

5G 网络切片安全研究

孙同伦

(中国移动通信集团广东有限公司中山分公司, 广东 中山 528403)

摘要: 在科学技术日益进步和社会经济快速发展的背景下, 人们对网络安全提出了更严格的要求。基于此, 阐述了网络切片技术的含义, 分析了 5G 网络切片技术的安全架构, 介绍了 5G 网络切片安全应用的必要性, 深入研究了 5G 网络切片技术的各部分需求, 提出了保证 5G 网络切片安全开展的措施, 旨在为相关人士提供参考建议, 进一步推动我国通信事业的蓬勃发展。

关键词: 5G 网络; 切片安全; 技术研究

中图分类号: TN929.5 **文献标识码:** A **文章编号:** 1003-9767 (2019) 05-193-02

5G Network Slice Security Research

Sun Tonglun

(Zhongshan Branch of China Mobile Communications Group Guangdong Co., Ltd., Zhongshan Guangdong 528403, China)

Abstract: In the context of the increasing progress of science and technology and the rapid development of social economy, people put forward stricter requirements for network security. Based on this, the meaning of network slicing technology is elaborated, the security architecture of 5G network slicing technology is analyzed, the necessity of 5G network slicing security application is introduced, the requirements of each part of 5G network slicing technology are deeply studied, and the measures to ensure the security of 5G network slicing are put forward. The purpose is to provide reference suggestions for relevant persons and further promote the vigorous development of communication industry in China.

Key words: 5G network; slicing security; technology research

0 引言

随着互联网、物联网和各种应用的不断出现, 人们对流量分布、连接数量和管理移动等提出了更高的要求。在这种情况下, 人们研发了 5G 通信技术, 不仅可以优化社会大众在互联网环境下的体验度, 而且可以满足物联网的多元化需求, 缩减了网络运营的成本。

1 网络切片技术概述

将某个物理网络分割成无数个虚拟终端的过程叫做网络切片技术。这些虚拟终端内的接入设备、传输设备和中心网络在逻辑上相互独立, 若某一个虚拟终端发生问题, 其他虚拟终端仍然可以正常工作。5G 网络通信技术按照应用场景可以划分为移动宽带网络、物联网海量网络 and 关键性任务物联网。这三个场景所对应服务主体的需求不同, 需要大批量设备接入网络, 此刻, 5G 网络切片将以多个虚拟终端为目标详细分割物理网络, 用于满足不同场景的需求^[1]。

2 5G 网络切片安全的总体架构

保障系统信息安全的结构化架构是 5G 网络切片安全的总

架构。架构中各模块的安全性较强, 是系统设计研发的重要保障。这种通信安全技术突破了传统通信系统的固有限制, 实现了安全与通信技术的同步发展, 极大程度落实了内部系统和外部环境的实时安全治理。由此可见, 设计 5G 网络切片安全总体架构时, 需要以“可塑性”和“拓展性”为基础, 为其未来的发展创造良好环境。5G 网络切片的架构逻辑如图 1 所示。

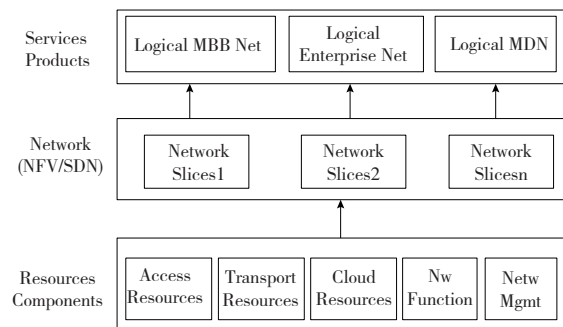


图 1 5G 网络切片的架构逻辑

3 应用 5G 网络切片安全管理的意义

第一, 国际电联电信标准化部门定义通信系统的安全管

作者简介: 孙同伦 (1979—), 男, 安徽淮南人, 硕士研究生, 中级工程师。研究方向: 移动通信网络关键技术与网络运营管理。

理时,将通信和内容作为安全管理的基础,完善安全管理体系。这不仅可以优化通信网络的总体环境,提升安全系数,而且可以保障信息处理在健康的环境下开展。安全管理主要包含认证网络、授权网络、审计网络、用户访问资源的合理控制、安全管理和配置等方面的内容。但是,互联网技术加入5G通信技术的过程中增加了一定风险,需要通过切片安全管理监督和优化网络环境^[2]。

第二,5G网络切片安全管理的解决能力较强,可以满足通信网络的特有需求。信息通信技术有效融合的氛围下,5G网络通信技术获得了一定的发展机遇。其实现了SDN技术和NFV技术的有效融合,但会造成一些负面影响,如频繁的网络攻击和网络威胁等。随着多方位应用场景和虚拟技术的联合使用,模糊了安全的边界,具体表现为两个方面。一是无处不在的攻击危机。攻击主体或目标在5G网络环境下被物联网放大,攻击路径被短时间扩张,且SDN技术控制设备的防控能力降低,可能导致网络瘫痪。二是模糊的安全界限。网络常规的安全界限已经在分割后的架构中弱化,新的安全界限需要重新判定,且各个租户没有明确的物理界限,易产生信任危机。

4 5G网络切片安全的相关研究

基于5G网络环境重新架构的切片具有较强的虚拟化,主要原因在于NFV技术,但其可以提升网络环境的可缩性和灵动性。网络功能虚拟化(NFV)由十几家运营商在2013年发起,欧洲电信标准化协会(ETSI)将其定义为一种竖井机制。网络功能虚拟化能够以虚拟技术为基础,突破传统电信设施的限制,其中心主旨是引入新的管理机制——MANO。网络功能虚拟化基础设施解决方案(NFVI)由虚拟资源、硬件资源和虚拟层构成,能够为VNF供应相应资源。MANO管理机制的引入可以为NFVI机构管理提供更多方式,如虚拟资源的VNF分配、虚拟资源的上报和监督硬件故障等。SDN技术可以集中控制硬件设备的数据,优化网络的灵活性。

4.1 NFV对于安全的需求

网络功能虚拟化的安全需求在于提升VNF软件的安全管理能力,把控该软件的访问权限,保护私密数据。网络功能虚拟化对于安全的需求还包括安全通信的相关需求(如通信双方认证等)和网络组建安全的相关需求(如安全区域识别、阻隔流量等)。

4.2 SDN对于安全的需求

软件定义网络(SDN)对于安全的需求主要有以下四点。第一,应用层面的需求。计算机应用程序需要认证控制器身份和通信机制,以保护通信的私密性,计算机应用程序也要加强安全系数,提升应对恶意攻击的能力。第二,控制设备的需求。软件定义网络的控制设备需要具备限制速度和防护的能力。它不仅可以加固控制设备服务器的安全,而且可以利用检查工具排查网络环境,如各类杀毒软件和杀毒工具等,提升系统修复

安全漏洞的能力。另外,这种控制设备需要具备检测冲突的能力,为管理和执行安全策略创造条件。第三,转发层面的需求。通信网络可以对ACL、不必要的服务或端口进行关闭处理,可以及时修补漏洞,强化设备安全性能,同时,转发器可以实现限速功能。第四,接口的需求。位于南北向的接口设备需要进行双向验证,保护通信内容的完整度,减少重复率。

4.3 网络切片对于隔离的安全需求

第一,不同的网络切片实例可以提供不同的隔离体系,降低其他网络节点混入本切片资源的验证访问。以医疗行业的网络切片为例,由于网络中患者的隐私性较强,只希望医生进行定向查看,其他网络切片人员不能查阅。第二,同类型的网络切片具有隔离性。以不同公司使用相同业务的网络切片为例,本公司的资源不想被其他网络切片的公司访问。第三,只有网络切片隔离保护信息数据的效果与传统物联网一致,才能够消除使用者的戒心,保证信息数据的私密性。第四,网络切片内的授权和认证。决定管理网络切片中的某项资源是否授权于第三方时,需要二次认证和融合授权控制^[3]。

4.4 网络切片安全

5G网络体系中,网络切片占据重要位置,其可以促使运营商满足市场的个性化定制需求,提升解决方案的科学性,比如功能需求、性能需求和隔离需求等。基于网络切片环境下的安全隐患通常由共享网络功能和隔离切片组成,但某些网络切片环境可以为第三方运行创造条件,尤其是某些公司的特别管理需求,充分证明了网络切片中隔离性的重要。据了解,5G通信网络可以介入的业务模型种类较多,比如3GPP连入系统、非3GPP连入系统、可信网络和不可信网络都可连接5G网络技术,且不同种类的网络切片可以连入不同的服务。基于5G网络环境下的网络切片能够为网络提供不同安全系数的保护,可以根据需求组建网络和划分安全等级。简单来说,可以在安全等级分化的切片网络中实施安全技术,以业务需求和业务环境为基础隔断、分化切片网络环境,继而提升网络切片间的安全通信能力和接口认证能力。

5 结语

未来,5G通信技术会应用于各种各样的业务环境。由于业务种类不同,因此提供的安全服务也不相同。5G通信技术可以为多层次切片创造一个安全的生存环境,满足业务间的差异化安全需求,提升5G网络通信的可靠性和稳定性。现阶段,相关部门应以切片的安全性为基础开展后续工作。

参考文献

- [1] 李侠宇,沈鸿.5G网络安全发展趋势研究[J].电信网技术,2016(12):42-44.
- [2] 李硕,蔡世杰.5G网络安全需求分析[J].中国安防,2017(12):72-75.
- [3] 李雪永.浅析5G网络切片安全[J].现代信息科技,2018,2(4):72-73.