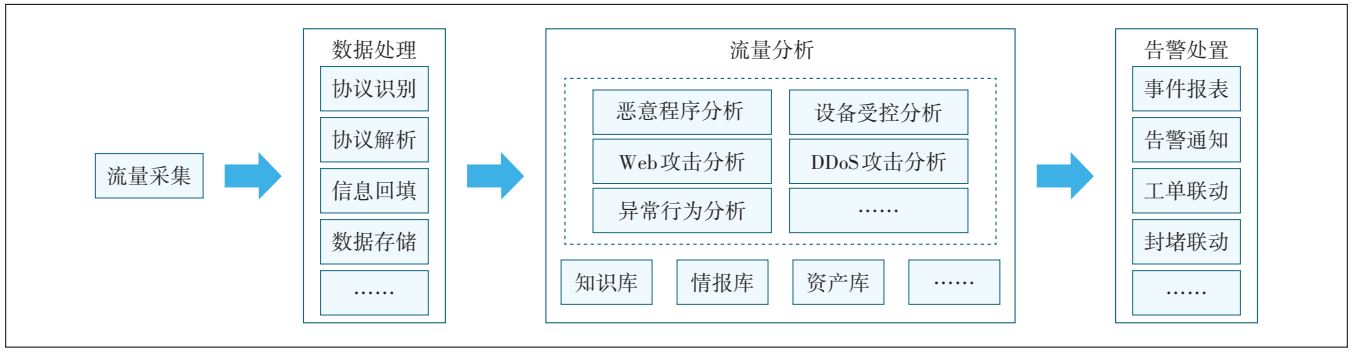

图1 传统流量安全监测流程

算法，按不同应用协议识别处理、解析、还原和分析流量，对网络安全事件进行深度挖掘，从而分析网元间信令攻击和可能遭受的网络攻击事件，对网络安全态势做出评估；并结合5G专网用户特点和行为特征，识别异常终端设备，从而有效管控终端。

2.1 技术架构

5G网络流量安全监测的技术架构如图2所示。数据源为5G网络中N1、N2、N4、N8、N10、N11、N12、N14、N15、N16、N22、N26、N28、N29、N32、N33、N40等接口的信令流量，涵盖NGAP、PFCP、HTTP2、GTP等各类协议。数据采集解析包括流量采集、信息回填、协议识别、数据分类、数据存储等，将采集的原始流量解析处理成全接口统计话单日志、N1N2话单日志、N4话单日志、异常XDR话单日志等，向上提供给信令流量监测分析使用。信令流量监测结合5G网络特点及其流量特征，根据安全模型对信令面流量进行异常流量检测与分析，包括异常终端监测、网元非法接入监测、信令风暴监测、异常信令监测、异常服务网元监测等。

2.2 关键特性

5G信令流量安全监测关键特性可分为异常终端监测、网元非法接入监测、信令风暴监测、异常信令监测和异常服务网元监测这五大特性。

2.2.1 异常终端监测

5G网络中的终端数量巨大、类型多样，一些物联网终端性能较低，安全防护能力弱，面临着被黑客劫持从而攻击网络的风险。例如5G网络中非法终端频繁地发起注册请求，但是由于鉴权流程不通过导致注册失败，凭空浪费大量的无线及网络资源；一部分合法终端可能因为自身或被黑客控制等原因反复进行开关机、周期性地发送大量信令、反复切换等行为，浪费网络资源。

基于N1、N2接口的信令流量，通过对注册流程的检测和解析，识别来历不明的非法终端，监测频繁发起网络接入用户、频繁开关机用户、频繁发起连接业务请求用户、信令交互量过大用户、频繁发起5G内切换用户、频繁发起4G/5G切换用户等；通过解析终端接入切片的信令消息，识别试图接入非本终端签约切片的异常终端行为，为运营商及行业客户提供发现异常终端的运维手段。

2.2.2 非法网元接入监测

5G网络为了给垂直行业客户提供低时延、更个性化的服务，将网络能力和计算能力延伸到了网络边缘和用户边缘，但是下沉的UPF网元更靠近用户侧，增加了网络的暴露面，网元更容易被攻击者控制和仿冒。为了监测和防范此风险，针对非运营商登记资产进行监控，通过信令流量数据解析，主动探测5G网络中的各网元，及时发现不属于5G网络的基站、UPF等非法网元，避免攻击者仿冒5G网元向运营商网络及业务平台发动攻击。

2.2.3 信令风暴监测

5G网络中大量终端接入网络时将产生大量的接入信令，尤其是大量物联网用户同时开机接入网络时会产生大量接入网络请求，一旦网络收到的终端信令请求超过了网络各项信令资源的处理能力，将会引发网络拥塞以至于产生雪崩效应，导致网络不可用。依据关键信令访问量构建信令风暴模型，根据对N1N2话单的注册流程、SR（Service Request）流程、PDU（Packet Data Unit）建立流程以及N4话单的会话流程和PFCP节点类信令流程的统计分析，监测5G网元维度的信令负荷情况，发现基站、AMF、SMF等关键网元

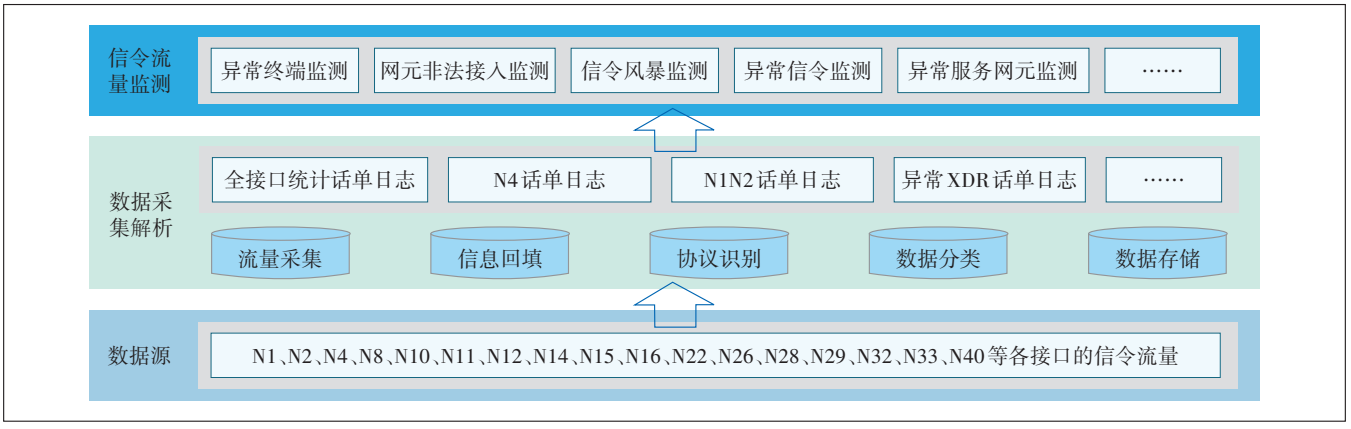

图2　5G网络信令流量安全监测技术架构

的信令风暴,预警空口信令风暴攻击行为,避免5G网元被攻击,影响客户网络质量和业务正常运行。

2.2.4 异常信令监测

由于5G网络承载的业务重要性越来越高,对于黑客的吸引力也越来越大,攻击者的攻击能力和攻击手段在不断更新提升,要防止攻击者通过构造畸形消息、异常方向攻击引发5G网络设备处理异常,影响客户网络服务和业务运行。通过对5G网络信令流量的解析识别,根据各接口双向的信令消息进行智能关联分析,发现交互过程中的协议异常、格式异常、方向异常、服务异常等行为,综合判定疑似受攻击的用户及5G网元,识别通过构造异常信令等方式发起信令攻击的威胁。

2.2.5 异常服务网元监测

5G网络中的物联网终端、行业客户的专网终端的位置较为固定,因此为其提供服务的AMF、SMF、UPF、gNB等网元也相对固定。考虑专网用户的部署特点,通过监测信令流量中为固定位置终端提供服务的网元,可及时发现网元异常变更行为,从而进一步挖掘出可能受到攻击的5G网元。

2.3 部署应用

5G信令流量安全监测的适用场景广泛,通过交换机镜像或者分光器复制5G网络信令流量的方式,将网络流量引流后进行分析监测,可实时、快速地监测到第2.2节提到的异常终端、非法网元接入、信令风暴、异常信令、异常服务网元等各类网络安全威胁。一方面可以为运营商提供网络安全监测态势预警,另一方面可以使行业客户及时发现异常行为的终端,从而提升发现5G网络威胁和态势感知的能力。图3给出了5G信令流量安全监测的部署应用示意。

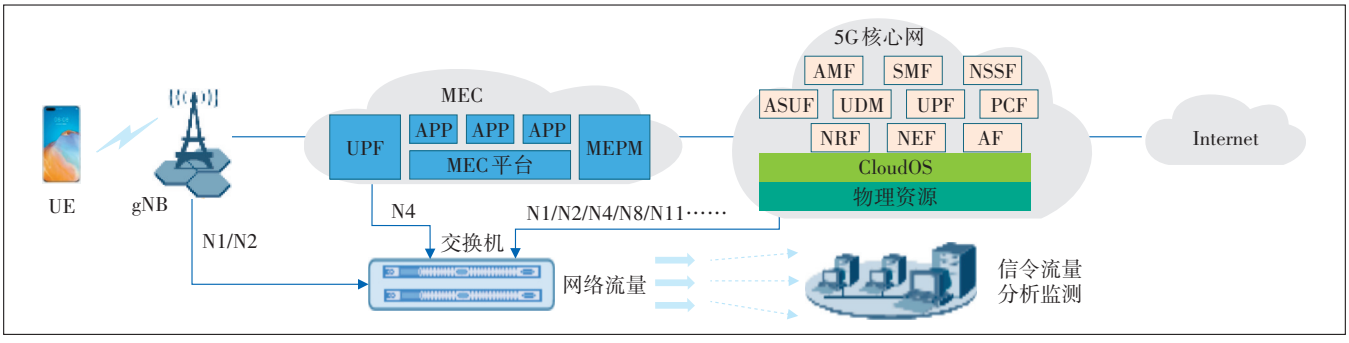

图3 部署应用示意

3 结束语

本文梳理了现有的流量安全监测技术及其应用场景,并对信令流量安全监测技术架构和关键特性进行了介绍,通过加强5G网络信令面流量的识别和解析能力,能够有效扩充对于信令攻击的威胁发现能力、拓展5G安全监测的维度。根据信令流量的静态特征和动态特性,运用大数据及智能检测技术,主动监测5G信令交互异常并进行深度挖掘和评估,对可能遭受的信令攻击和终端异常等事件进行预警,充分考虑了行业用户和专网用户的行为特点,切实满足了行业客户和5G专网对于全流量检测和态势感知的需求,有助于全面掌握5G网络的安全态势,打造更加安全的5G网络。

参考文献:

[1] 何丽华,王少波,程玉松,等. 2G/4G/5G核心网融合组网架构下信令监测系统建设思路研究[J]. 数据通信,2021(3):26-28.

[2] 中国信息通信研究院,FreeBuf咨询. 中国网络流量监测与分析产品研究报告(2020年)[EB/OL]. [2023-05-04]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202009/P020200929395414861521.pdf.

[3] 程定国,曾浩洋. 无线通信网络中流量分析技术综述[J]. 电讯技术,2023,63(3):441-447.

[4] 王陈喜. 基于网络全流量行为分析的异常威胁检测[C]//2022年西湖论剑·网络安全大会——数字城市安全治理论坛论文集. 杭州:《信息安全研究》杂志社,2022:105-107.

[5] 周耀胜. 网络流量分析技术的应用及方案比较[J]. 现代电信科技,2009,39(7):62-67.

[6] 王涛,潘乐荣,邹初建. 5G场景下的全流量安全检测与分析[C]//2022年网络安全优秀创新成果大赛论文集. 北京:《信息安全研究》杂志社,2022:66-69.

作者简介:

郑涛,工程师,硕士,主要从事网络与信息安全管理工作;谢泽铖,工程师,硕士,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;陆勰,工程师,硕士,主要从事网络与信息安全研究工作;王姗姗,工程师,博士,主要从事网络与信息安全研究工作。