5G典型应用场景安全需求及安全防护对策

Security Requirements and Protection Countermeasures for Typical 5G Application Scenarios

闫新成/YAN Xincheng，毛玉欣/MAO Yuxin，赵红勋/ZHAO Hongxun
（中兴通讯股份有限公司，广东 深圳 518057）
(ZTE Corporation, Shenzhen 518057, China)

摘要：系统地分析了5G 3大应用场景的典型安全需求，以及5G新架构的引入所带来新的安全需求。针对性地提出了安全防护对策，包括虚拟化基础设施可信运行及资源隔离、网络安全功能服务化与按需重构、虚拟化网络切片的安全保障、统一身份管理和多元信任机制、网络服务接口的安全保障、网络功能域安全防护等，为5G网络更好地适应垂直行业差异化的安全需求提供网络安全研究、设计方面的参考。

关键词：增强移动宽带；高可靠低时延；大规模机器连接；安全功能服务化；网络切片；信任管理

Abstract: The typical security requirements for the main 5G application scenarios and new security challenges which are brought by the new 5G architecture are systematically analyzed. The security protection countermeasures are proposed, including trust operation of virtualization infrastructure and resource isolation, service-oriented and on-demand reconstruction of security network functions, network slicing security, unified identity management and multi-trust mechanisms, service based interface security, and security protection of network function domains, etc. These countermeasures provide network security research and design reference for 5G network to better adapt to the security needs of vertical industry differentiation.

Key words: enhanced mobile broadband; ultra reliable low latency; massive machine connections; security function virtualization; network slicing; trust management

DOI：10.12142/ZTETJ.201904002
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190719.1722.003.html

网络出版日期：2019-07-19
收稿日期：2019-06-20

5G作为新一代信息技术的核心引擎，力图牵引信息网络从消费互联网向工业互联网转型，实现人与机器信息化互联的愿景，打造网络与业务融合的服务模式。5G在无线接入、传输、核心网络方面采用了大量先进技术，例如丰富的接入能力、统一认证框架[1]、灵活的网络架构以及服务化的业务模式[2]。这些使得5G在技术、架构和业务等方面与3G、4G或其他无线通信系统存在很大的区别。全新的网络设计在更好地支撑多样化应用场景的同时，也将会带来全新的安全风险和需求，对现有的网络安全提出新的挑战。

5G的行业应用仍处于初步阶段，不同行业、不同业务、不同客户对于安全的需求也有着一定的差异。但我们仍然可以针对典型应用场景的共性安全需求进行分析，重新审视5G网络中新的防护对象、新的信任体系，以及对新的网络功能和新业务模式的防护。

1 5G安全需求和威胁分析

3G、4G移动通信系统重点面向移动互联网，满足个人电话、信息及数据访问等方面的需求。而5G需要同时满足以移动互联网、车联网

以及物联网为典型代表的多种应用，因此为单一接入场景而设计的安全防护机制将难以应对5G网络新的安全需求[3]。

不同垂直行业应用对5G网络的安全需求是不同的，甚至可能是相悖的，若要以相同的安全机制和策略满足所有的垂直行业要求是不现实的；因此需要以服务化思想来构建5G网络安全架构和安全基础设施，为行业用户提供按需可定制的网络服务以及差异化的安全防护能力等。

1.1 典型应用场景的典型安全需求

5G有3类主要应用场景：增强移动宽带（eMBB）、海量机器类通信（mMTC）、高可靠低时延（uRLLC）。

在eMBB应用场景下，5G网络峰值速率和用户体验速率较4G增长10倍以上[4]，这对安全基础设施的计算与处理能力提出了挑战。在网络入口处通常需要部署安全基础设施，来进行网络或业务策略的访问控制。同时，为了保护用户隐私，对数据或信息也要进行访问控制。传统安全基础设施以单设备、高性能来提升计算与处理能力，这种模式将很难适应超大流量的5G网络防护需求。因此，构建云化或服务化的安全基础设施，通过服务间的配合与协同机制来实现高性能的安全处理能力，将是未来安全基础设施提高其计算与处理能力、应对海量数据的主要途径。

在uRLLC场景下，要求端到端时延从10 ms降到1 ms[4]。典型应用包括车联网与自动化辅助驾驶、远程医疗以及工业自动化控制等。由于这类应用本身关系到人身安全或高额经济利益，因此对安全能力的要求与对网络自身能力的要求同等重要。针对这类应用的安全防护机制是严苛的，在实现高安全防护的同时不能影响到应用体验，例如传统网络架构中基于多层隧道等补丁式防护手段很难满足这类应用的要求。低时延应用需要依赖网络部署移动边缘计算（MEC）能力降低网络时延；但是MEC需要将部分原本位于运营商核心机房的功能下沉至近用户位置的网络边缘进行部署，部署位置甚至完全脱离了运营商控制区域（例如企业园区等），这增加核心设备遭受攻击的风险。

在mMTC场景下，连接密度从10万台/km^{2}增大到100万台/km^2[4]。数量的变化也会带来新的安全问题：首先，终端设备数量巨大，即使正常情况下发包频率不高，数据包也不大，但其认证过程以及正常的业务数据都有可能带来极高的瞬时业务峰值，从而引发信令风暴；其次，无人值守的终端设备一旦被劫持，可能会构成一个巨型的“僵尸网络”，进而对其他关键网络基础设施发起分布式拒绝访问服务（DDoS）攻击。因此，需要研究海量终端设备接入安全机制，加强细粒度的设备管控。

1.2 适应行业应用的新网络架构带来的安全挑战

5G在网络设计上进行了软件和硬件解耦、控制与转发分离，并引入网络切片和网络能力开放等新技术提升网络灵活性、可扩展性、可重构能力。5G服务化架构在满足不同垂直行业应用需求的同时，也引发了一些新的安全问题：

（1）安全防护对象发生变化。

5G网络基础设施云化和虚拟化，使得资源利用率和资源提供方式的灵活性大大提升，但也打破了原有以物理设备为边界的资源提供模式。在3G、4G网络中，以物理实体为核心的安全防护技术在5G网络中不再适用，需要建立起以虚拟资源和虚拟网络功能为目标的安全防护体系。

（2）信任关系由二元变为多元。

3G、4G网络的价值链中只有终端用户和网络运营商2个角色，并没有明确而完整地提出信任管理体系。5G网络与垂直行业应用的结合使得一批新的参与者、新的设备类型加入价值链。例如，传统移动网络中网络运营商通常也是基础设施供应商，而在5G时代，可能会引入虚拟移动网络运营商的角色。虚拟移动网络运营商需要从移动网络运营商/基础设施提供商中购买网络切片。相比传统网络的终端用户，5G网络除了手机用户之外，还有各种物联网（IoT）设备用户、交通工具等。因此，5G网络需要构建新的信任管理体系、研究身份和信任管理机制以解决各个角色之间的多元信任问题。

（3）集中管理带来了安全风险。

3G、4G较少地采用集中式管理方式，除了少数网元外，其他网元之间的管理更多依赖于自主协商。

5G 使用不同的网络切片来满足不同的行业应用需求，不同的切片需要分配不同的网络资源。切片管理以及与切片相关的网络资源管理不可能再基于自主协商方式，因此集中式管理将成为主要方式。5G 网络中使用网络功能虚拟化管理和编排（MANO）、软件定义网络（SDN）控制器等对网络集中编排和管理。MANO 和 SDN 属于网络中枢，一旦被非法控制或遭受攻击，将对网络造成严重影响，甚至瘫痪。集中式管理网元的安全防护问题迫切需要解决。

（4）新服务交付模式的相关安全需求。

5G 网络为了更好地应对各种不同的业务需求，接纳了新的参与角色并将其加入网络价值链与生态系统中，由此产生了新的服务交付模式[5]。5G 通过将能力开放，同时配合资源动态部署与按需组合机制，为垂直行业提供灵活、可定制的差异化网络服务。能力开放改变了传统网络以能力封闭换取能力提供者自身安全的思路，使得能力使用者通过控制协议对能力提供者发起攻击成为可能。一旦能力使用者被恶意入侵，利用能力开放接口的可编程性，经由控制接口对 5G 网络进行恶意编排，将会造成严重后果，因此新服务交付模式需要解决网络能力开放的安全防护问题。

2 5G 网络安全防护技术

2.1 安全防护对策分析

我们将上述提到的威胁和安全需求进行汇总，并列举了相应的典型安全防护对策，如表 1 所示。需要说明的是，实际上一个特定场景并非只有一种安全需求或威胁，也绝非一种安全方案就可以解决的。同样，一类解决方案也不仅限于只解决一类特定需求。这里仅列举了一些典型而重要的安全功能和方案，以便对问题进行清晰的剖析。

2.2 5G 安全关键防护技术

（1）基础设施的虚拟化隔离。

软件和硬件的解耦，网络功能虚拟化（NFV）、软件定义网络的引入，使得原来私有、封闭的专用网络设备变成标准、开放的通用设备，也使得网络防护边界变得模糊。网络虚拟化、开放化使得网络更易遭受攻击，并且集中部署的网络将导致网络威胁传播速度更快，波及更广。由于网络功能实体共享基础设施资源，因此需要其提供资源的安全隔离技术来保障上层 5G 网络功能系统运行的安全性。可以通过虚拟隔离机制来实现计算、网络、存储等资源的隔离，让承载每个网络功能实体无法突破虚拟机/容器管理器给出的资源限制。虚拟化网络的安全防护还需要保证网络基础设施的可信，这一点对于非信任环境部署的基础设施，例如基站云化、边缘计算等来说更为重要。通过可信计算技术，在网络功能实体平台上植入了硬件可信根，以构建从计算环境、基础软件到应用及服务的信任链，并依托逐级完整性检查，来实现网络功能实体的软硬件环境的完整性保护。

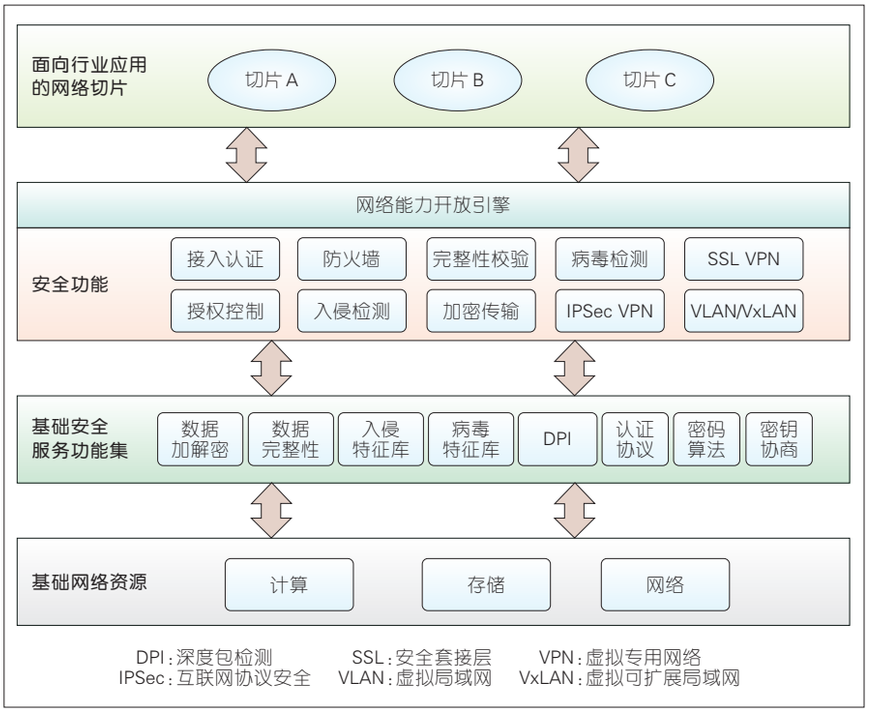
（2）网络安全功能按需重构。

5G 网络本质是一种按需定制的网络，其优势在于除了可以为各垂直行业提供差异性的连接服务之外，还能按需提供差异化的安全防护能力。通过借鉴网络功能服务化的思想，构建安全功能的服务化，如图 1 所示，并将虚拟化的安全功能按需编排到网络切片中，使安全资源、网络资源、数据资源在网络切片中独立提供，达到近似于传统私网的安全保障和用户体验。

安全功能虚拟化是按需重构的前提。通过对传统安全功能的虚拟化，可设计出适应不同应用安全需求的虚拟安全功能单元，例如防火

▼表 1 5G 安全功能/方案分析表

安全需求和威胁		典型 5G 安全功能/方案
3 大应用场景的典型安全需求	增强移动宽带	网络安全功能按需重构
	高可靠低时延	多接入边缘计算安全
	大规模机器连接	抗分布式拒绝服务攻击
满足行业应用差异化需求的服务化网络架构	安全防护对象发生变化	• 基础设施的虚拟化隔离 • 按需服务的网络安全功能 • 网络功能域安全防护
	信任关系由二元变为多元	统一身份管理和多元信任机制
	集中管理带来了安全风险	• 基础设施的虚拟化隔离 • 网络功能域安全防护
	新服务交付模式的安全需求	• 切片隔离与安全保障 • 网络安全功能按需重构 • 网络服务接口的安全保障



▲图1 安全服务虚拟化体系架构示意图

墙、接入认证、互联网协议安全（IPsec）、安全套接层（SSL）虚拟专用网络（VPN）、入侵检测、病毒检测等。各个虚拟安全功能单元通过按需调用各类基础安全服务功能集，从而满足性能可扩展、功能可裁剪等要求，实现安全功能虚拟化。

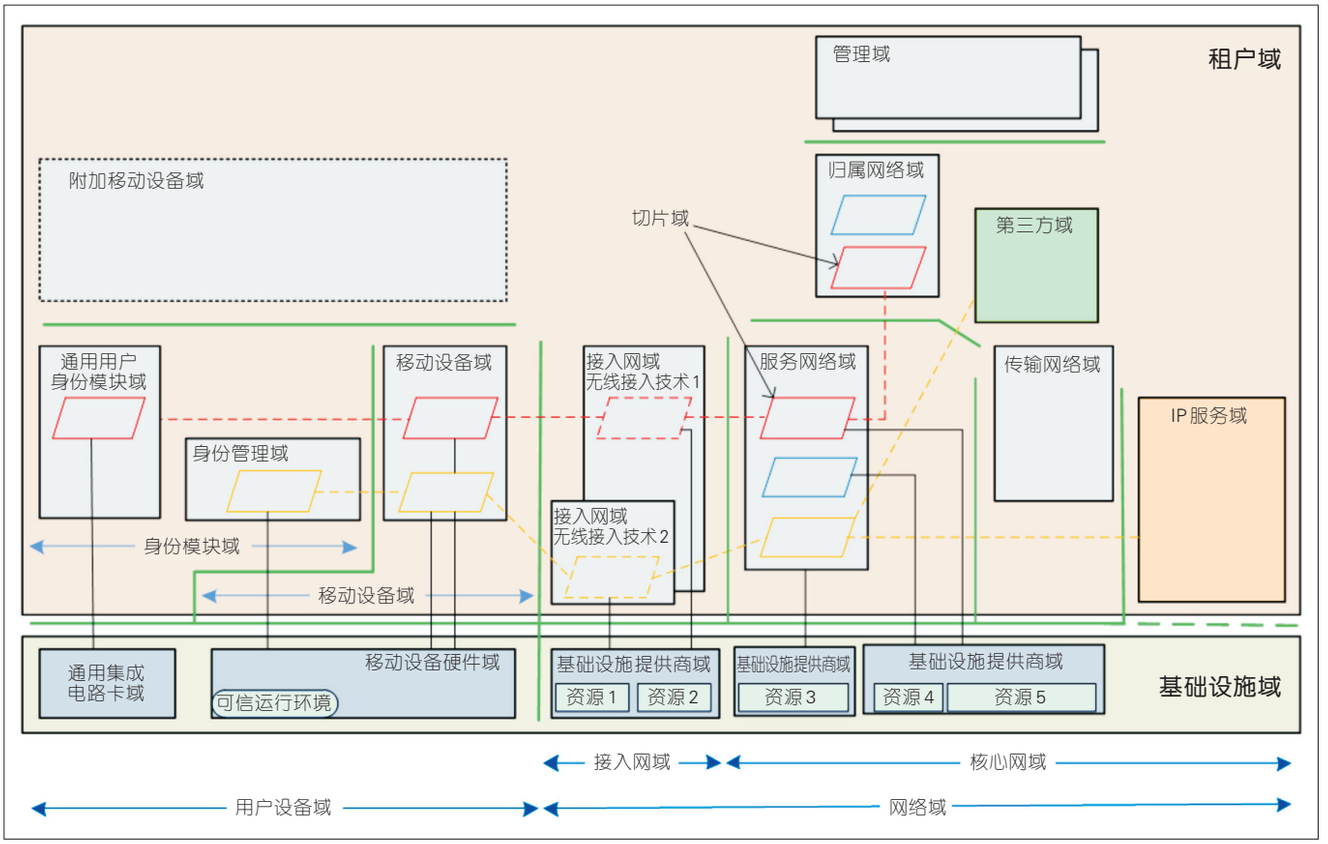
基础安全服务功能集由各类基础服务功能组成。基础服务功能的服务性能可根据应用程序编程接口（API）进行配置，以满足上层的差异化服务要求。基础服务功能再通过对基础资源层提供的虚拟化网络资源进行按需调度来实现性能的差异化配置。

行业应用需求的差异决定了网络切片功能的差异化。并非所有切片都包含相同的网络功能，有些网络功能基于需求可以不用配置。应用需求的差异性决定了切片所提供的安全服务也是差异化的。在实现网络安全服务功能虚拟化后，可以为服务于不同行业的网络切片提供网络安全功能的按需重构。例如，服务于车联网（V2X）的低时延网络切片，需要在网络边缘节点实例化一些必要的网络功能，选择适应低时延要求的认证方法、加密算法和密钥长度，以便在时延约束下提供对应的安全防护，更好地支持第三方的垂直应用；对于服务于mMTC的网络切片，仅需配置基本的控制面接入认证功能，而诸如移动性相关的网络功能则无需配置。我们还可以考虑在切片内部署虚拟的物联网网关以及安全态势感知系统，来防止DDoS攻击和威胁横向扩散。

（3）网络功能域安全防护。

网络虚拟化和网络切片的应用，使得原本用于传统移动通信网络域安全防护的架构增加了新的元素。在第3代合作伙伴（3GPP）标准中，传统“域”是指“物理实体组”，即“域”仅限于物理网络实体的划分，尤其是地理位置区域。而5G网络，尤其是5G核心网构建在虚拟化网络之上，相比传统网络又出现了虚拟网络功能实体。更进一步地，5G引入了网络切片，不同的切片有着不同运营者，5G网络的基础设施供应商和移动网络运营商也可能不同，因此我们需要将所有权属性也纳入考虑范畴。分析5G的安全威胁，需要首先将5G网络进行合理地分域；而对5G网络分域，需要将传统域的概念扩展为“与5G网络相关的物理、逻辑和运营等方面的网络功能实体组”。

根据5G网络特征，5G系统可分为基础设施域、租户域以及附加的移动设备域。每个域根据不同功能又可进一步划分为若干子域[6]，各个子域对应着相对比较独立的功能。5G系统的域划分情况如图2所示，其中绿线标记域之间的逻辑或物理通信接口，棱形表示各个域中的切片，同类切片互联以后形成切片域，为5G系统提供端到端的网络服务功能。在确定了域/子域边界后，可以针对每个域/子域进行威胁分析：针对其业务属性给出相应的防护方案，如在域/子域网络边界设置虚拟防火墙等安全防护功能，并结合防护策略为域/子域内网络功能提供安全防护。对于域/子域间如果存在通信需求，可配置IPsec、SSL VPN等为数据交互提供安全通道。



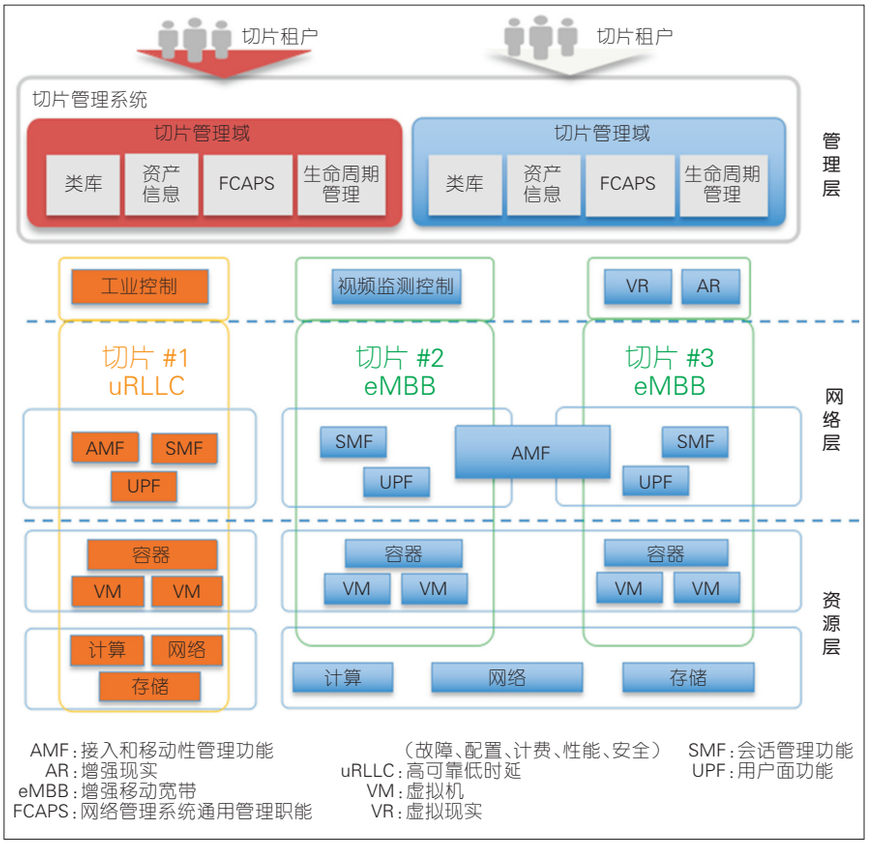
▲图2 5G网络的域划分示意

(4)切片隔离与安全保障。

网络切片是5G提供网络服务的主要形态。5G可以在相同的网络基础设施上同时构建多个网络切片,为多个应用提供差异化网络服务。网络切片使得5G组网更加灵活,网络服务更贴合应用需求;但由于共享网络基础资源,如果管理不当就会引发切片数据泄露、切片间资源竞争、非法用户接入切片等安全威胁,因此需要提供切片安全隔离技术、切片接入控制等技术。

切片安全隔离可通过切片对应基础资源层的隔离、网络层的隔离以及管理层隔离的三级隔离方式实现,如图3所示。切片在基础资源层隔离使用基于NFV技术的资源隔离技术实现,例如为不同的切片分配不同的虚拟机/容器承载切片网络功能,通过虚拟机/容器隔离机制实现切片在基础资源层的隔离,文献[7]中,作者详细描述了NFV安全隔离机制。切片在网络层的隔离分为无线接入控制(RAN)隔离、承载隔离和核心网隔离,根据切片承载的应用对安全性的要求,可以分为切片完全隔离或者切片部分隔离。例如,对于安全性要求严苛的工业控制应用,需要采取完全隔离方式,即为所述切片分配独立的网络功能;对于安全性要求不高的普通应用(如视频监测控制、上网类应用),在建立对应的网络切片时可以共享部分网络功能。参考文献[8]中,作者描述了切片在网络层的隔离实现。切片在管理层的隔离通过为使用切片的租户分配不同的账号和权限。每个租户仅能对属于自己的切片进行管理维护,而无权对其他租户的切片实施管理。另外,我们需要通过通道加密等机制保证管理接口的安全。

切片的接入控制用于保证合法用户接入正确的网络切片,防止非法用户接入网络或合法用户接入非授权切片而引发的网络攻击和破坏行为。首先,通过网络接入认证机制对附着到网络的用户进行认证鉴别,只有签约网络用户才能接入网络。在接入认证过程中,为防止攻击者仿冒签约用户的身份标识,需



▲图3 网络切片的三级隔离

要对用户身份等隐私信息进行保护，同时也需要安全机制对认证过程中的信令交互进行安全防护，防止攻击者窃听、篡改认证信息。其次，对于用户访问切片也需要进行管理和控制，可以通过签约的方式规定用户接入切片类型。在用户接入切片时，需要进行切片认证，以验证用户接入切片的权限，防止非授权用户接入切片，窃取信息或破坏切片正常运行。

（5）多接入MEC安全。

MEC是5G业务多元化的核心技术之一。MEC将部分网络服务能力和业务应用推进到网络边缘，通过业务靠近用户处理来缩短业务时延，提供可靠、极致的业务体验。

以缩短业务时延和提高资源使用效率为原则，MEC服务一般部署在边缘数据中心、基站等近用户位置，如园区和一些特定场所内。由于其物理位置脱离了运营商核心网，基础设施的物理安全不可忽略，例如出于对企业的安全考虑，要求私有云数据不出园区，因此MEC就要部署在企业网内部区域。这样虽然满足了企业的数据安全需求，但是关键网络基础设施部署脱离了运营商控制范围，对其造成了安全风险。对此运营商需要进行基础设施安全加固，例如引入门禁、环境监测控制等安全措施，对MEC设备加强自身防盗、防破坏方面的结构设计，对设备输入输出（I/O）接口、调试接口进行权限控制等。

为实现垂直行业的业务定制，MEC需要提供开放平台。但网络能力开放后，MEC对应用的注册、安全管理、行为审计等都需要制定完整的保障机制，应用的注册除了身份的合法性验证之外，还可以根据可信评估机构签发的健康度进行严格控制；对第三方业务的访问权限也需要进行严格控制，一旦发现越权的资源调度行为应及时阻断，并需要对所有访问行为实施日志记录以便安全审计。

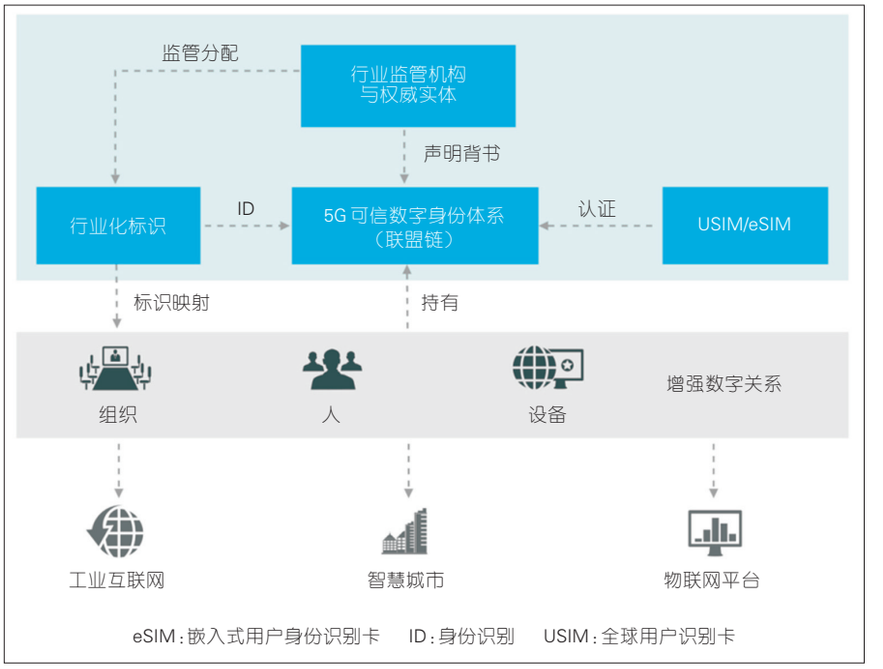
由于MEC实现业务和内容的本地化处理，用户终端在越区切换时，MEC应用的低延时通信和服务连续性所需的信息，例如移动终端的身份和网络地址，需要从切换前网络功能实例传送到目标切换的网络功能实例。在越区切换过程中，需要考虑通信安全，例如在网络功能实例间建立安全隧道以保证切换过程中的信息传送安全。目标切换的网络功能实例在完成用户越区认证后，需要将切换前网络实例传送过来的网络及业务信息进行对应绑定和切换，以确保服务的连续性。

（6）统一身份管理和多元信任机制。

5G面向垂直行业的半封闭特征，以及众多不同类型新参与者的加入（例如新行业、新商业主体、新业务类型、新机器连接等），使得基础设施提供商、运营商、第三方服务提供商、网络用户等参与者之间的信任关系变得复杂，因而需要构建用户、终端、网络、服务之间的多元信任模型，以应对不同应用场景的

信任需求[9]。

5G 支持多样化及海量的终端接入，不论是对身份管理的能力需求上，还是实现网络和业务的深度融合机制上，都需要构建新的身份管理体系。另外，5G 存在多个虚拟网络切片，需要支持网元在不同网络切片、不同网络域之间的信任关系和可信身份传递。因此，需要充分融合现有的移动通信网、不同的垂直行业、不同的物联网平台的身份管理体系，实现统一身份管理，构建统一信任服务体系。图 4 所示为保障 5G 网络、业务和服务健康前行的重要因素。



▲图 4 统一信任服务框架

统一身份管理需要解决 5G 参与者的身份标识和身份管理问题。通过标识技术对所有接入 5G 网络的实体进行唯一标识映射，实现不同层次身份标识的统一管理、融合，用户的管理、身份标识生成、签发、发布、验证等功能，解决现实空间中人、设备、应用服务等实体向网络空间的身份可信映射，实现网络空间与现实空间身份的可信对应。网络空间活动的主体可以准确地对应到现实空间中的用户，用户为其网络行为负责，解决统一身份管理、身份信息融合、隐私保护等问题。

传统移动通信网络中，网络对用户入网认证，并作为管道承载用户与服务间的业务认证，用户与网络、用户与服务分别构成二元信任模型。5G 网络下的统一身份认证服务需要结合不同业务应用的特点，以基于 eSIM 身份为基础，充分融合垂直行业标识体系、面向物联网的数字证书体系、5G 融合身份认证、跨运营商的切片联盟等身份体系，构建用户、终端、网络、服务之间的多元信任模型。在该信任模型下，根据不同业务不同行业的用户需求，可采用网络认证用户、切片认证用户（垂直行业对用户的认证）、应用认证用户以及运营商和垂直行业的认证等多元认证关系实现多元信任，实现面向 5G 网络与垂直行业的新型数字关系。

（7）网络服务接口的安全保障。

5G 网络开放能力通过运营商向垂直行业提供 API，如图 5 所示，以便垂直行业可以创建和管理服务于自身的网络切片。网络开放能力创造了网络新的营运模式，同时也为攻击者开放了攻击网络的接口。例如，如果非授权的第三方获取了访问接口，会发起针对网络的攻击；每个应用程序能够访问的 API 接口如果缺少限制，则可能导致网络核心数据会被访问和篡改。

为此，需要对网络服务接口提供安全防护，实施对垂直行业应用服务的认证，并提取评估机构签发的安全可信性的评估结果。通过审

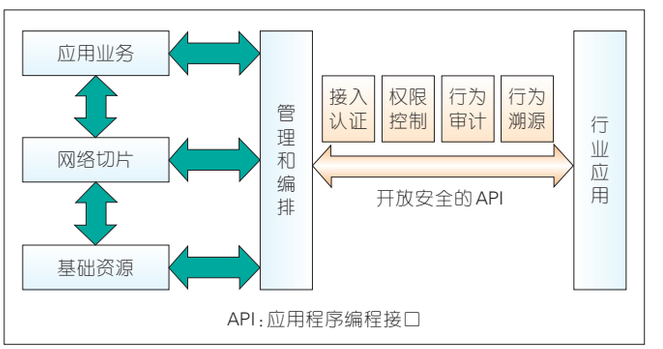


图 5▶ 网络服务接口安全保障示意图

查之后向信任基础设施获取对应服务的访问权限，对垂直行业应用在网络服务调用的全过程进行合规性监测控制，对越权访问行为进行阻断。服务接口安全防护具体措施可包括：

• 认证授权。网络通过向信任服务基础设施提交对访问应用的身份验证，根据验证的结果进行授权服务的开放，并且需要根据可信评估机构的评估数据，进行综合决策。

• 权限控制。网络通过向信任服务基础设施提交对访问应用的权限获取，并通过获取的权限进行资源的隔离控制，防止带有攻击或越权行为的发生。

• 安全审计。在应用业务接入网络后需要进行访问行为的严格安全审计与分析，对应用业务的行为实时跟踪监测，对发生的攻击或越权行为进行告警，为响应处置的策略决策提供依据。

（8）DDoS。

网络DDoS主要通过5G网络各类感知点进行海量事件的收集，包括路由交换设备上报的流量统计信息、网络编排和管理器上报的拓扑信息、安全防护功能上报的安全威胁信息，以及5G功能实体，例如接入和移动性管理功能（AMF）、会话管理功能（SMF）、用户面功能（UPF）等，上报的日志事件等，通过对搜集的海量信息进行大数据关联分析，并通过智能分析引擎完成策略决策，按照决策结果调用可重构的安全流量清洗资源池完成攻击阻断。根据大数据关联分析结果，我们对网络攻击源进行追踪溯源，并通过安全审计进行安全取证，为DDoS攻击认定提供依据。

为实现整个5G网络抗DDoS攻击，需要一个完备的动态防御体系，并建立安全模型和闭环流程，包括信息采集上报、安全策略决策、安全响应与处置等。

• 信息采集上报：需要针对网络不同域、不同逻辑层部署采集功能，完成全网信息采集。

• 威胁分析感知：通过大数据智能分析等手段，进行海量信息的综合处理，并利用安全威胁特征库来分析识别安全威胁。

• 安全策略决策：根据智能决策的理论、模型、方法，针对发生的安全威胁做出全面综合科学的响应决策。

• 安全响应与处置：根据响应决策，研究实施响应处置的方法，包括大容量威胁流量清洗、追踪溯源等，能够实时完成威胁处置等。

3 结束语

5G架构的革新使得5G网络为eMBB、mMTC、uRLLC 3个主要应用场景提供网络服务变为可能，也使得传统电信网络的安全防护体系面临挑战。为了满足5G网络自身防护需求，适应垂直行业差异化安全需求，我们需要深度分析研究5G移动通信网络及垂直行业带来的新的网络架构、业务需求，甚至全新的生态系统，采用全新安全防护理念构建全新的5G安全架构，以实现对5G网络从基础设施、网络功能、业务服务、信任关系等多个维度全方位地进行立体防护。

5G的应用和需求也才刚刚展开，我们要紧密地结合个人用户和行业用户的核心安全诉求，重视产业互联网的网络业务和网络安全建设，唯有如此，才可能让5G使能垂直行业，实现安全可靠万物互联。

参考文献

[1] 3GPP. Security Architecture and Procedures for 5G System: 3GPP TS 33.501[S]. 2019
[2] 3GPP. System Architecture for the 5G System: 3GPP TS 23.501[S]. 2019
[3] 陆平,李建华,赵维铎. 5G在垂直行业中的应用[J]. 中兴通讯技术, 25(1):67–74. DOI: 10.12142/ZTETJ.20190111
[4] IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond[R]. ITU–R, 2015
[5] 5G网络安全需求与架构白皮书[R]. IMT–2020, 2017
[6] 5G–ENSURE_Deliverable D2.7 Security Architecture (Final) [R]. 5GPPP, 2017
[7] 基于SDN/NFV的电信网安全技术白皮书[R]. SDN/NFV产业联盟, 2018
[8] 5G Security White Paper: Security Makes 5G Go Further[R]. GSMA, 2019
[9] 5G信息安全白皮书[R]. 未来移动通信论坛, 2017

作 者 简 介

闫新成，中兴通讯股份有限公司高级工程师、安全技术专家委员会主任，国家科技专家委员会专家委员，国家科技重大专项5G网络安全任务负责人；主要研究方向为5G网络安全，具体负责中兴通讯网络安全技术研究和规划工作。

毛玉欣，中兴通讯股份有限公司高级工程师、安全技术专家委员会委员；主要研究方向为5G网络安全、网络虚拟化安全；拥有10余项发明专利和国际标准提案。

赵红勋，中兴通讯股份有限公司软件研发资深专家、项目经理；主要研究方向为5G网络安全、网络虚拟化安全，从事5G网络安全产品研发和架构设计工作。