5G 安全风险分析与防护体系建设

刘笑凯[1]，王文东[1]，国佃利[1]，王　萍[2]
（1.中国电子信息产业集团有限公司第六研究所，北京 100083；
2.中国联合网络通信有限公司北京市分公司，北京 100052）

摘　要： 随着移动通信世代的不断演进，人类社会从移动互联时代逐步迈向万物互联时代，5G 网络将打破传统移动通信行业局限，颠覆和重塑社会发展模式，引领实现新一轮的信息革命。5G 作为全新一代的移动通信技术可为当前物联网、无人驾驶、工业互联网等创新应用提供基础通信保障，满足数据流量爆炸式增长及其数以千亿计的海量设备连接需求。5G 安全是其全面推进的不容忽视的核心支撑要素，首先分析研究了 5G 网络面临的安全风险，明确了 5G 网络安全需求，并提出了相应的防护体系架构，对后续 5G 网络安全技术发展有一定的借鉴意义。

关键词： 5G 网络；网络安全；防护体系；安全架构
中图分类号： TN918.91；TP309.7　　**文献标识码：** A　　**DOI：** 10.16157/j.issn.0258-7998.201031

中文引用格式： 刘笑凯，王文东，国佃利，等. 5G 安全风险分析与防护体系建设[J].电子技术应用，2021，47(5)：69-72.
英文引用格式： Liu Xiaokai，Wang Wendong，Guo Dianli，et al. Security analysis and protection system construction in 5G networks[J]. Application of Electronic Technique，2021，47(5)：69-72.

Security analysis and protection system construction in 5G networks

Liu Xiaokai[1]，Wang Wendong[1]，Guo Dianli[1]，Wang Ping[2]
（1.The 6th Research Institute of China Electronics Corporation，Beijing 100083，China；
2.China Unicom Beijing Branch，Beijing 100052，China）

Abstract： With the continuous evolution of the mobile communication generation，human society has gradually convert from the era of “Mobile Internet” to the era of “Internet of Everything”. 5G networks will break the limitations of the traditional mobile communication industry and reshape the social development model. 5G will realize a new round of information revolution. As a new generation of mobile communication technology，5G could provide basic communication guarantee for current innovative applications，such as the Internet of Things，autonomous vehicles and industrial Internet，and meet the explosive growth of data traffic and massive device connections. Security is a core for the comprehensive promotion of 5G networks. This paper analyzes the security risks in 5G networks and clarifies its security requirements. Finally，it proposes the corresponding security architecture，which will provide reference for the subsequent development of 5G network security technology.

Key words： 5G networks；network security；security protection；security architecture

0 引言

移动通信作为信息基础设施已经完全融入了人们生活中的方方面面，深刻改变了人类的交互方式。移动通信经历了五个世代的演进，不断涌现出与时代相匹配的业务场景，驱动实现信息技术革命性发展。

第五代移动通信系统(5G)将突破传统信息交互局限，以人类为核心，以服务为基础，以信息为纽带，围绕“信息随心至，万物触手及”的愿景构建全方位的信息生态体系，赋能未来各个垂直行业[1-2]。5G 网络划分为 3 种业务场景：增强移动宽带(Enhance Mobile Broadband，eMBB)、海量机器连接(Massive Machine Type Communication，mMTC)、超可靠低时延连接(Ultra Reliable & Low Latency Communication，uRLLC)，上述 3 种业务场景通过差异化服务分别满足移动通信领域对于极高带宽、海量物联与时延敏感的需求[3-4]。eMBB 是移动宽带业务场景的拓展，聚焦高清视频、VR(虚拟现实)、AR(增强现实)等对移动带宽有极高要求的典型业务[5]。mMTC 专注海量物联场景，面向数以千亿计的物联网设备连接，可满足智慧家居、智慧电网、智慧农业等对于超大连接密度要求的业务[6]。uRLLC 支持低时延与高可靠的场景需求，可为自动驾驶、智慧工业等对时延极为敏感的业务提供基础支撑[7]。5G 引入了网络切片、软件定义网络(Software Defined Network，SDN)、网络功能虚拟化(Network Functions Virtualization，NFV)、移动边缘计算等，能够以灵活部署、按需配置、软硬件解耦的方式为 eMBB、mMTC、uRLLC 3 种业务场景提供差异化支持[8]。

全新的、多类别的业务场景，能力跨度大的、复杂形态的终端设备，融合异构的、按需适配的网络架构为5G网络带来了极为严重的安全风险，同时也为5G网络的大规模推广应用带来了新的安全挑战。5G安全作为开启万物互联时代的基石，需明确安全风险与社会效益的两面性，本文系统地梳理了5G网络中创新技术、应用场景以及攻击理念发展引发的安全风险，并针对上述风险给予了相对应的应对措施建议，能够对未来5G产业生态推动提供风险评估与安全对策支撑[9-12]。

1 5G网络安全风险分析

1.1 差异化的场景带来的安全风险

5G网络重点划分了3种类型的应用场景，包括eMBB、mMTC、uRLLC，5G网络需针对这3种类型迥异的应用场景提供统一架构下的差异化的安全保护。

(1)eMBB场景

与4G网络一致，eMBB场景面向的是以人为主体的通信模式，旨在向用户提供超极致体验的数据连接，用户体验数据传输速率最高支持1 Gb/s，每平方公里内最高可支持一百万的连接数密度，并支持每小时500 km的移动性。相对于4G网络，其超大连接流量对于现有的移动安全防护机制带来了巨大的挑战，无论在以防火墙和入侵防御为核心安全边界防护设备，还是以流量分析、安全审计、Web安全防护为核心的服务端内网安全防护设备，都将面临极其严重的冲击。此外，现有终端侧安全防护机制以及数据安全存储仍缺乏行之有效的手段以应对eMBB场景下数据流量的巨大提升。

(2)mMTC场景

mMTC聚焦物联网场景，主要面向海量边缘节点的蜂窝网络接入，具有业务应用众多、地域覆盖广阔、终端能力有限、设备标准分化、连接数量庞大等特点，将对安全防护措施提出非常严格的要求。物联网业务应用不同，设备的种类、能力、形态各不相同，生产供应商的标准分散，迫切需求在统一架构下实现差异化的安全防护策略。物联网终端接入数量未来预计将以千亿计量，其中大部分为计算和存储资源受限的边缘节点终端，无法配置相应的较为复杂的安全防护措施，由于边缘节点部署位置的泛在特性，一旦被敌手捕获并进行攻击，极易形成僵尸网络，对业务应用后台服务器带来非常严重的安全问题，对5G网络运行造成中断、瘫痪等安全风险。

(3)uRLLC场景

uRLLC场景能够支持终端用户面上行与下行低至0.5 ms的超低时延，并满足垂直行业用户接近100%超高可靠性的数据传输需求，可为工业控制、无人驾驶、自动化处理等提供极高可用性的通信保障。为满足uRLLC场景超低时延与高可靠性要求，需在终端侧至核心网侧的通信链条中部署一系列的高级别安全防护机制，并通过优化举措降低由此带来的时延。从安全视角来看，低时延与高可靠这两种特性是相悖的，添加接入鉴权、传输加密、存储加密等安全保密机制必然会导致通信时延的增加，但满足高可靠特性又无法在安全性方面进行妥协，轻量级的鉴权协议以及密码算法可为权衡低时延与高可靠对于安全措施的保障要求提供新的解决思路。

1.2 全新的网络架构与技术带来的安全风险

(1)移动边缘计算

5G网络采用了移动边缘计算架构，颠覆了传统移动网络架构设计理念，将业务体系下沉至接入网侧，通过将接入管道与业务服务的融合，能够为终端提供便捷的边缘云服务[13-14]。移动边缘计算在继承了云计算中心面临的安全风险外，由于自身特点还引入了更为严峻的攻击威胁。当边缘云部署在相对复杂的物理环境中，其受到接口劫持、物理破坏、数据窃取、硬件入侵等攻击的可能性非常大。此外，虚拟化与分布式架构安全的不确定性对边缘基础设施影响巨大，一旦攻击者突破某个边缘安全防护体系，可将其作为跳板，影响云体系的整体安全。

(2)网络切片

5G将云计算思维引入核心网的架构设计中，利用NFV/SDN技术为不同的业务场景以及垂直行业提供可灵活定制的网络切片，其安全性不再依托传统的硬件设备防护措施，网元设备间的安全隔离机制已被虚拟隔离取代，以往被认为安全的物理环境也不再被认同[15]。网络切片可为不同的业务体系提供定制化的部署策略，为支持差异化的服务，同样需满足差异化服务安全要求，对网络切片的整体化安全设计提出了全新的挑战。此外，网络切片间部署逻辑隔离措施同样面临巨大风险，防护能力强度的不同可为攻击者利用木桶原理攻破5G核心网防御体系提供便利。

(3)网络能力开放

为更好地向其他网络提供优化的服务能力，5G网络能力开放框架能够充分利用自身的优势，配置网络资源，实现更为友好化、智能化的网络功能。控制面网元功能接口向其他网络进行开放，必然会引入运营商无法掌控的安全风险，数据面信息也将不再仅仅由运营商进行管理和维护，如此庞大的隐私数据向第三方进行开放，并摆脱运营商的监督和管理，可能会引发数据外流、隐私泄露等安全风险。随着移动网络的不断迭代发展，为了实现接口的开放性，将互联网通用协议引入网络能力开放接口是最直接也是最有效的方式，但互联网面临安全威胁也将对网络能力开放平台产生极为严重的影响。

1.3 复杂形态的终端设备带来的安全风险

5G网络不再仅仅注重人与人之间的通信，而是划分出了eMBB、mMTC、uRLLC 3种业务场景，终端设备的形态、处理能力、接入方式、身份标识各不相同。eMBB场景中的终端设备普遍具备超高的计算与存储能力，并能

够配备通用用户身份识别模块(Universal Subscriber Identity Module,USIM);mMTC 场景聚焦物联网业务,终端形态各异,甚至部分传感器仅仅具有感知和通信能力,没有足够的处理能力支持复杂的接入鉴权协议;uRLLC 场景中终端设备需满足几乎为零的通信时延。因此,构建一个统一融合的认证鉴权体系给 5G 终端侧安全带来了巨大的挑战。此外,5G 为支持未来应用场景的发展,需同时支持多种异网接入技术,终端设备的接入能力将得到极大的扩展,由此将触及诸多安全风险,例如:接入切换、多终端异网接入等,如何保证在一个统一的鉴权体系将其他异网接入鉴权框架进行融合处理,提升终端在切换和接入时实现连续不中断的业务保护是未来 5G 网络安全研究的重点和难点。

1.4 日益增强的的隐私保护需求

5G 网络中多元化的业务场景以及较为开放的接入技术,给用户隐私数据的保护带来非常大的困扰。首先,多元化的业务场景引发的隐私泄露风险各不相同,例如在 eMBB 场景中用户身份标识(Subscription Permanent Identifier,SUPI)、访问记录、浏览内容等存在被非法搜集使用的风险;在 mMTC 场景中节点信息、汇聚内容、处理事务等存在被暴露的风险;在 uRLLC 场景中车辆的位置、行驶轨迹、车辆标识等存在被非法跟踪使用的风险。其次,5G 网络的异构特性,散布在各个网络位置的隐私数据通过多种接入技术实现网络服务,海量用户隐私数据穿越 5G 网络必然引发诸多隐私暴露风险,需制定相应的安全防护机制以满足高级别的隐私保障需求。

2 5G 网络安全防护体系设计

2.1 5G 安全防护目标

5G 网络三大业务场景以及引入的诸多关键技术在一定程度上带来了与 4G 网络截然不同的安全威胁,在隐私保护、数据安全、网络安全等方面提出了更为严格的要求,需在 4G 网络安全防护机制的基础上进行演进升级,并统筹各个业务场景安全需求,建立统一融合的安全防护机制,以应对 5G 未来发展中的未知安全挑战。

面对多形态的终端设备、多样化的场景要求、多类别的接入方式,5G 网络安全架构需提供统一的认证体系,并打造按需的安全功能模块,既能保障所有终端设备的安全接入,还能够满足典型的应用场景下的要求(包括低时延、高可靠、低功耗、超大连接、高带宽等方面)。

5G 网络引入了全新的网络架构,采用了 NFV/SDN、网络切片与网络能力开放等新技术,5G 网络安全需提供全新的安全防护体系,满足 5G 系统虚拟安全、切片安全、数据安全、软件安全、网络安全等,并保证网络能力开放安全,实现在高等级隐私保护。

2.2 5G 安全防护架构

5G 安全防护架构需满足网络接入安全、系统域安全、应用域安全以及能力开放安全,通过融合统一的认证框架、安全防护体系及隐私保护策略实现 5G 系统内生安全。5G 安全防护架构如图 1 所示。

(1)网络接入安全

5G 网络支持使用 EAP-认证与密钥协商协议,可在统一框架下完成终端与系统侧的双向认证。在接入认证方面增加 5G-AKA 认证,通过归属网络提供终端已在访问网络成功接入鉴权的证明。完成接入鉴权后,通过派生密钥可建立终端至 5G 核心网之间控制面信令以及用户面数据安全通道。当终端设备与 5G 系统建立承载,需提供信令数据的机密性与完整性保护。此外,用户面承载数据同样需要机密性与完整性保护,实现终端设备与基站间的空口侧数据安全,以及基站与核心网间网络侧数据安全。

(2)系统域安全

系统域安全可为基站与核心网侧提供数据传输安全,能够实现服务网络与归属网络交互安全,以及网元功能间的信令保护,并将适用于垂直行业的切片建立起物理或逻辑隔离,保障终端设备访问切片的接入安全与切片间的安全隔离。5G 规范中将传统 PKI 体系纳入了网络安全范畴中,通过在基站、核心网网元功能配置相应的数字证书,可实现基站间、基站与核心网以及核心网网元功能间的信任连接。

(3)应用域安全

5G 安全不仅体现在终端、接入网与核心网侧,还为业务服务商提供了二次认证的接口,业务服务商通过在终端应用以及服务侧部署相应的鉴权设备实现对于用户在应用域的二次认证授权,赋予了业务服务商更为开

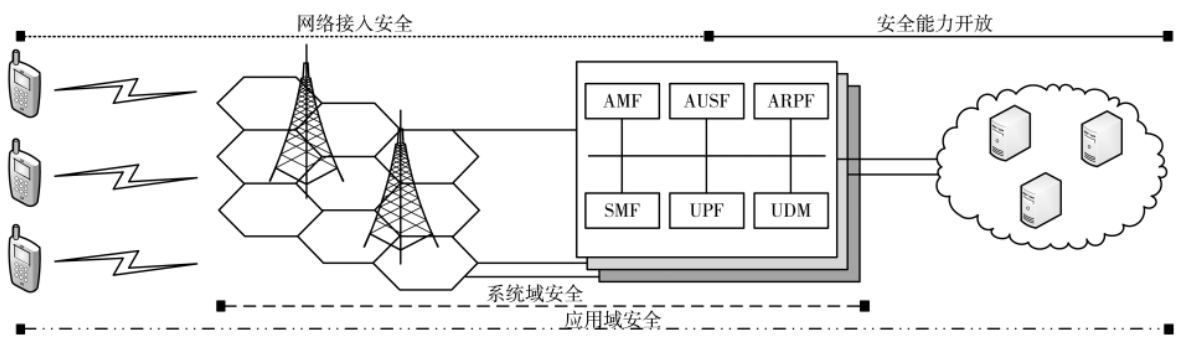

图 1 5G 安全架构图

放、自由的安全权限管理，进一步增强了 5G 网络数据安全保护。

(4)安全能力开放

5G 网络能力开放为垂直行业开放 API 接口，不仅仅为第三方开放业务服务，还拓展了相应的安全能力，可将系统侧的安全能力渗透至业务层面，传统的业务提供商专注于业务逻辑开发，提升用户的友好体验，同时通过安全层面的边云协同处理，将 5G 中心侧安全能力拓展至网络边缘，能够为垂直行业用户提供相匹配的安全防护能力，支撑其将关键业务迁移至 5G 网络，真正实现 5G 安全能力的开放。

(5)隐私保护

5G 网络对于多种应用场景以及垂直行业的支持，加深了用户对于隐私数据泄露的担忧，5G 网络需提供差异化的按需的隐私保护能力，可对用户身份标识、位置信息、用户行为以及信息内容进行可配置的隐私保护。通过明确 5G 网络涉及的隐私范围，引入数据最小化、数据访问控制、匿名化处理与数据加密存储等技术，在空口、网络、控制面、数据面、传输层以及应用层各个层面对数据提供隐私保护能力。

3 结论

5G 网络作为驱动社会信息化转型的关键通信基础设施，将为社会各个领域的发展带来颠覆性的影响。5G 网络在终端、接入网、核心网以及业务领域引入了诸多创新技术，并采用了更为灵活、开放的网络架构，为开启 5G 全面发展格局打下了重要基石，但同时也带了全新的安全挑战。本文全方位地分析了 5G 网络在各个层面存在的安全风险，并给出了具体的防护体系建设建议，可支撑未来 5G 网络安全部署和发展。

参考文献

[1] 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.

[2] 刘光毅，方敏，关皓，等.5G 移动通信系统：从演进到革命[J].电信科学，2016，32(11)：166.

[3] 唐连雷，王海龙.5G 移动通信应用场景及关键技术探讨[J].中国新通信，2018，20(22)：141.

[4] 陈虹旭，李菲，李晓坤，等.基于 eMBB，mMTC，uRLLC 场景的第五代移动通信方法研究[J].智能计算机与应用，2019，9(6)：13-20，23.

[5] 杨燕玲，阮丹.eMBB 应用场景下的 5G 无线网络部署方案研究[J].广东通信技术，2018，38(10)：55-58，79.

[6] 赵丽彤.面向 5G 的大规模机器类通信关键技术研究及标准化[D].北京：北京邮电大学，2018.

[7] 朱红梅，林奕琳，刘洁.5G URLLC 标准、关键技术及网络架构的研究[J].移动通信，2017，41(17)：28-33.

[8] 任驰，马瑞涛，REN，等.网络切片网络切片：构建可定制化的 5G 网络[J].中兴通讯技术，2018，24(1)：26-30.

[9] 常志泉，谢玉娟.5G 网络安全技术探究[J].信息安全研究，2019，5(12)：1124-1128.

[10] 崔媛，淦贵生.第五代移动通信技术网络安全问题研究[J].通信企业管理，2020(9)：77-79.

[11] 黄开枝，金梁，赵华.5G 安全威胁及防护技术研究[J].邮电设计技术，2015(6)：8-12.

[12] 季新生，黄开枝，金梁，等.5G 安全技术研究综述[J].移动通信，2019(1)：34-39，45.

[13] 李子姝，谢人超，孙礼，等.移动边缘计算综述[J].电信科学，2018，34(1)：87-101.

[14] 齐彦丽，周一青，刘玲，等.融合移动边缘计算的未来 5G 移动通信网络[J].计算机研究与发展，2018，55(3)：478-486.

[15] 聂炜玲.论 NFV 和 SDN 架构下的核心网生态系统[J].电信技术，2016，8(1)：82-84.

(收稿日期：2020-10-22)

作者简介：

刘笑凯(1977-)，男，硕士，高级工程师，主要研究方向：信息安全、保密通信。

王文东(1979-)，女，工程师，主要研究方向：移动管理、企业安全。

王萍(1990-)，通信作者，女，硕士，主要研究方向：移动安全、企业安全，E-mail：guoguo_w@163.com。

扫码下载电子文档

(上接第 68 页)

[11] PARK B E，KIM K H，KANG H S，et al.Improved relay feedback method under noisy and disturbance environments[J].Journal of Chemical Engineering of Japan，2019，52(5)：430-438.

[12] Wang Liuping.Automatic tuning of PID controllers using frequency sampling filters[J].IET Control Theory & Applications，2017，11(7)：985-995.

[13] Li Hongyan.The ziegler-nichols PID parameters setting method based on the ideal relay feedback identification and its improvements[J].Advanced Materials Research，2013，2534：756-759.

[14] 宋以鹰，颜杰.一种测试电子产品关机温度的系统[J].电子技术与软件工程，2020(6)：85-86.

[15] 孙琦，于兰英，吴文海.电子产品高温试验箱的温度场分析及优化[J].中国测试，2019，45(12)：159-164.

(收稿日期：2020-12-08)

作者简介：

秦琴(1978-)，女，博士，副教授，主要研究方向：智能检测与运动控制。

姜景科(1994-)，通信作者，男，硕士研究生，主要研究方向：智能检测与运动控制、环境工程，E-mail：1548101311@qq.com。

扫码下载电子文档

版权声明