

面向 5G mMTC 的网络切片安全研究

徐子钧¹, 刘建伟¹, 李耕^{1,2}

(1. 北京航空航天大学网络空间安全学院, 北京 100191;

2. 国家计算机网络应急技术处理协调中心, 北京 100029)

摘要: 随着 5G 新业务、新架构、新技术的不断出现, 其中的安全问题和潜在安全风险正受到越来越多研究人员的重视。海量机器类通信是 5G 三大应用场景之一, 在提供“大连接、低功耗”等高性能的同时, 由于 MTC 设备资源受限等, 可能弱化 5G 网络的安全性。与此同时, 不同场景和应用领域对网络性能、服务质量、安全等级均有较为明显的差异化需求。网络切片技术的引入, 适应了 5G 组网的灵活性, 满足了 5G 网络为用户提供服务的多样性、定制化, 也带来了新的安全威胁。5G 商用发展迅猛, 物联网设备数量成指数倍增加。为确保 5G 网络提供更加高效安全的按需服务, 针对 5G mMTC 应用场景, 对网络切片安全机制和安全策略的研究尤为重要。因此, 详细分析了 5G mMTC 具有的特点及安全需求, 并列举分析了网络切片主要的安全威胁。结合上述安全需求和安全威胁, 围绕特定网络切片认证、切片安全隔离、安全管理和编排等方面, 总结并阐述了相关现有安全策略方案的贡献和不足, 并对未来该领域的研究进行了展望。提出了一个基于 SM2 国密算法的 5G mMTC 网络切片二次认证与安全隔离模型。该模型框架通过引入批量认证和预认证机制, 满足了 5G 机器类用户大规模认证的高效性; 通过对不同通信数据分级加密, 实现了 5G mMTC 网络切片间的安全隔离; 并对该模型进行了性能分析和安全性分析。

关键词: 网络切片; 5G mMTC; 安全隔离; 接入认证

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022006

Research on network slicing security for 5G mMTC

XU Zijun¹, LIU Jianwei¹, LI Geng^{1,2}

1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China

2. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

Abstract: With the emergence of new 5G business, architecture and technology, more and more researchers pay attention to security issues and potential security risks. Massive machine type communication is one of the three major application scenarios of 5G. It provides high performance such as large connection and low power

收稿日期: 2021-05-20; 修回日期: 2021-07-08

通信作者: 刘建伟, liujianwei@buaa.edu.cn

基金项目: 国家重点研发计划 (2017YFB1400702); 国家自然科学基金 (61932014, 61972018)

Foundation Items: The National Key R&D Program of China (2017YFB1400702), The Natural Science Foundation of China (61932014, 61972018)

引用格式: 徐子钧, 刘建伟, 李耕. 面向 5G mMTC 的网络切片安全研究[J]. 网络与信息安全学报, 2022, 8(1): 95-105.

Citation Format: XU Z J, LIU J W, LI G. Research on network slicing security for 5G mMTC[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 95-105.

consumption. Due to factors such as limited resources of MTC equipment, it may also weaken the security of 5G networks. At the same time, different scenarios and applications have obvious demands for network performance, service quality and security level. The flexibility of 5G networking is realized by network slicing technology. It meets the diversity and customization of 5G network services, but also brings new security threats. 5G commercial rapid development. The number of IoT devices has increased exponentially. In order to ensure that 5G networks provide more efficient and safe on-demand services, it is particularly important to study the security mechanism and strategy of network slicing for 5G mMTC application scenarios. Therefore, the characteristics and security requirements of 5G mMTC were analyzed. The main security threats of network slicing were listed. In view of the above security requirements and threats, the contribution and deficiency of existing security schemes around the aspects of specific network slice authentication, slice security isolation, security management and arrangement were summarized and expounded. And the future research in this field was prospected. A SM2-based secondary authentication and security isolation model for 5G mMTC network slicing was proposed. This model framework met the efficiency of large-scale authentication for 5G devices and users by introducing batch authentication and pre-authentication mechanisms. By hierarchical encryption of different communication data, the security isolation between 5G mMTC network slices was realized. The performance and security of the model were also analyzed.

Keywords: network slicing, 5G mMTC, safe isolation, access authentication

0 引言

第五代(5G)移动通信技术作为新一代移动通信技术,是支撑万物互联和大规模异构网络通信的关键基础设施。第三代合作伙伴计划(3GPP, 3rd generation partnership project)已经推出 R15、R16、R17 和 R18 这 4 个 5G 规范版本, R15、R16 版本均已冻结, R17 版本预计在 2022 年 9 月完成冻结,在第 46 次 PCG(项目合作组)会议中 3GPP 正式将 5G 演进的名称确定为 5G-Advanced,并将从 R18 版本开始更新^[1]。我国 IMT-2020(5G)推进组顺利完成了第一阶段 5G 网络设备安全测试, 5G 毫米波测试取得新进展。我国 5G 商用两年间,建成 5G 基站 85 万站, 5G 终端连接数 2.8 亿, 5G 套餐用户超 3.5 亿, 5G 专网超 1 000 个, 5G 商用的发展速度远超预期^[2]。“十四五”规划针对 5G 在网络建设、终端数量和应用方面的发展提出了要求和部署,这意味着移动互联网将很快完全进入 5G 时代。

5G 聚焦三大应用场景^[3],分别为增强移动宽带(eMBB, enhanced mobile broadband)、超可靠超低时延通信(uRLLC, ultra reliable and low latency communication)和海量机器类通信(mMTC, massive machine type communications),这意味着 5G 可以提供超高速率,满足

低时延、高可靠性,承载超高密度用户容量,并支持高移动性的需求^[4]。此外,5G 网络呈现终端多样化、节点数量众多、节点超高密度部署、多种无线网络技术和安全机制共存、端到端通信等特点,并且引入了包括网络切片、V2X^[5]、边缘计算、服务化架构(SBA, service based architecture)、控制与用户面分离(CUPS, control and user plane separation)、软件定义网络(SDN, software defined network)和网络功能虚拟化(NFV, network functions virtualization)等多种新技术、新架构。

随着 5G 新业务、新架构、新技术、新应用场景的不断发展,5G 安全面临诸多新挑战。三大应用场景对网络性能、服务质量、安全等级均有着较为明显的差异化需求,这为搭建 5G 网络安全架构提出了更高要求;5G 引入了 SDN 和 NFV 技术,使得控制面和数据面分离,业务开放性、网络资源共享化以及基础设施的集中部署,打破了传统网络域的安全边界,而开源可配置的网络架构会引发更多的安全威胁;为了满足 5G 网络高带宽、海量接入、服务可用性的需求,研究人员提出了新空口理念和包含新编码技术、新多址技术、接入协议在内的新的支撑技术^[6]。5G 网络的灵活性、开放性和异构性,使用户接入认证和访问控制更加灵活,安全需求更高。

1 5G mMTC 的特点及安全需求

1.1 5G mMTC 应用场景的特点

作为 5G 三大应用场景之一, mMTC 具备“大连接、低功耗”网络性能, 以传感和数据采集为目标。mMTC 要求支持每平方千米 100 万个设备的高连接密度, 这是 4G 最大连接密度的 10 倍^[7]。

5G mMTC 应用场景覆盖政务与公用事业、工业、农业、交通运输、电力等行业, 支持智慧城市、智慧环保、智能制造、智慧农场、智慧交通、智慧物流、智慧用电等应用领域服务, 如图 1 所示。为应对 5G mMTC 场景的需求, 3GPP 提出了两种关键支撑技术——窄带物联网 (NB-IoT, narrow band internet of things) 技术和增强机器类型通信 (eMTC, enhanced MTC) 技术, 主要为具有资源受限、低速率、超低成本、低功耗、广深覆盖、大连接需求的物联网业务提供服务支持。5G mMTC 应用场景覆盖领域广、接入设备数量巨大、业务种类多, 主要有支持小数据包收发、超低功耗和超低成本、海量连接、高效的轻量级通信等特点。

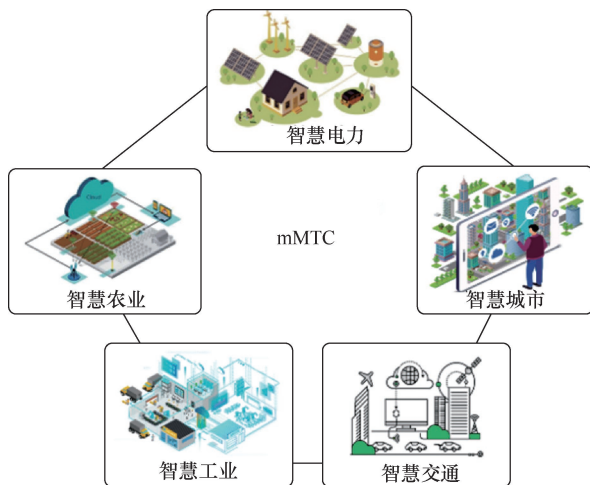


图 1 5G mMTC 应用场景
Figure 1 5G mMTC scenario

1.2 5G mMTC 应用场景下的安全需求

海量终端并发接入网络极有可能产生信令风暴, 造成网络拥塞, 大多数设备存储计算资源有限, 拓扑结构多样化, 信息交互以数据为中心, 与应用程序紧密关联。海量终端对各类移动应用程序的使用所带来的如周期性心跳消息、重启动

等大规模小数据量的频繁交互, 会大量消耗信令信道资源, 导致信令量的增幅远大于业务流量的增幅, 这就容易同时造成移动基站与核心网的信令过载, 使移动网络很容易出现服务严重超时、降级或设备直接宕机瘫痪的情况。因此, 如果没有建立小数据传送的安全通道, 攻击者将会通过访问小数据接口, 加速终端设备的功耗, 威胁 5G 网络系统的安全性能。因此, mMTC 应用场景下的 5G 网络更容易受到威胁和攻击。现有的标准和相关研究主要针对 5G 物联网系统的架构、性能和服务质量方面^[8], 对 5G mMTC 应用场景下安全问题的研究仍处于初步阶段, 本文主要介绍以下几方面的安全需求。

(1) 针对大规模设备的有效认证机制

由于 5G 网络对物联网设备和 MTC 设备的支持, 共计 1 000 亿个设备将连接到 3GPP 5G 网络中^[9]。一旦这些大规模的终端设备受到攻击者的远程控制、木马挟持、肉机攻击等安全攻击^[10-11], 可能会对 5G 网络的正常运行造成严重的损害。而如果每个设备都需要执行完整的身份认证过程, 将会导致两方面问题: 一是认证过程需要多轮信令交换, 如果数据包丢失, 消息分组必须再次传输, 这将会导致资源受限设备性能下降^[12]; 二是可能造成大量信令开销和通信成本, 触发信令风暴, 从而导致网络服务乃至整个移动通信系统故障和崩溃。

因此, 需要简化已有的认证机制, 采用如表 1 所示的 128 位 SNOW 3G 加密算法、128 位 AES 算法、祖冲之 (ZUC-128、ZUC-256) 密码算法、SM 系列算法等标准密码算法^[13], 设计更加轻量级密码算法和协议流程, 建立支持大规模设备的、可靠且灵活的认证机制, 在保证接入设备安全合法的情况下, 减少认证复杂度带来的网络系统安全威胁。

(2) 隐私敏感数据保护

在 5G mMTC 业务场景中, 网络服务、功能及数据的开放共享, 增加了对用户隐私和敏感数据的完整性和机密性保护难度。相关研究人员指出, 在传统接入认证协议中存在可追溯性攻击^[14]、用户标识符破解攻击^[15]、中间人攻击^[16]等安全威胁, 这些攻击会导致用户标识符泄露、用户传输

的隐私信息被泄露或者被篡改。另外，物联网设备的安全存储能力有限，传输数据完整性校验大多采用弱哈希算法（如 SHA1）。因此，攻击者很容易恶意修改物联网设备中存储的数据，影响数据完整性^[17]。

表 1 标准密码算法
Table1 Standard cryptographic algorithm

算法类别	算法名称
5G 标准密码相关算法	对称密码算法 128-NEA1(SNOW 3G 算法)
	对称密码算法 128-NEA2 (AES 算法)
	对称密码算法 128-NEA3 (祖冲之算法)
SM 国密算法	杂凑算法 SM3
	公钥密码算法 SM2、SM9
	对称密码算法 SM1、SM4、SM7

(3) 防止多种类型的 DoS 攻击

5G mMTC 应用场景中海量多样化终端和复杂的拓扑结构易遭受拒绝服务（DoS, denial of service）攻击，将会阻碍整个网络正常工作。例如，槽洞攻击中的攻击者频繁引诱区域中的流量

通过恶意节点，一旦数据经过该节点，就可以篡改数据，并引发更多其他类型的攻击。此外，攻击者可能反复恶意地发送有效数据，从而导致服务器崩溃。

2 5G 网络切片的安全需求

传统移动通信网络主要用来服务单一的移动宽带业务，无法适应未来 5G 多样化应用场景的需求，为解决这一问题，网络切片技术应运而生。通过使用 SDN 和 NFV 技术部署的网络切片，在物理网络上创建相互隔离的、逻辑上独立的端到端虚拟网络，可实现网络、计算、存储资源共享，用户可以得到按需定制的差异化网络服务。然而，在实际应用中网络切片仍存在一些安全挑战，NGMN（next generation mobile network）联盟分析并列举了切片安全的十大问题^[18]，其中包括切片隔离安全、切片鉴权认证、切片间通信安全、虚拟化安全等方面。网络切片主要的安全威胁如图 2 所示。针对图中的安全威胁，本文分析总结出 4 部分安全需求。

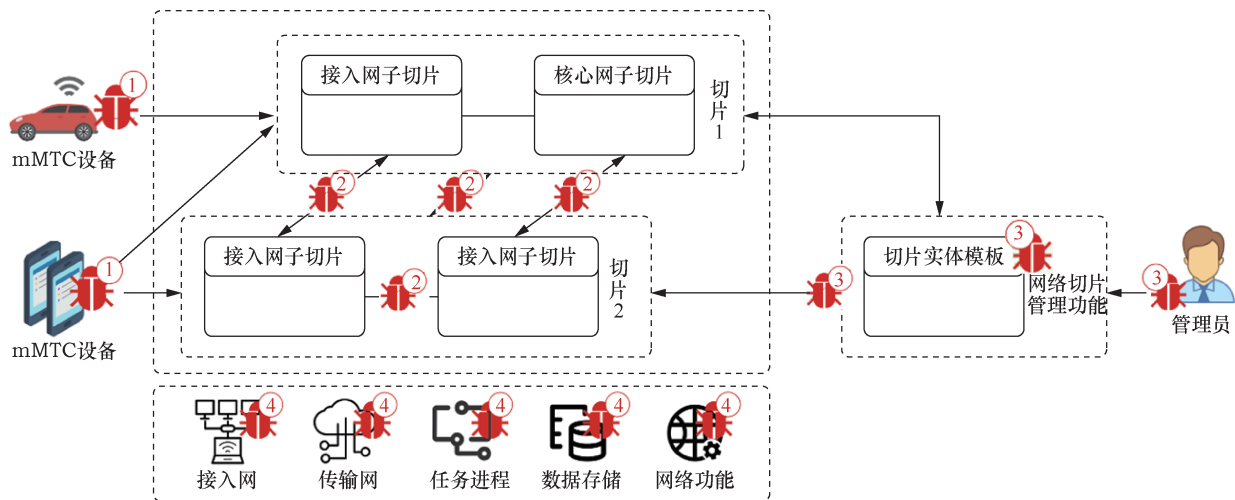


图 2 网络切片安全威胁

Figure 2 Network slicing security threats

2.1 特定于网络切片的二次认证和访问控制

5G mMTC 设备类型繁多，数量巨大，而设备使用者（UE, user equipment）大多为非技术人员，这使 5G mMTC 用户侧成为最易受攻击的切入点之一。一些已经使用 3GPP 凭据成功完成 5G 网络主身份认证的常规用户，未经网络切片层面授权，过度频繁访问网络切片，消耗资源，进而

导致网络性能降低。此外，黑客可以利用频繁访问的网络机制，制造 DoS 攻击。为防止黑客利用 UE 合法凭证频繁访问网络制造 DoS 攻击，需要针对特定的网络切片在完成主认证之后，制定切片层面的二次认证和访问控制机制。这样 5G 网络就能够有效地满足垂直行业定制化、独立化服务的需要，实现第三方的安全交互。

2.2 网络切片通信交互的安全隔离

由于资源共享和支持网络可编程性开放接口的存在,不同服务类型的网络切片可能具有不同的安全等级,如果单一 UE 具备同时访问多等级切片的权限,就存在敏感数据从安全等级高的切片泄露到安全等级低的切片中的风险。因此,需要建立一套安全隔离机制,保障实际情况中不同等级切片间的数据流转。不同用户访问同一类型切片服务时,可能所需的安全等级是不同的,需要通过设置不同用户对切片的访问隔离。例如,使用普通物联网设备(如智能电插座和智能安全锁)的用户所需的实际安全等级是不同的,接入网络时数据要进行隔离^[14]。这样既可以满足用户差异化安全需求,保证切片资源被合法使用,也可以防止恶意用户过度占用切片资源,对正常用户使用该类切片带来影响。

2.3 网络切片管理需要具备安全功能

基于当前标准定义,产业在商用初期产品实现上的进展以及结合垂直行业需求经验,中国移动联合华为等多家产业伙伴发布《网络切片分级白皮书》,给出当前 5G 端到端网络切片的 5 个能力等级^[19],如表 2 所示。

表 2 网络切片能力等级
Table 2 Network slicing capability level

切片等级	网络类型	等级划分	安全
L0	公众网	普通	基本安全
L1		VIP	eMBB 增强安全
L2	行业网	普通	业务特性安全
L3		VIP	业务特性高阶安全
L4		特需	全面高阶安全

网络切片具有各自的生命周期,分为 4 个阶段:准备阶段,安装、配置和激活阶段,运行阶段,撤销阶段。在整个生命周期中,用于切片管理的交互接口必须具备机密性和完整性的保护能力,并能够避免重放攻击^[13]。生命周期内每个阶段有不同的安全性需求,如准备阶段需要防止对网络切片模板的攻击,安装、配置和激活阶段以及运行阶段需要对 API 接口进行保护和访问控制,避免对网络切片实例配置的伪造和篡改,撤销阶段需要对敏感数据和资源进行安全处理,避免信息泄露和 DoS 攻击。

2.4 网络资源及基础设施的安全性

支撑网络切片服务的资源和网络功能可能受到攻击,从而给网络切片的性能带来影响,可能遭受的攻击包括物理攻击、软件攻击和 DoS 攻击等。例如,攻击者可能在访问切片过程中篡改代码,从而导致使用相同代码的所有切片执行过程也被篡改^[18]。

3 面向 5G mMTC 网络切片的安全策略

3.1 现有的安全策略分析

结合 5G mMTC 应用场景的特点和网络切片的安全需求,5G 标准组织和研究人员针对不同方面给出了一些方案,本文针对上述分析的安全需求,对现有研究方案进行说明和分析。

(1) 特定网络切片鉴权

3GPP 在 TR33.813 “网络切片增强的安全方面研究”中详细说明了用户访问特定网络切片的接入认证和认证过程中的隐私保护问题^[20],针对特定切片的二次认证触发条件和认证具体流程给出了解决方案。规定了认证管理功能(AMF, authentication management function)通过存储在认证服务器功能/统一数据管理功能(AUSF/UDM, authentication server function/unified data management)中的用户订阅信息选项是否支持网络切片鉴权来触发认证过程。同时,对二次认证框架进行了标准化说明,即认证架构要基于可扩展认证协议(EAP, extensible authentication protocol)框架,如图 3 所示。

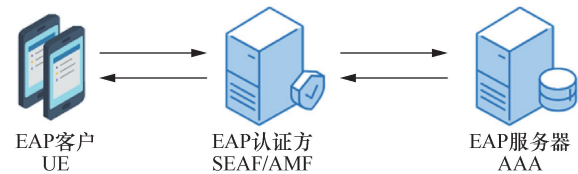


图 3 5G 切片二次认证框架
Figure 3 Secondary authentication framework for 5G slicing

核心网中的安全锚功能/认证管理功能(SEAF/AMF)被赋予了验证器角色,具体的认证方法和细节可由认证、授权、计费(AAA, authentication、authorization、accounting)服务器与用户进行协商选择,认证架构更加灵活,能够更好地适应 5G mMTC 差异化的接入技术和安全

需求。该标准虽然能够实现用户对特定网络切片的二次认证,但仍存在很多有待研究解决的问题。一是认证过程是否能够保护用户隐私^[20];二是标准只适用于一个或几个用户逐一进行认证,无法落实到 5G mMTC 应用场景下大规模机器设备的认证过程中。

除了 5G 标准化组织的进展外,有研究者提出了一种借助第三方认证实现跨网络切片认证的机制,并通过将认证部署到边缘云中达到降低时延的效果^[21]。Ren 等^[22]通过引入基于区块链、变色龙哈希和环签名的快速且通用的片间 (FUIS) 切换认证框架,来解决网络切片间匿名服务的身份认证问题,减少了认证过程中用户侧的计算开销,并保护了用户隐私。Behrad 等^[23]提出了一种 5G 特定切片的身份验证和访问控制机制 (5G-SSAAC),通过借助第三方根据特定用户的安全需求,给出灵活的访问认证机制,从而降低了核心网络负载。虽然这些研究均对切片二次认证过程给出了较为合理的方案,但针对大规模设备的二次认证问题并没有在方案中涉及,需要进一步的研究和验证。

(2) 切片安全隔离

以资源隔离为目的的端到端的网络切片隔离机制主要分为两种:一种是由 FlexE 或专用 TDM 时隙提供的电路交换连接实现的硬隔离^[24];另一种是通过使用 NVO3、MPLS、VLAN、沙箱以及容器等技术实现网络资源复用和软隔离。而为避免切片通信时敏感数据泄露,可以基于 VPN 技术使用 IPSec、SSL/TLS、DTLS、MPPE、SSTP、SSH 等协议,以支持认证和机密性等安全特性,保证网络切片间的安全通信,实现切片安全隔离。

3GPP 标准中提出了一种网络切片间访问控制的方案,如图 4 所示。网络存储功能 (NRF) 成功认证用户后生成相应切片的访问令牌,在用户请求切片服务时,切片管理者通过检验访问令牌中的切片信息是否与被请求访问的切片匹配,来防止用户在切片间的非法访问,从而达到切片间安全隔离的目的^[20]。

Sattar 等^[25]使用一种以切片隔离为优化约束的安全数学模型,来按需实现切片硬隔离,缓解 5G 核心网络切片中 DDoS 攻击,并使网络时延满足要求。Sathi 等^[26]提出了一种新型隐式认

证和基于组匿名的密钥协商协议,通过建立安全密钥实现了安全切片隔离。还有研究者结合性能隔离和安全隔离两方面因素,将网络切片的隔离等级划分为 5 个等级后再进行部署^[27]。Liu 等^[28]提出了一种相互异构的签密方案,实现了在公钥基础设施和无证书密码术两种不同的公共密码系统中 5G 网络切片之间的安全通信,他们提出的这种安全模式可以保护网络切片避免遭受传统的安全威胁。这些已经提出的安全隔离方案虽然可以在一定程度上解决切片的安全隔离问题,但必须进一步研究网络切片中密钥管理的相关问题^[29]。

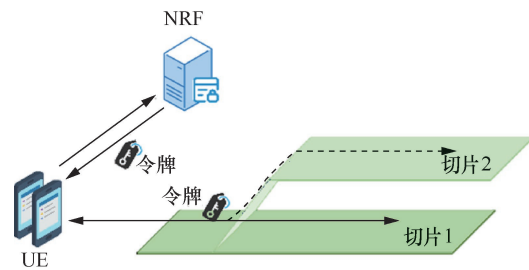


图 4 网络切片间访问控制方案
Figure 4 Access control scheme between network slices

(3) 安全管理和编排

网络功能虚拟化的管理和编排功能提供网络切片的编排和生命周期管理,以在整个生命周期中自动生成对应的网络服务并监视其完整性和性能,以确保网络切片的安全运行。可以通过安全管理功能的自动化来保证 NFV 资源和网络切片的安全性,使网络运营商能够适应 NFV 部署的动态性和复杂性^[30],安全管理功能可通过虚拟化安全功能的部署来实现,如虚拟身份和访问管理系统、虚拟防火墙^[31]和虚拟网络入侵检测系统^[32]。

3.2 未来研究方向的展望

针对海量用户应用场景,5G 网络切片安全仍有许多值得研究的方向。例如,需要研究用户组认证的相关轻量级密码技术^[33-35],以解决特定切片的认证机制下海量用户同时请求接入的问题;在切片间安全通信方面,需要解决切片使用自主身份认证的密钥情况下,由密钥派生函数引入的密钥管理问题^[36];在切片安全管理方面,由于 5G mMTC 涵盖工业制造、智慧城市等业务场景,如

在工业制造场景下，工业数据包括从客户需求、销售、研发、设计、制造等各个环节的各类数据，这就需要各个业务环节的切片协同交互、数据共享，为保证各个环节不同等级切片的安全协同，在将切片根据服务环节类型进行分级分组时，需要解决切片组身份认证、切片组安全管理和组成员更新机制的问题^[37-38]。在考虑上述方面时，用户的敏感隐私数据保护同样是一个关键问题。此外，方案在安全性与性能上的平衡协调^[39]，及如何实现算法协议最优化，也是值得研究的问题之一。

4 5G 切片二次认证与安全隔离模型

针对上述安全问题，本文提出一个切片二次认证框架，此框架基于对不同通信数据进行分级加密来保证切片间安全隔离。框架模型如图 5 所示。

4.1 5G mMTC 用户同时访问同一切片服务

4.1.1 基于 SM2 的无证书批量签名方案

针对实际应用场景中 5G mMTC 用户对轻量级通信的需求，此方案采用基于 SM2 国密算法的无证书批量签名方案。SM2 国密算法^[40]是一种基于椭圆曲线密码机制的非对称国产加密算法，主

要应用于数字签名、密钥交换协议以及公钥加密场景。本方案利用 SM2 国密算法的签名机制，实现 5G mMTC 用户与切片之间的互相认证和会话密钥协商。认证流程如图 6 所示。

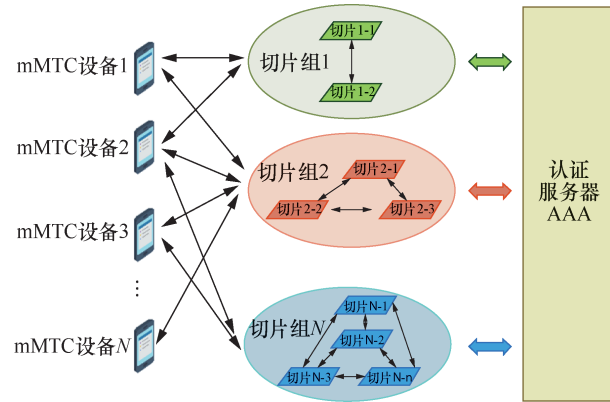


图 5 5G 切片二次认证与切片隔离框架模型
Figure 5 The frame model of 5G slicing secondary authentication and slice isolation

(1) 认证准备阶段

这一阶段为用户公私钥对生成阶段。每个用户 UE_i 公私钥对 (S_i, Q_i) 的生成采用的是无证书签名方案思想^[41]，即依托于一个可信的第三方密钥生成中心 (KGC, key generate center), KGC

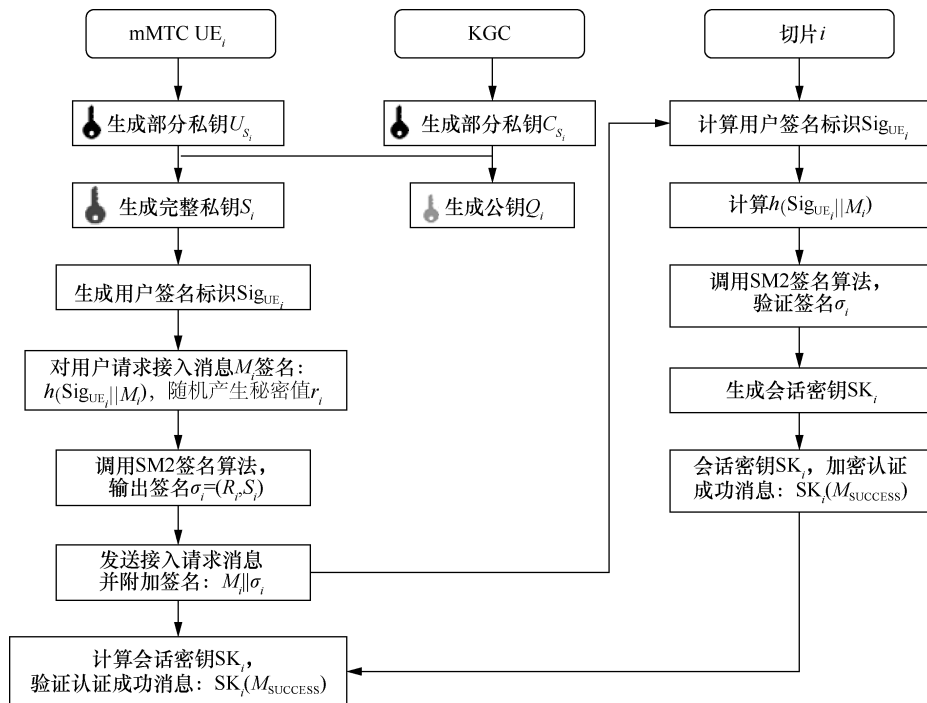


图 6 用户接入切片认证流程
Figure 6 User access slice authentication process

根据用户的身份与系统主密钥计算出用户的部分私钥 C_{S_i} 发送给用户, 同时用户通过产生随机秘密值计算自己的部分私钥 U_{S_i} , 而后用户将两部分私钥合并生成完整私钥 S_i 。用户的公钥 Q_i 则通过用户的部分私钥 U_{S_i} 生成。

(2) 用户接入请求阶段

这一阶段利用 SM2 数字签名算法, 通过给接入请求消息签名, 用户发起与切片之间身份认证和会话密钥协商的请求。用户利用 KGC 提供的系统参数和自身的身份信息计算用户签名标识 Sig_{UE_i} , 并将用户接入请求消息 M_i (包含用户的身份信息) 一并作为输入, 产生一个哈希值 $h(\text{Sig}_{\text{UE}_i} \parallel M_i)$, 同时随机产生秘密值 r_i 。而后, 用户利用 SM2 签名算法, 生成签名 σ_i , 并将其附加到 M_i 后, 发送给切片 i 。

(3) 切片认证阶段

这一阶段切片根据收到的用户请求消息, 利用 SM2 算法认证用户。切片认证成功后, 计算与用户的会话密钥 SK_i , 并将用户成功接入切片的消息 M_{SUCCESS} 用会话密钥 SK_i 加密发送给用户。

(4) 用户认证阶段

用户收到切片响应的消息后, 计算与切片间的会话密钥 SK_i , 并对消息进行解密。若能成功解密, 则用户认证切片成功, 否则用户认证失败。

该方案可扩展为多用户批量签名认证的方案, 设定切片 i 一次批量认证用户消息的数量为 m , 当切片 i 收到 m 个接入请求后, 随机选取 m 个随机数, 用于一次批量认证 m 个用户。

4.1.2 方案分析

(1) 性能分析

该方案基于 SM2 签名算法, SM2 算法具有存储空间小、签名速度快等特点^[42], 可以满足 mMTC 用户计算性能受限的需求; 本方案引入了批量签名的思想, 将海量用户进行封装批量认证, 减少了切片的认证次数; 同时, 由于方案中用户与切片在认证与密钥协商过程的交互轮数仅为一轮, 不仅有效地降低了时延, 而且减少了系统中信令的传输数量, 可以在一定限度上降低系统产生信令风暴的风险。

(2) 安全性分析

本方案通过无证书的方式生成用户的公私钥

对, 解决了基于证书和基于身份的签名方案中证书管理与密钥托管的问题, 有利于系统的灵活扩展, 可适应于 5G 网络海量终端和灵活拓扑下的安全需求; 由于采用随机化签名方案并引入了新鲜的随机数, 用户接入请求阶段的协议设计可有效抵抗以重放攻击为代表的身份假冒攻击; 在此协议下, 会话密钥生成所需的参数除双方各自安全存储的私钥外, 均为系统公开参数, 攻击者无法通过对协议传输的副本的监听获取密钥相关信息, 理论上保证了会话密钥的安全产生。

通过对方案性能与安全性上的分析, 可以看出, 本方案可以在保证安全需求的同时, 兼顾性能上的高效和轻量, 实现安全性与性能的平衡。

4.2 5G mMTC 用户同时访问多个切片服务

这一部分主要包括切片预分组、切片相互认证、切片组密钥更新、用户切片认证和切片隔离通信这 5 个阶段, 最终实现 5G mMTC 用户与网络切片间的安全通信, 保证网络切片间的安全隔离。协议框架如图 7 所示。

4.2.1 方案介绍

(1) 切片预分组阶段

这一阶段主要将切片按照不同服务类型进行分组形成若干个网络切片组。切片组形成机制是动态更新的, 从而满足 5G 网络灵活部署的特性。

(2) 切片相互认证阶段

这一阶段每个网络切片组中的网络切片间通过借助服务网络和归属网络, 实现组内切片的相互认证, 并分别建立切片组间的会话密钥, 同时保证仅网络切片组间知悉该会话密钥, 包括服务网络和归属网络在内的第三方无法获取该密钥。

(3) 切片组密钥更新阶段

这一阶段用于保证切片组的动态管理和切片组间会话密钥的新鲜性和安全性。切片组间密钥更新主要分为两个场景: 一是组成员未发生变化, 会话密钥过期, 需要更新会话密钥; 二是会话密钥未过期, 组成员存在新进入与退出的情况, 需要更新会话密钥。

(4) 用户切片认证阶段

这一阶段分为认证阶段与密钥协商阶段。该阶段方案用户首先与网络切片组进行相互认证,



图7 5G mMTC 用户同时访问多个切片服务的协议框架
Figure 7 Framework for 5G mMTC users to simultaneously access multiple slicing services

认证过程仅需选取网络切片组中的任意组员与用户进行认证,即可实现用户与整个网络切片组的认证。认证后用户与切片组内各个网络切片建立各自的会话密钥。

(5) 切片隔离通信阶段

这一阶段利用在切片相互认证阶段和用户切片认证阶段协商的密钥,针对不同的通信对象和通信数据内容,对通信会话进行分级加密,从而保证用户与切片通信过程各个阶段数据的安全与隔离:在用户与切片间的通信过程中采用用户切片认证阶段协商的会话密钥进行加密,保证用户端数据的安全隔离;切片与切片之间交互的共享数据和资源采用用户切片认证阶段协商的密钥进行加密传输,实现切片协同工作过程中切片的数据隔离。

4.2.2 方案分析

(1) 性能分析

该方案从系统架构层面,考虑了网络切片按需服务的特性,方案具有灵活性、动态性和可扩展性;方案通过切片预分组和切片组间预认证的设计,让切片的安全动态管理针对用户接入是透明的,即认证组内任意切片可认证整个组内切片,节省了用户认证切片的计算开销和时间开销。

(2) 安全性分析

切片相互认证阶段和用户切片认证阶段,保证各个实体间合理的访问权限和信息知悉范围,保证网络在预期下运行。在切片组密钥更新阶段,当有新的成员加入时,或者原组成员退出切片

组时,切片组的会话密钥均会更新。这在保证密钥新鲜性的同时,保证了前向安全性和后向安全性,使切片隔离方案既满足灵活性,又具备高安全属性。

整个 5G 切片二次认证与安全隔离模型很好地解决了大规模机器类用户与切片间的认证问题,基于 SM2 批量认证的方式在满足安全属性的前提下,提高了认证效率;同时,通过切片间的预分组和相互认证,解决了切片认证和切片隔离的问题,为用户安全接入切片提供了保障。

5 结束语

本文首先介绍了 5G mMTC 应用场景和 5G 网络切片技术,分析了其特点、面临的安全威胁以及安全需求。在以上工作的基础上,详细分析了现有研究的进展与不足,并展望了一些未来可能的研究方向。最后,针对网络切片二次认证提出了一个模型框架,该框架可以满足 5G 机器类用户大规模认证,使认证过程更加高效且可靠,并且能够实现切片间的安全隔离,为今后的相关研究提供了一个较为合理的模型基础。

参考文献:

- [1] LIN X Q. An overview of 5G advanced evolution in 3GPP release 18[J]. arXiv preprint arXiv:2201.01358, 2022.
- [2] 网络安全管理局. 工业和信息化部部署推进 5G 安全工作[EB]. China Network Security Administration. Ministry of Industry and Information Technology deployed to promote 5G security work. [EB].

- [3] IMT-2020 (5G) 推进组. 5G 愿景与需求白皮书[Z]. 2014. IMT-2020(5G) Promotion Group. White paper on 5G vision and requirements[Z]. 2014.
- [4] 3GPP TS 22.261 V18.1.1. 3rd generation partnership project; technical specification group services and system aspects; service requirements for the 5G system; stage 1(release 18)[S]. Valbonne: 3GPP, 2021.
- [5] 3GPP TS 22.186 V16.2.0. 3rd generation partnership project; technical specification group services and system aspects; enhancement of 3GPP support for V2X scenarios; stage 1(release 16)[S]. Valbonne: 3GPP, 2019.
- [6] 张东. 探秘 5G 新空口技术[J]. 华为技术, 2016, 75: 56-60. ZHANG D. Exploring 5G new air interface technology[J]. Huawei Technology, 2016, 75: 56-60.
- [7] O'CONNELL E, MOORE D, NEWE T. Challenges associated with implementing 5G in manufacturing[J]. Telecom, 2020, 1(1): 48-67.
- [8] HARWAHYU R, CHENG R G, WEI C H, et al. Optimization of random access channel in NB-IoT[J]. IEEE Internet of Things Journal, 2018, 5(1): 391-402.
- [9] KUHLLINS, BELA RATHONYI, ALI ZAIDI, et al. Ericsson white paper: cellular networks for massive IoT[Z]. Sweden: Ericsson, 2020.
- [10] JAVED M A, KHAN NIAZI S. 5G security artifacts (DoS/DDoS and authentication)[C]//Proceedings of 2019 International Conference on Communication Technologies (ComTech). 2019: 127-133.
- [11] RIM K, LIM D. DoS attack control design of IoT system for 5G era[J]. Journal of Information and Communication Convergence Engineering, 2018, 16(2): 93-98.
- [12] JANG S, LIM D, KANG J, et al. An efficient device authentication protocol without certification authority for Internet of Things[J]. Wireless Personal Communications, 2016, 91(4): 1681-1695.
- [13] 3GPP TS 33.501 V17.0.0. 3rd generation partnership project; technical specification group services and system aspects; security architecture and procedures for 5G system (release 17)[S]. Valbonne: 3GPP, 2020.
- [14] CAO J, MA M D, LI H, et al. A survey on security aspects for 3GPP 5G networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 170-195.
- [15] HUSSAIN S R, ECHEVERRIA M, CHOWDHURY O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information[C]//Proceedings of 2019 Network and Distributed System Security Symposium. 2019.
- [16] CAO J, MA M D, LI H, et al. A survey on security aspects for LTE and LTE-A networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 283-302.
- [17] KHAN M A, SALAH K. IoT security: Review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2018, 82: 395-411.
- [18] NGMN 5G Security-Network Slicing Version 1.0, 5G security Recommendations Package# 2: Network Slicing[S]. UK: ngmn Ltd., 2016.
- [19] 网络切片分级白皮书[Z]. 深圳: 中国移动, 2021. White Paper: Network Slice Grading[Z]. Shenzhen: China Mobile, 2021.
- [20] 3GPP TR 33.813 V16.0.0. 3rd generation partnership project; technical specification group services and system aspects; security aspects; study on security aspects of network slicing enhancement (release 16)[S]. Valbonne: 3GPP, 2020.
- [21] FAN C N, SHIH Y T, HUANG J J, et al. Cross-network-slice authentication scheme for the 5th generation mobile communication system[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 701-712.
- [22] REN Z, LI X H, JIANG Q, et al. Fast and universal inter-slice handover authentication with privacy protection in 5G network[J]. Security and Communication Networks, 2021, 2021: 6694058.
- [23] BEHRAD S, BERTIN E, TUFFIN S, et al. 5G-SSAAC: slice-specific authentication and access control in 5G[C]//Proceedings of 2019 IEEE Conference on Network Softwarization (NetSoft). 2019: 281-285.
- [24] 王睿, 张克落. 5G 网络切片综述[J]. 南京邮电大学学报(自然科学版), 2018, 38(5): 19-27. WANG R, ZHANG K L. Survey of 5G network slicing[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2018, 38(5): 19-27.
- [25] SATTAR D, MATRAWY A. Towards secure slicing: using slice isolation to mitigate DDoS attacks on 5G core network slices[C]//Proceedings of 2019 IEEE Conference on Communications and Network Security. 2019: 82-90.
- [26] SATHI V N, SRINIVASAN M, THIRUVASAGAM P K, et al. A novel protocol for securing network slice component association and slice isolation in 5G networks[C]//Proceedings of MSWIM '18: Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. 2018: 249-253.
- [27] 潘启润, 黄开枝, 游伟. 基于隔离等级的网络切片部署方法[J]. 网络与信息安全学报, 2020, 6(2): 96-105. PAN Q R, HUANG K Z, YOU W. Network slicing deployment method based on isolation level[J]. Chinese Journal of Network and Information Security, 2020, 6(2): 96-105.
- [28] LIU J W, ZHANG L H, SUN R, et al. Mutual heterogeneous signcryption schemes for 5G network slicings[J]. IEEE Access, 2018, 6: 7854-7863.
- [29] 杨志强, 栗栗, 齐旻鹏, 等. 5G 安全技术与标准[J]. 电信科学, 2020, 36(12): 1-19. YANG Z Q, SU L, QI M P, et al. Overview and prospect of 5G security[J]. Telecommunications Science, 2020, 36(12): 1-19.
- [30] GARDIKIS G, TZOULAS K, TRIPOLITIS K, et al. SHIELD: a novel NFV-based cybersecurity framework[C]//Proceedings of 2017 IEEE Conference on Network Softwarization (NetSoft). 2017: 1-6.
- [31] LI H D, DENG J, HU H X, et al. Poster: on the safety and efficiency of virtual firewall elasticity control[C]//Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. 2017: 129-131.
- [32] LI H D, HU H X, GU G F, et al. vNIDS: towards elastic security with safe and efficient virtualization of network intrusion detection systems[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 17-34.
- [33] 冯琦, 何德彪, 罗敏, 等. 移动互联网环境下轻量级SM2 两方协同签名[J]. 计算机研究与发展, 2020, 57(10): 2136-2146. FENG Q, HE D B, LUO M, et al. Efficient two-party SM2 signing protocol for mobile Internet[J]. Journal of Computer Research and

- Development, 2020, 57(10): 2136-2146.
- [34] CAO J, YU P, MA M D, et al. Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network[J]. IEEE Internet of Things Journal, 2019, 6(2): 1561-1575.
- [35] POTHUMARTI R, JAIN K, KRISHNAN P. A lightweight authentication scheme for 5G mobile communications: a dynamic key approach[J]. Journal of Ambient Intelligence and Humanized Computing, 2021: 1-19.
- [36] DE REE M, MANTAS G, RADWAN A, et al. Key management for beyond 5G mobile small cells: a survey[J]. IEEE Access, 2019, 7: 59200-59236.
- [37] FAN CHUN-I, SHIH Y T, HUANG J J, et al. Cross-network-slice authentication scheme for the 5th generation mobile communication system[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 701-712.
- [38] NI J B, LIN X D, SHEN X S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644-657.
- [39] SICARI S, RIZZARDI A, COEN-PORISINI A. 5G in the internet of things era: an overview on security and privacy challenges[J]. Computer Networks, 2020, 179: 107345.
- [40] ZHOU L, SU C H, HU Z, et al. Lightweight implementations of NIST P-256 and SM2 ECC on 8-bit resource-constraint embedded device[J]. ACM Transactions on Embedded Computing Systems, 2019, 18(3): 1-13.
- [41] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[M]//Advances in Cryptology - ASIACRYPT 2003. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 452-473.
- [42] 谷国进. 基于 SM2 算法的认证授权系统研究与实现[D]. 济南: 山东大学, 2013.

GU G J. Study and implementation of authentication and authorization system based on SM2Algorithm[D]. Jinan: Shandong University, 2013.

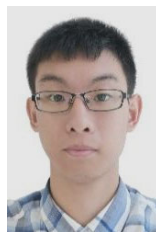
[作者简介]



徐子钧（1998—），女，辽宁鞍山人，北京航空航天大学硕士生，主要研究方向为 5G 网络安全。



刘建伟（1964—），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为网络安全。



李耕（1993—），男，浙江温州人，主要研究方向为公钥密码学、后斯诺登密码学、信息安全。