研究与开发

基于图数据库的 5G 数据流转安全防护机制

粟栗，陆黎，张星，刘畅
（中国移动通信有限公司研究院，北京 100032）

摘　要：5G 网络与关乎国计民生的政务、医疗、金融等行业紧密融合，5G 网络所承载数据的安全性至关重要。首先对 5G 数据及流转场景进行了分析，然后对 5G 数据进行分类分级；结合数据全生命周期防护要求，创新提出了一种基于图数据库的 5G 数据安全标记模型，能同时满足静态分类分级与动态流转防护的需求。以该模型为基础，从节点自身安全、数据流转监控及数据安全风险处置 3 个方面构建了 5G 数据安全防护机制，实现了对 5G 数据的全生命周期防护。

关键词：5G 安全；数据安全；数据流转；数据分类；安全模型
中图分类号：TP399
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021058

Graph database based security protection mechanism of 5G network data flow

SU Li, LU Li, ZHANG Xing, LIU Chang
China Mobile Research Institute, Beijing 100032, China

Abstract: As the 5G mobile network is closely integrated with government, medical, financial and other industries related to national economy and people's livelihood, the security of the data carried by 5G network is crucial. 5G data and flow scenarios were firstly analyzed, then 5G data was classified. Combining with the protection requirements of the life cycle of data, an innovative 5G data security labeling model based on graph database was proposed, which could meet the protection requirements of static classification and dynamic flow simultaneously. Based on this model, 5G data security protection mechanism was constructed from three aspects of node security, data flow monitoring and data security risk disposal, realizing life-cycle protection of 5G data.

Key words: 5G security, data security, data flow, data category, security model

1　引言

5G 作为赋能各行业数字化转型、促进商业模式创新和经济发展的新型信息化关键基础设施，5G 数据的安全具有重要的意义。首先，随着网络数据量的激增、数据应用的蓬勃发展，数据安全已成为个人用户、行业用户乃至国家政府共同关注的重要问题，国家发布了系列法律加强数据安全监管，5G 作为我国“新基建”之首，其数据安全不仅关乎运营商数据合规性，更影响着国家的

收稿日期：2020−09−27；修回日期：2021−04−03

安全。其次，5G 网络具备高速率、低时延、大连接的特性[1]，为电力能源、交通运输及工业制造等垂直行业的广泛接入提供了条件，进一步促进了网络与业务的融合，也使得 5G 数据的安全与经济安全紧密相关。

5G 网络采用全新的 SBA（service based architecture，基于服务的架构），引入了网络功能虚拟化、网络切片、边缘计算等新技术，并将传统的人与人通信能力扩展到物与物之间[2]，在大幅提升移动通信网业务能力的同时，也让 5G 数据安全面临一些新的挑战：一是海量数据种类多、保护难度大；二是数据流转场景复杂加大安全防护复杂度；三是新技术引入带来潜在安全风险[3]。

参考文献[4]提出了 5G 数据的技术和管理手段，但主要针对用户数据的隐私安全。参考文献[5]主要针对电信云自身的安全，提出 5G 虚拟化平台中的数据安全机制。参考文献[6]主要讨论了 5G 网络中可能的漏洞，并针对漏洞提出相应解决办法。参考文献[7]根据数据的机密性、完整性及可用性被破坏后产生的影响对数据分类，主要通过不同级别的加密方式保护虚拟化网络中的重要数据。参考文献[8]主要描述了 5G 安全架构和 5G 主要安全问题，以及对应解决方案。

考虑 5G 数据的动态流转特性以及巨大的数据量和复杂的数据安全挑战，仅对已识别出的 5G 网络漏洞和安全问题设计解决方案，不足以维护数据全流程的安全，要对所有数据施加高安全级别的保护并屏蔽所有风险也是不切实际的[9]，所以要更加系统地识别、分析 5G 中的各类数据，并制定对应的防护措施。因此，对于 5G 网络涉及的各类数据，需要进行如下分析：一识别数据，确定数据类型与重要性；二识别数据的流转过程，明确数据流转场景；三结合数据生命周期制定防护措施。本文提出一种基于图数据库的数据安全标记模型，在 5G 数据分类分级的基础上，创新结合数据流转与操作的特性，形成四维向量模型。基于图数据库进行分析，可对网络数据进行全生命周期管理，并最终形成全程全网的安全防护机制。

2　5G 数据安全需求

为了分析 5G 数据安全，必须首先识别 5G 数据，即对 5G 数据进行分类分级，识别不同数据类型的安全保护需求，确定针对不同级别数据的基本安全防护措施。

2.1　5G 网络关键数据

在 5G 网络中，涉及多种类型的数据，基于 ITU-T X.805[10]的定义，可以将其映射到控制平面、用户平面、管理平面。在本文中，控制平面数据包括实现网元之间的信息通信活动以及为用户提供适当服务所必需的数据；用户平面数据包括 5G 用户访问和使用 5G 网络而产生的实际用户数据流；管理平面数据包括网元及切片生命周期管理、操作维护管理涉及的数据。3 个平面的主要数据示例见表 1[11-20]。

表 1　主要数据示例

数据平面	数据种类
控制平面	用户标识、鉴权数据、计费数据、签约数据、UE 上下文、位置信息、切片信息、会话管理数据、策略数据、NF 配置数据等
管理平面	日志、网管接口认证数据、网元状态监控数据、与 VNF 相关信息、与 MANO 相关信息、NFV 管理编排信息、与切片相关信息、与切片管理系统相关信息、切片管理编排信息等
用户平面	互联网应用数据（即时通信内容、用户上网访问内容等）、电信服务数据（语音、短消息等）、切片业务数据、边缘计算业务数据等

2.2 5G 数据安全防护需求

3 个平面数据及每个平面细分数据种类因泄露或遭到篡改、破坏后，受到的不良影响程度不同，从而数据的安全需求也不一样。安全防护级别与防护需求相匹配，可降低安全防护成本，实现安全性与实施成本之间的平衡。《信息安全技术 大数据安全管理指南》[21]对电信行业数据分类分级进行了示例，参考标准中的数据分类分级，本文将 5G 数据安全防护等级分为 4 级、10 个子类；安全防护需求随级别升高而递增，每个安全防护等级包含一个或多个子类，每个子类下是属于 3 个平面的细分数据类型，见表 2。“√”表示 3 个数据平面各包含的数据类型。

表 2 5G 数据分类分级

等级	子类及范围	控制平面	用户平面	管理平面
第 4 级	网络设备及 IT 系统密码及关联信息	√		√
	用户密码及关联信息	√		
	核心网络设备及 IT 系统资源类数据	√		√
第 3 级	服务记录和日志信息	√		√
	服务内容和资料数据		√	
	位置数据	√	√	
	用户网络身份标识数据	√		
第 2 级	终端设备标识和资料	√		
	消费信息和账单	√	√	
第 1 级	业务订购关系	√		

第 1 级数据是业务订购关系，安全防护需求最低，在 5G 网络关键数据中业务订购关系指用户的签约数据。第 2 级数据一方面是终端的资料和标识，另一方面是用户的消费数据，分别包含终端标识、终端能力、终端配置等终端的数据，以及计费信息等用户消费记录。第 3 级数据的 4 个子类从上至下分别对应：（1）UE（user equipment，用户设备）上下文、会话管理数据等与用户服务紧密相关的控制平面数据及网元生成的操作日志、系统日志等服务记录和各类日志信息；（2）用户服务内容和资料数据；（3）用户位置数据；（4）用户网络身份标识数据。第 4 级数据包含的 3 个子类从上至下分别对应：（1）网元及管理系统的认证、密钥、账号数据；（2）用户的鉴权数据；（3）切片配置、运营状态监控信息等与 5G 设备及系统资源相关数据。由于 5G 会接入大量行业用户，可能涉及安全防护需求极高的用户数据，安全防护等级会超越目前最高的“第 4 级”，本文暂不讨论该类型特殊数据。

2.3 5G 数据生命周期安全防护

不同级别数据在生命周期各阶段均存在安全需求。根据相关标准[22]定义，本文将 5G 数据生命周期分为数据采集、数据传输、数据存储、数据处理、数据销毁阶段。本文综合数据安全防护等级及通信行业标准等技术要求，定义了 4 级 5G 数据安全防护等级对应的生命周期基本防护措施，见表 3，其中每级安全防护措施均在下一级基础上增强。

3 5G 数据流转分析

每个平面的数据根据既定的机制和规则在不同网元、设备或系统间流转。控制面数据种类多、流转场景复杂，用户发起业务或位置变动、网元业务活动等均会触发数据流转。根据控制平面数据在流转过程中传输通道两端设备所属网络域不同，5G 控制平面数据流转可包含多种场景[10]。控制平面数据流转如图 1 所示。

用户数据主要在终端、基站、UPF（user plane function，用户平面功能）与外部数据网络之间传递，对于边缘计算场景，用户数据可从分流 UPF 直接卸载到边缘计算节点或从基站直接接入边缘计算平台。用户平面数据流转如图 1 所示。管理数据主要在网元、网管、MANO（management and orchestration，管理和编排）[17]和切片管理系统内部及系统间流转，并可能与第三方平台及业务支撑系统间交互[17-20]。管理平面数据流转如图 2 所示。

表 3　数据安全防护等级与安全措施对应

安全防护等级	数据采集	数据传输	数据存储	数据处理	数据销毁
第 4 级	错误、问题数据识别	完整性检测恢复机制	完整性检测恢复机制及访问控制机制强度粒度增强	细粒度权限控制；实时监测告警；数据关联、挖掘风险分析	彻底销毁不可恢复
第 3 级	接入鉴权；认证鉴权	完整性机制	更细粒度的访问控制和完整性机制	更严格的认证及行为监测	
第 2 级	异常行为记录告警	机密性、可靠性	机密性及访问控制	认证、异常行为记录和告警	
第 1 级	—	—	访问控制	—	—

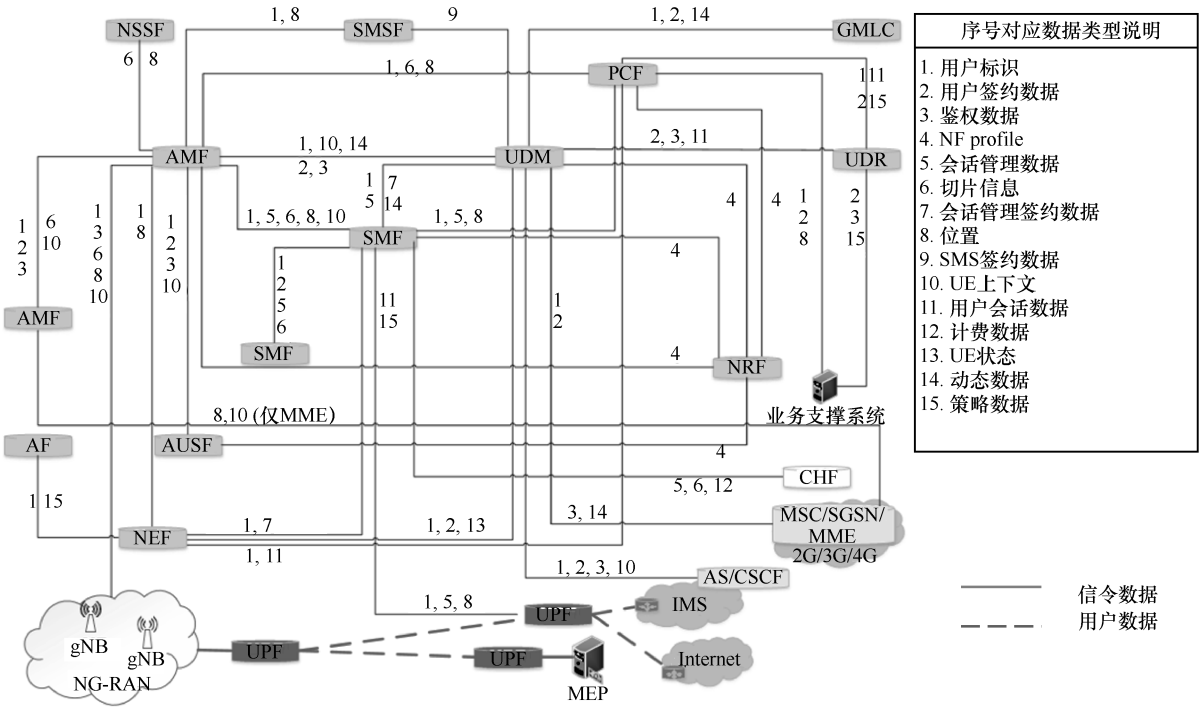

图 1　5G 数据流转（图中仅画出主要流转关系）

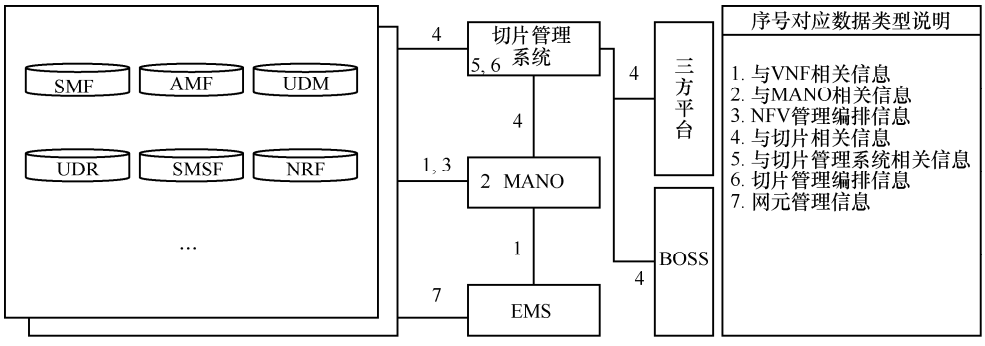

图 2　5G 管理数据流转

4　基于图数据库的 5G 数据安全模型

5G 数据种类多样且存在复杂的流转场景，仅依靠数据防护等级与安全机制的映射无法满足运营商数据安全保护需求[23]。5G 数据安全防护需要考虑多样化的数据流动、复杂的数据操作等情况，

并最终落地到网络节点或专门的安全设备。本文提出一种基于图数据库的安全模型，基于该安全模型能够建立细粒度、动态的 5G 数据安全体系，为动态流转的 5G 数据提供有效的安全保障。

4.1 基本结构

本文提出的 5G 数据安全模型以 5G 网络中的主要网络功能或系统组件为节点，节点功能名称作为节点标签，节点中的数据类型及可对该数据执行的操作作为节点属性，如 [数据类型，数据操作]。两两节点间数据流向及节点之间的操作作为节点间的有向边，边属性分别为传输的数据类型以及数据操作与数据类型值对。此安全模型抽象出包括网络节点、数据种类、数据操作以及数据流向 4 种主要元素在内的 5G 全网数据流转图谱。5G 数据安全模型基本结构如图 3 所示。

图谱中网络节点具体包括 5G 网元、网管系统各组件、MANO 各组件、切片管理系统各组件。节点对数据的操作包括采集（含导入、配置等）、存储、处理（包括修改、计算、查询、导出等）、删除、转发。如 UDM（unified data management，统一数据管理）网元主要涉及用户标识、用户鉴权、签约、UE 上下文数据，对用户标识、用户鉴权、签约数据可执行的操作一般包括采集、存储、处理、转发、删除，对 UE 上下文可执行的操作一般包括存储、转发、删除，则 UDM 节点属性包含[用户标识，（采集、存储、处理、转发、删除）]、[用户签约数据，（采集、存储、处理、转发、删除）]、[用户鉴权，（采集、存储、处理、转发、删除）]及[UE 上下文，（存储、转发、删除）]属性值。节点之间每传递一种数据，节点间就增加一条有向边，边属性即传递的数据类型；节点间每进行一种数据操作，节点间同样增加一条有向边，边属性为数据操作及操作的相应数据类型。

4.2 构建过程

根据已有数据节点备案信息、数据分类分析结果及数据流转知识可以建立静态的 5G 全网安全模型，该模型不包含属性为数据操作及数据类型的边，仅根据 5G 数据流转场景构建节点间静态数据流转关系，参考图 1 及图 2 中节点间的连接关系。但是 5G 网络是动态变化的，静态的模型难以满足动态网络安全需求，本文通过对网络数据的采集及实时分析，形成与网络当前场景相匹配的，基于图数据库的全网动态安全模型。动态安全模型构建过程如下。

（1）网络节点发现：首先采用资产发现技术对专网中节点进行扫描，自动发现网络节点，将节点 IP 地址及相关信息导入图数据库，建立安全

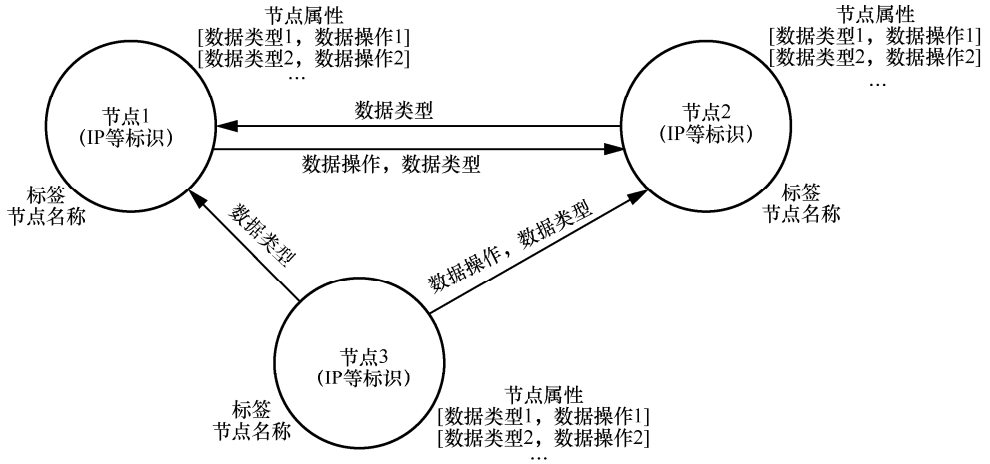

图 3　5G 数据安全模型基本结构

模型主体架构。其次，将 IP 地址与 MANO 中 VNF（virtual network function，虚拟化网络功能）IP 地址及运营商资产备案信息进行比对，获得 IP 地址对应的网络功能名称，如 UDM、AMF（access and mobility function，接入和移动管理功能）等，为节点打上标签。节点属性按照自定义的规则自动导入。

（2）网络数据采集：实时采集 5G 网络中的数据。采集的方式主要包括在网络功能部署软采模块，由软采模块主动上报数据；在路由器或交换机部署分光设备或通过镜像方式外置采集数据。采集的数据内容主要包括网络节点间的数据流量，至少包含业务触发后网元间传递的信令数据、网元与管理组件间的管理数据以及网络节点实时生成的操作日志、系统日志。

（3）5G 关键数据自动识别：采用数据自动识别技术识别 5G 关键数据。识别方法主要包括根据 5G 各数据类型的特点，构造正则表达式，通过字符串匹配自动识别数据；建立 5G 关键数据词库，将待检测内容与词库中关键词进行比对。

（4）数据流量分析：对采集数据进行实时分析，针对节点间数据流量，自动识别出关键数据后，定位传递数据的两个节点，并将数据流向和数据类型作为动态安全模型中节点间的有向边及边属性导入图数据库；针对节点间的数据操作指令及节点实时生成的日志信息，分析识别任意两个节点间的数据操作及操作的数据类型，将两个节点间的操作关系以及数据操作和数据类型再作为动态安全模型节点间的有向边及边属性导入图数据库。

以 AMF 与 SMF 典型流程为例，节点构建过程包括如下步骤。

步骤 1　给定 IP 专网网段，基于 Nmap 或更先进的技术扫描网络中在线主机的 IP 地址，将 IP 地址导入图数据库。

步骤 2　将 IP 地址与运营商资产列表比对，通过不同 IP 地址分别映射出 AMF 与 SMF 节点，并作为节点标签导入图数据库。

步骤 3　UE 发起 PDU 会话建立流程，AMF 与 SMF 之间传递用户永久身份标识（subscriber permanent identifier，SUPI），相关信令被采集至专门设备。

步骤 4　通过数据识别和分析，确定用户标识由 AMF 传递至 SMF，形成一条由 AMF 至 SMF 的有向边，边属性为用户标识，导入图数据库。

同样以 AMF 与 SMF 为例说明数据更新过程。当通过对采集的数据做实时分析，发现两个节点之间传递了新的数据类型或数据操作，则在节点间增加一条边，完成数据的更新。如果传递的数据类型或操作已经存在，则不增加新的边。

4.3　安全架构

基于安全模型，本文将 5G 数据安全架构划分为“节点”的数据安全和“边”的数据安全两个部分。

（1）节点数据安全

节点安全由节点自身安全机制保障。需要结合数据操作及数据安全防护等级制定节点安全机制，针对节点中数据的不同安全需求提供细粒度、差异化安全保护。

（2）边的数据安全

“边”包含两个含义，一是节点间的数据流动，二是节点间的数据操作。针对动态的“边”，需要从两个维度构建安全能力，分别是对正常状态的监控以及异常情况发生后的预警和处置。

5　基于安全模型的 5G 数据安全防护体系

基于安全模型及模型中定义的 5G 数据安全架构，本文从节点自身安全防护、数据流转的监控预警及数据安全风险处置 3 个方面构建 5G 数据安全防护体系。

5.1　节点自身安全防护

本文以满足数据的不同安全防护需求为目标，设计节点的差异化安全防护框架。首先将表 3

中的数据生命周期分别映射到安全模型中网络节点的数据采集、转发、存储、处理、删除操作，然后将不同数据安全防护等级的安全需求对应到节点数据操作中。节点安全即由节点能够对数据执行的操作以及相应操作涉及的最高数据安全防护等级决定。具体如下。

根据节点属性，得到节点涉及数据操作，针对每一类操作：（1）获取操作的数据类型，并根据数据类型映射数据安全防护等级；（2）根据数据安全防护等级与安全措施的对应关系，得到本操作涉及数据类型的最高安全防护等级，将该操作的安全措施作为本节点此类操作的安全措施。节点中不同操作类型的安全措施合集即节点安全措施。例如，某节点涉及的数据操作包括转发、存储、删除，操作涉及的数据最高安全防护等级分别为 4、2、4，则该节点转发、存储、删除的安全能力应分别符合第 4 级数据的传输安全、第 2 级数据的存储安全及第 4 级数据的销毁安全要求。网络节点中节点属性变更，即数据类型或数据操作权限变更后，安全需求也会相应变更，节点的安全机制随之加强或减弱。

5.2 数据流转监控预警

基于动态的 5G 安全模型，能够对网络中的数据及数据流转、操作情况进行实时监控，及时发现数据安全风险并做出反应，主动消除风险。

（1）关键数据资产监控

利用数据自动识别技术对 5G 全网关键数据进行扫描，可获得每个网络节点中实际存储的关键数据类型，展现全网关键数据分布。将静态模型节点属性中的数据类型作为网络节点数据类型基准，对比实时扫描得到的每个节点中存储的数据，当发现网络节点中出现基准范围外的数据，进行告警，由管理员手动执行或系统按策略自动执行销毁或数据迁移等操作。

（2）数据异常流转监控

5G 网络节点间数据总是按照一定的规则进行传输，每两个节点间可触发的流程是确定的，流程可携带的数据范围也是确定的。以静态模型中边及边属性为基准，分析动态模型中网络节点间传递的数据类型，对于不符合基准，即两节点传输不符合规则数据的情况，进行告警。网络依据策略执行阻断等操作，及时消除风险。

（3）异常数据操作监控

对网络节点间数据操作情况进行分析，建立异常数据操作模型，对于偏离模型的行为进行监控预警，并进行风险预判。同时基于聚类分析等机器学习算法，对主要节点行为进行画像，建立节点特征画像图谱，并对节点的实时操作和特征画像图谱进行比对，发现异常行为。对于预判的危险行为及发现的异常行为，进行告警。

5.3 数据安全风险处置

5G 安全模型是动态网络的抽象呈现，展现了数据在网络中而非单个节点的流转过程，基于模型的数据安全风险处置能力至少包括以下两点。

（1）数据泄露节点定位

5G 网络中数据可能在同一物理服务器内部的几个节点间流转，如果数据在服务器内部泄露，则部署在服务器中的节点均为潜在攻击者。例如用户位置数据会在多个流程中于多种网元间传递，可能的泄露点众多，难以有效分析识别出数据泄露点。如果发生数据泄露事件，依据动态模型中记录的边属性（节点间传输的数据类型），能够排除网络中大量无关节点，快速识别数据流转路径。通过对流转路径中各节点进行风险排查，可快速定位数据泄露点，阻断数据泄露源。

（2）被攻击节点定位

当在某个节点发现数据被篡改时，存在两种情况：（1）数据在当前节点被篡改；（2）数据在流转到当前节点前已经被篡改。根据动态安全模型还原数据流转路径，并结合路径中每个节点的数据修改操作，能够定位出发生数据篡改的节点，然后对节点进行修复和安全加固。

6　实验和评估

本文提出的 5G 数据安全防护体系实现的基础主要是安全模型的构建，其主要部分为数据的获取和识别分析，本文设计了简化的原型系统实现该部分功能，并对系统性能进行了测试和评估，以说明系统在实际场景中的可实现性。

6.1　实验设置和结果

实验设备均采用配备 8CPU Intel 处理器、32 GB RAM 的机器。基于现网模拟数据，在实验环境下进行分析、实验与仿真计算。经过测试，平均每台机器解析数据量的性能如图 4 所示，机器解析效率基本稳定在 450 MB/s。

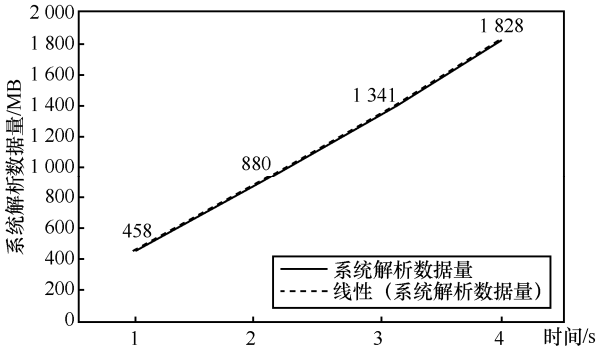

图 4　测试结果

6.2　性能评估

本实验未包括数据采集部分，并且因为实验室环境中难以模拟在大型 5G 网络中采集数据的真实环境，实验室测试结果也难以作为参照。本文选择以已建设的运营商数据采集网络为参照，其采集方式包括分光镜像等方式，采集内容包括运营商网络中大量控制和管理数据，采集传输时延能够达到百毫秒级，数据完整性可达 99%。本文提出的安全模型数据采集过程和采集内容与该系统类似，基于其数据采集的经验，理论上可保证本文所述数据采集的时延和完整性。

另外，根据实验结果，本实验系统解析效率基本保持线性增长，处理性能基本稳定在 450 MB/s 即 3.5 Gbit/s。由于 5G 网络节点众多，数据量较大，可采用多进程高并发的方式，为每个节点间数据接口单独设置处理模块，首先按接口对数据进行分拣，然后不同接口数据送至不同模块，并行进行数据分析处理，理论上可实现数据并发处理量随机器数量线性增长。

依据上述理论分析及实验室测试结果，按照采集的 5G 数据流量为 100 Gbit/s 计算，可搭建包含 20 余台处理节点的环境进行数据处理。但依据处理环节进行分析，评估在 5G 网络中实际应用的处理性能可能降为现有实验室测试性能的 80%左右，所需计算资源会同步增长。通过提高机器配置或进一步优化算法的方式能够减少机器数量。

7　结束语

随着信息技术水平及社会数字化程度的提升，数据将向着数量快速增长、数据流转融合更加频繁的方向发展，《中华人民共和国数据安全法（草案）》的发布也将更加促进数据的安全与发展。在数据保护方面，必须结合数据的发展趋势及特点，设计针对海量及流转数据的动态灵活的安全保护措施，才能有效提供数据安全保障能力。5G 数据既是典型的动态流转数据，同时又具备数据量大、数据安全保护需求高的特点，需要结合动态流转、静态分类分级两方面考虑数据安全防护。本文首次提出了 5G 数据分类方法与数据流转图，并设计了基于图数据库的 5G 数据安全模型，在安全模型的基础上提出与数据操作、数据流转相结合的 5G 数据安全解决方法，能够有效保障动态数据安全性。本文提出的 5G 数据安全模型及数据保护思路对动态数据安全保护具有很好的借鉴意义，基于安全模型能够进一步探索数据安全机制，完善数据流转安全体系。

参考文献：

[1] ITU-R. IMT vision–framework and overall objectives of the future development of IMT for 2020 and beyond: M.2083-0[S]. 2015.

[2] 黄宇红, 王晓云, 刘光毅. 5G 移动通信系统概述[J]. 电子技术应用, 2017, 43(8): 3-7.
HUANG Y H, WANG X Y, LIU G Y. Overview of 5G mobile communication system[J]. Application of Electronic Technique, 2017, 43(8): 3-7.

[3] 张鉴, 唐洪玉, 刘文韬, 等. 面向云网融合的电信网安全防护体系参考架构[J]. 电信科学, 2020, 36(5): 10-15.
ZHANG J, TANG H Y, LIU W T, et al. Reference architecture of the telecom network security protection system for cloud network convergence[J]. Telecommunications Science, 2020, 36(5): 10-15.

[4] 方琰崴. 5G 核心网安全解决方案[J]. 移动通信, 2019, 43(10): 19-25.
FANG Y W. 5G core network security solution[J]. Mobile Communications, 2019, 43(10): 19-25.

[5] 王全, 方琰崴. 5G 电信云网络安全解决方案[J]. 邮电设计技术, 2018, 513(11): 63-68.
WANG Q, FANG Y W. Security solution in 5G cloud core network[J]. Designing Techniques of Posts and Telecommunications, 2018, 513(11): 63-68.

[6] HASNAT M A, RURNEE S T A, RAZZAQUE M A, et al. Security study of 5G heterogeneous network: current solutions, limitations & future direction[C]//Proceedings of 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). [S.l.:s.n.], 2019.

[7] SINGH K P, RISHIWAL V, KUMAR P. Classification of data to enhance data security in cloud computing[C]//Proceedings of 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU). [S.l.:s.n.], 2018.

[8] AHMAD I, SHAHABUDDIN S, KUMAR T, et al. Security for 5G and beyond[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3682-3722.

[9] 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): 1813-1825.
FENG D G, XU J, LAN X. Study on 5G mobile communication network security[J]. Journal of Software, 2018, 29(6): 1813-1825.

[10] ITU-T 805.Securityarchitectureforsystemsprovidingend-to- end communications[S]. 2003.

[11] 3GPP. System architecture evolution (SAE); security architecture: TS33.501 V16.0.0[S]. 2019.

[12] 3GPP. System architecture for the 5G system (5GS): TS23. 501 V15.7.0[S]. 2019.

[13] 3GPP. Procedures for the 5G system (5GS): TS23.502V16. 2.0[S]. 2019.

[14] 3GPP. NG general aspects and principles: TS38.410 V16.1.0[S]. 2020.

[15] 3GPP. Technical specification radio access network; NG-RAN; NG layer 1: TS38.411 V15.0.0[S]. 2018.

[16] 3GPP. NG-RAN; NG application protocol (NGAP): TS38. 413 V16.1.0[S]. 2020.

[17] 3GPP. Study on management and orchestration architecture of next generation networks and services: TR28.800 V15.0.0[R]. 2018.

[18] 3GPP. Study on management and orchestration of network slicing for next generation network: TR28.801 V15.1.0[R]. 2018.

[19] 3GPP. Study on management aspects of next generation network architecture and features: TR28.802 V15.0.0[R]. 2018.

[20] 3GPP. Study on management aspects of edge computing: TR28.803 V16.0.1[R]. 2019.

[21] 全国信息安全标准化技术委员会. 信息安全技术 大数据安全管理指南: GB/T 37973-2019[S]. 2019.
National Information Security Sandardization Technical Committee. Information security technology—big data security management guide: GB/T 37973-2019[S]. 2019.

[22] 全国信息安全标准化技术委员会. 数据安全能力成熟度模型: GB/T 37988-2019[S]. 2019.
National Information Security Sandardization Technical Committee. Information security technology—data security capability maturity model: GB/T 37988-2019[S]. 2019.

[23] 赵文, 田永春, 曾浩洋. 5G 安全架构分析[J]. 电讯技术, 2020, 60(8): 876-882.
ZHAO W, TIAN Y C, ZENG H Y. Analysis of 5G security architecture[J]. Telecommunication Engineering, 2020, 60(8): 876-882.

[作者简介]

粟栗（1981− ），男，博士，中国移动通信有限公司研究院安全技术研究所副所长、教授级高级工程师，长期从事移动通信网安全技术研究工作，先后承担多个国家重大专项，累计申请发明专利 50 余项、发表科技论文 20 余篇，曾获得省部级科学技术奖 7 项。

陆黎（1991− ），女，中国移动通信有限公司研究院安全技术研究所网络安全研究员，主要从事移动通信网加密通信及数据安全技术方面的研究工作。

张星（1980− ），男，现就职于中国移动通信有限公司研究院安全技术研究所，长期从事大数据、数据安全等方面的研究工作。

刘畅（1992− ），男，中国移动通信有限公司研究院安全所网络安全研究员，主要从事 5G 通信网络安全技术研究及 5G 安全标准化工作。