

软件定义 5G 通信网络的虚拟化与切片安全

Virtualization and Slice Security of Software-Defined 5G Communication Network

罗珂榕/LUO Yurong, 曹进/CAO Jin, 李晖/LI Hui

(西安电子科技大学, 陕西 西安 710071)
(Xidian University, Xi'an 710071, China)



摘要: 软件定义网络(SDN)的虚拟化与网络切片能支持 5G 网络多元服务及业务模型,并在功能、性能和安全保护方面提供差异化的技术方案。第3代合作伙伴计划(3GPP)组织已经深入研究了网络切片并在各个方面对其进行标准化。介绍了软件定义 5G 网络的虚拟化与切片的发展情况,分析了其中潜在的安全问题与相应的解决方案,并对网络切片的安全研究方向和未来的技术发展进行了展望。

关键词: 5G 安全;网络切片;SDN;网络功能虚拟化

Abstract: Software-defined network (SDN) virtualization and network slicing can support 5G network multiple services and business models, and provide differentiated technical solutions in terms of functionality, performance and security. The 3rd Generation Partnership Project (3GPP) organization has delved into network slicing and standardized it in all aspects. In this paper, the development of virtualization and slicing of software-defined 5G networks are introduced, and the potential security issues and solutions are analyzed. Finally, the security research directions and future technology development of network slicing are put forward.

Key words: 5G security; network slice; SDN; network function virtualization

DOI: 10.12142/ZTETJ.201904006

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.TN.20190703.1554.002.html>

网络出版日期: 2019-07-04

收稿日期: 2019-05-25

1 5G 面临的挑战及网络切片技术简介

1.1 5G 的发展与挑战

2016年3月,第3代合作伙伴计划(3GPP)组织启动R14 5G标准研究项目,5G技术标准研究全面启动;2017年12月完成非独立组网(NR)标准;至2018年6月,3GPP组

织确定了5G独立组网(SR)功能冻结,标志着5G的首个正式标准R15诞生。目前,5G已经完成全功能标准化工作的第1阶段。一些机构已经完成5G关键技术、R15技术标准和核心频段等方面的技术验证,实验性商业网络也已进入实用测试阶段,预计2020年正式推出商用服务。5G网络可实现2G、3G、4G、WiFi等接入的无缝集成,提供超过10 Gbit/s的速度、低延迟、高可靠性、超高密度用户容量、高移动性等

功能支持。

3GPP组织定义了5G服务描述及需求^[1],超过74项服务和技术要求被分为3大类:即增强移动宽带(eMBB)、海量机器类通信(mMTC)、高可靠低时延通信(uRLLC)。5G核心网能同时支持这些应用场景,灵活性和适应性是其关键特征。在5G时代,数十亿台设备将连接到网络,但不同类型的设备和应用场景具有不同的网络要求,如何满足同一网络物理设施上

基金项目: 国家重点研发计划(2017YFB0802700)、国家自然科学基金(61772404, U1836203)

的不同业务的服务质量(QoS)要求是5G技术关键点。3GPP已经为运营商定义了专用核心网络功能,以部署支持高数据速率移动宽带和低数据速率窄带(NB)物联网等服务的网络;但灵活性的进一步提高,需要通过网络切片及相关技术来进一步实现。

1.2 网络切片技术简介

网络切片指将底层公共物理网络分成多个端到端(E2E)的逻辑网络。这些逻辑网络是相互隔离,独立管理并且按照需求创建,即在逻辑上将物理基础架构内的一组虚拟化网络功能(VNF)分开,以构建专用和定制的虚拟逻辑网络。网络切片根据用户需求调用不同的功能模块,实现定制化的服务。目前网络切片在物联网、关键通信网、eMBB等场景下已得到广泛运用。

在切片之前,各类网络资源需

形成整体统一管理,再进一步分割实现网络切片。资源的统一和网络的分割是基于软件定义网络(SDN)和网络功能虚拟化(NFV)实现的。网络切片包括横向切片和纵向切片,首先横向分为不同的虚拟网络功能,然后根据服务需求对这些虚拟网络功能进行纵向切片以得到不同的网络子切片^[2]。网络切片在5G网络中部署示例如图1所示,其中控制平面(CP)是传送控制信令的通道,用户平面(UP)是传送用户数据的通道。网络切片由服务实例层、网络实例层及资源层组成,每种服务由一个服务实例表示。服务运营商利用切片规划生成网络切片实例,切片实例则可以被多个服务实例所共享。网络切片可以为5G环境下差异化需求的应用场景提供灵活的适应方案,但网络切片实例的选择/部署、切片资源的管理、隔离与切片的移动性都存在一些安全问

题亟待解决。

2 网络切片技术

2.1 SDN 技术简介

作为网络切片的支撑技术之一,SDN技术可实现网络数据与控制分层,并设计了2个平面之间的开放接口,实现网络的灵活定义。SDN的概念最早由斯坦福大学的N. MCKEOWN教授所定义,它通过解耦网络控制及网络转发,构建开放、易修改、可编程的网络架构体系,使网络功能软件化,为用户提供开放的网络环境。其原理是将紧密绑定在单个网络设备中的控制权迁移到可访问的计算设备,使底层基础设施能够对应用程序和网络服务进行抽象,从而将网络视为逻辑或虚拟实体。首次建立SDN逻辑架构的、为负责定制SDN接口标准的开放网络基金会(ONF),在其发布

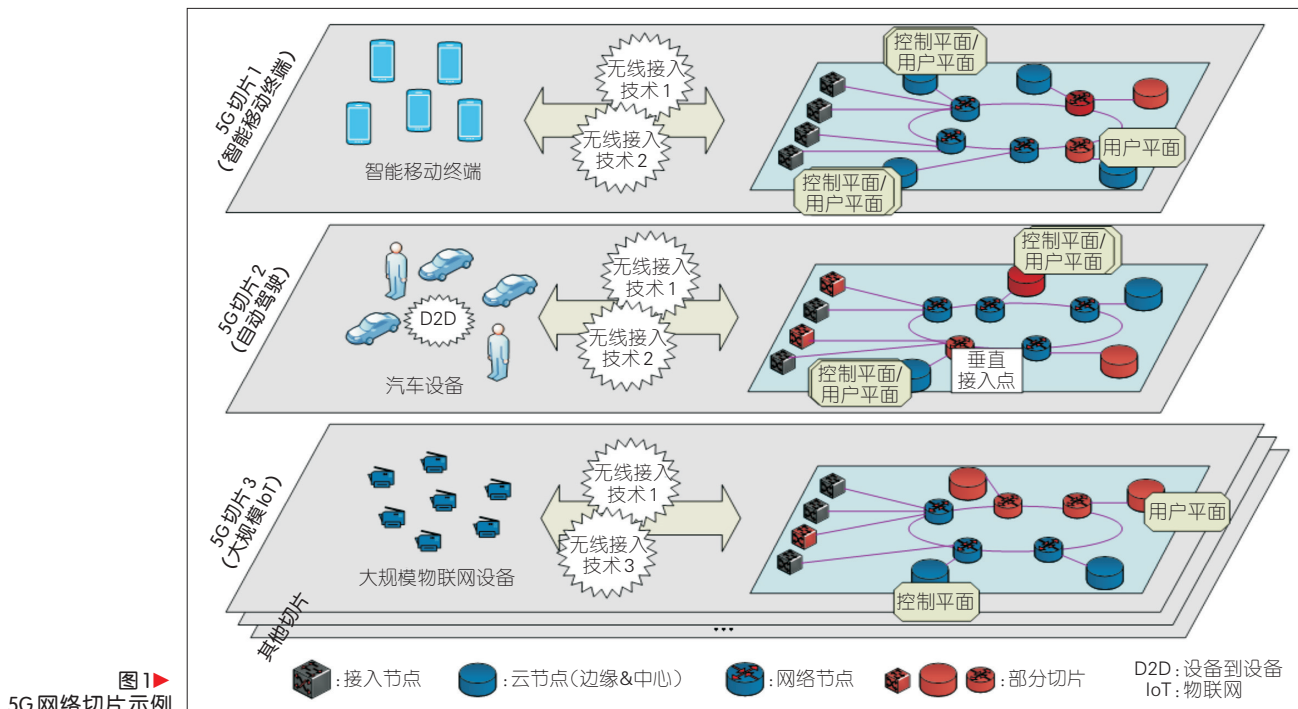


图1 5G网络切片示例

SDN 白皮书^[3]中提出的 SDN 架构被目前学术界和产业界普遍认可。

如图 2 所示,SDN 架构由 3 个平面组成,由下至上分别为基础设施层、控制层及应用层。基础设施层是由各类网络设备构成的底层网络,可以是一组用于转发网络流量的数据中心交换机和路由器,网络虚拟化功能通过控制层的 SDN 控制器在该层进行部署。控制层是 SDN 的控制平面,智能逻辑单元将部署于网络控制设施上,业务逻辑在控制器中获取和维护不同类型的网络、状态、拓扑、统计信息等。SDN 控制器用于管理网络,因此它必须具备现实网络使用环境的控制单元,如交换机、路由器、2 层虚拟专用网络(VPN)、3 层 VPN、防火墙安全规则、域名系统(DNS)、动态主机配置协议(DHCP)和群集等。控

制层位于中间,开放了北向和南向 2 种接口。北向接口用于与应用层通信,通常通过 SDN 控制器的 REST 应用程序编程接口(API)实现;南向接口用于与底层基础设施层的网络单元通信,通常通过南向协议,如 OpenFlow、NetConf、开放虚拟交换机数据库(OVSDB)等实现。应用层是利用网络拓扑、状态、统计等网络信息,开发创新应用程序的开放区域。服务提供商可以开发与网络自动化、网配置和管理、策略和安全等相关的应用程序,并为实用企业和数据中心网络提供各种端到端的解决方案。

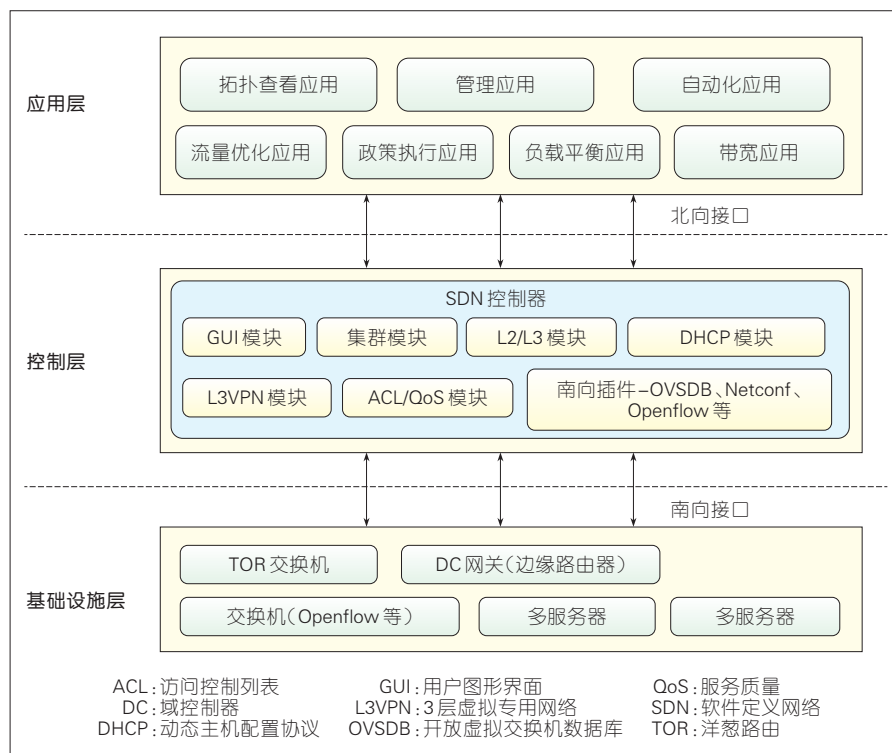
SDN 的目标是集中网络控制,提供更高的可视性和灵活性来管理网络并优化其性能^[4]。与覆盖网络方案相比,SDN 不仅能够控制选定的一组节点,还能够使用公共网络

传输数据。此外,SDN 不需要网络运营商暂时为特定的用例创建适当的覆盖网络。相反,它提供了一个固有的程序框架,用于托管集中开发的控制和安全应用程序,同时考虑到物联网要求,确保用户的体验质量(QoE)。但正因为 SDN 采用集中式控制机制,需由控制器集中完成路由设计。该机制适用于小规模网络,大规模网络下需要由多个控制器控制,因此 SDN 集中控制架构在扩展性、稳定性方面仍存在较大的挑战。此外,由于 SDN 的控制器开源和开放的特性,亟待建立一套隔离、防护机制来确保架构安全稳定的运行,其中包括控制器自身的安全管控问题,以及控制器与应用层之间以及控制器和转发设备之间安全通信问题。

2.2 NFV 技术简介

当前的网络服务依赖于专用设备 and 网络设备,这会导致网络骨化问题^[5],阻碍服务添加、更新和网络升级。为解决该问题并降低资本支出和运营成本,欧洲电信标准化组织(ETSI)提出了 NFV^[6]来虚拟化由某些专有、专用硬件设施执行的网络功能,旨在提高部署灵活性和新网络服务的集成度,提高运营商网络内的灵活性。

NFV 本质是将网络功能从基于专用硬件的独立空间定位到在云环境中运行的软件设备或通用商用服务器上。通过使用 NFV,每个传统网络功能(NF)生成 1:1 映射模型在虚拟机(VM)上运行,或者被分解为虚拟网络功能组件(VNFC)在多



▲图 2 SDN 架构

个 VM 上运行,如 1:N 映射模型。NFV 逻辑架构如图 3 所示,VNF 为 NF 的实现,在 NFV 设施上部署和执行。NFV 设施由虚拟资源组成,虚拟资源通过虚拟化层从底层硬件资源(计算、存储和网络)抽象和逻辑分区形成。NFV 管理和协调器负责编排和管理 VNF。NFV 协调器负责网络服务生命周期管理及新网络服务的加入等。此外,NFV 管理和协调器还允许与外部运营和业务支持系统集成。

SDN 和 NFV 由不同的社区和组织推广,它们有许多共同属性并高度互补。NFV 可以通过虚拟化 SDN 元素在云中运行来服务 SDN,从而允许这些组件动态迁移到它们的最佳位置。SDN 则通过在 VNF 之间提供可编程网络连接从而服务 NFV,以实现优化的流量工程和转向^[5]。SDN 和 NFV 框架并不相互依赖,NFV 可以在没有 SDN 的情况下完成虚拟化和部署网络功能,反之

亦然。图 3 中也给出了将 SDN 元素映射到 NFV 架构框架的示例,SDN 元素可以位于 NFV 框架中的不同位置。SDN 和 NFV 的结合实现了网络功能的动态、灵活部署和按需扩展,这是未来移动分组核心向 5G 系统发展所必需的。这些特征也促进了网络切片和服务功能链的进一步发展。

3 5G 网络切片安全问题及解决方案

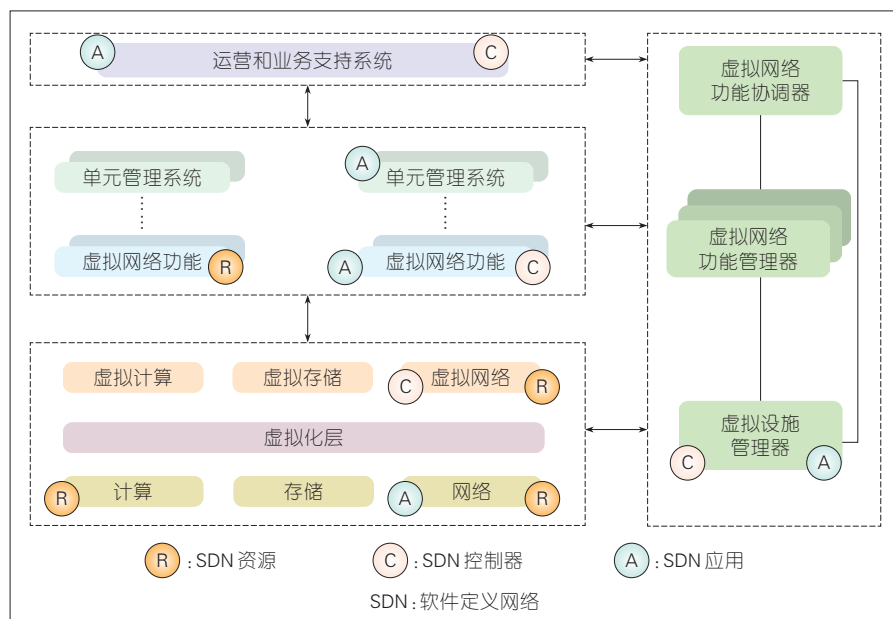
3.1 安全问题概述

由于网络切片之间的资源共享性和网络可编程性的接口的开放性,网络切片安全给 5G 发展带来挑战。各类服务的网络切片可能具有不同的安全需求并采用差异化的安全协议和机制。此外,当在不同管理域的基础设施上执行网络切片时,网络切片安全协议和方案的设计变得更加复杂^[7]。3GPP 已经对

5G 中的网络切片及虚拟化技术的安全问题进行分析^[8-9],并提出各类问题的解决方案建议,例如 3GPP 组织提出了 5G 二次认证机制以实现切片特定的认证和授权^[10]。在网络切片及虚拟化方面存在以下关键安全问题需要研究。

(1)管理接口的访问授权保护方案。网络切片支持运营商为客户提供定制服务,通信服务运营商/通信服务管理功能(CSP/CSMF)将服务需求转换为与网络切片需求,并通过切片管理接口通知运营商网络的网络切片管理功能(NSMF)。由于切片管理接口传输了大量的切片管理消息,例如激活、停止、修改、删除网络片实例产生的消息,因此需要对切片管理接口进行安全保护。保证只有授权对象才能创建、更改和删除网络切片实例,通信服务用户(CSC)和接入网络之间的相互认证和密钥协商也需要设置在连接到切片管理接口之前。运营商可以为用户提供切片即服务(NSaaS)中描述的定制服务^[11],CSC 可能需要指定网络切片特征,并且希望管理网络片,故 CSC 与 CSP 之间需要安全的协商通道。此外,应设计数据完整性和机密性保护机制以保障切片管理消息的安全性。

(2)切片实例管理及反馈消息的安全保护。在网络切片实例(NSI)的管理操作期间,监管和性能报告可以触发修改 NSI^[12],篡改的结果可能导致危害性或不适当的 NSI 修改,例如 NSI 成分的创建或修改,因此保护监管报告数据的完整性非常重要。此外,还需要保护监督和



▲图 3 网络功能虚拟化逻辑架构及 SDN 元素映射示例

报告数据的机密性,因为如果信息以明文形式发送,则攻击者能够提取如切片拓扑结构等敏感信息。

(3)网络切片子网模板(NSST)的安全保护。在创建切片实例期间将使用NSST^[8],模板描述了该切片的组成、连接结构和网络切片子网的配置,以及基于模板的配置实例所需的网络能力和其他有效信息。应保障NSST的保密性并检测可能创建受损NSI的篡改模板,以防攻击者获取有关正在运行的NSI的拓扑和配置等敏感信息。还应验证模板的来源及保护模板的正确性、完整性,以防非法成员提供伪造或篡改的NSST,导致切片实例的创建错误或失败。

3.2 网络切片安全保护方案

针对以上潜在威胁,3GPP提出了5G网络切片及虚拟化中管理、部署、接口通信和安全程序方案^[8-12]。在CSMF和NSMF的相互认证建议采用基于安全传输层协议(TLS)的客户端和服务端证书,或基于TLS-相移键控(PSK)的预共享密钥,其中PSK的密钥分发方案取决于运营商的安全策略。访问管理功能(MF)的授权是基于OAuth架构实现的,该方案能提供适用于关键问题(1)、(2)和(3)的一般授权过程,实现了NSI中监管和性能报告、NSST及切片特征协商过程的安全保护。

同时,也有许多学者提出一些新技术支撑的切片安全保护方案。为在多运营商切片创建过程中相互建立运营商之间的信任关系,J.

BACKMAN等人^[13]提出了区块链切片租赁的概念,在区块链中使用5G网络切片代理来简化服务创建过程,并帮助制造设备自主获取相关切片。HAN B.^[14]等人基于遗传算法,将切片管理策略转为二进制序列以适应切片请求及决策方案,提出了一种长期在线切片安全管理方案。为明确定义5G网络切片服务的安全性差异,NIU B.等人^[15]给出了网络切片信任度方案,并提供了信任度计算模型,其中网络切片信任值可以分为:网络切片主观信任值、网络切片历史信任值和奖惩值,由网络切片管理器根据不同的安全要求计算得到。P. SCHNEIDER等人^[16]为高敏感的第三方服务提供了5G移动网络切片安全隔离模型。ZHANG Y.等人^[17-19]分别利用消息认证码、同态签名以及聚合签名提出了适用于5G智能电网及车联网切片隐私感知功率注入方案。NI J.等人^[20]基于组签名技术提出了一个网络切片和面向服务的认证框架,通过集成网络切片,用户可以与5G运营商和物联网服务提供商建立信任,在切片上发送服务数据。目前中国缺乏切片安全保护相关机制的研究,仍有很多安全问题亟待解决。

3.3 5G网络切片安全研究趋势

尽管3GPP组织及行业研究者提出了以上的网络切片安全解决方案,但在网络切片安全中还有一些关键问题需要后续研究,以下为部分关键问题:

(1)针对不同类型的网络切片的差异化安全保护机制。不同类型

服务的切片可能具有不同的安全需求,并且需要为网络切片之间提供安全隔离,以防攻击扩散至多个切片,因此同时为差异化网络切片提供不同级别的安全保护是一个关键问题。此外,用户可以通过无线网络同时访问多个核心网络切片;但某些切片可能是矛盾的,应设计访问控制机制能够限制2种矛盾服务的并行提供。此外,有必要采用差异化的切片认证机制来满足特定的安全级别和QoS要求。由二次认证机制提供的可扩展的身份验证协议(EAP)框架可以兼容各种不同的认证方法。但若在EAP架构中的不同切片服务中采用多种独立的认证机制,会增加系统的复杂性,并可能导致计算存储资源有限的终端的大量能量消耗。因此,需要通用、安全且可灵活解构组合的身份认证框架,以便为5G网络中的切片服务提供全面和细粒度的支持。

(2)针对大规模切片安全管理机制。随着5G服务种类的多样化与细粒度划分,网络切片的数量也将急剧增长,甚至将加入大量的“微切片”,因此需要设计适合大规模网络切片的高效安全管理机制。网络切片可以根据提供服务的特征进行划分,在提供相同特征的前提下,还可以进一步通过切片对用户进行分组。在同一组切片内,网络切片可以协同服务于用户,以实现信令和服务优化,设计相应的组认证、组安全管理和组成员更新机制可以提高管理效率。其中,3GPP组织所提出的切片认证即二次认证方案只能适用于单用户的一或多切片的认证,

并需要较多的信令传输开销。当大规模用户并发请求切片认证或授权时,可能会造成信令拥塞,因此也需研究针对大规模切片群认证方案。

(3) 适应于演进分组核心网(EPC)和5G核心网(5GC)之间安全切换及安全互连机制。如果用户已经在EPC中建立了一组活动的分组数据网络(PDN)连接时,用户已经由核心网分配相应的单切片选择辅助信息(S-NSSAI),那么当用户从EPC移动到5GC时,与PDN连接有关的所有切片仍然需要在用户和接入/移动管理功能(AMF)之间服务,反之亦然。因此,应在EPC中的移动管理实体(MME)和5GC中的AMF之间设计相应的安全切换认证及通信保护机制,以确保切片实现无缝移动性。

4 结束语

5G移动网络即将启动商用,网络虚拟化及软件定义的网络切片可以很好地提高5G差异化服务部署的灵活性和开放性。3GPP组织一直致力于对网络切片管理及应用进行全面的标准化,强调、分析了其中潜在的安全威胁,研究者也在积极参与5G网络切片安全问题的研究,并提出一些建议的解决方案;但是目前仍存在大量的安全问题需要进一步关注、研究和解决。

参考文献

- [1] 3GPP. Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers for Critical Communications; Stage 1 (Rel 14): 3GPP TR 22.862 V14.1.0[S]. 2016
- [2] GUAN W Q, WEN X M, WANG L H, et al. A Service-Oriented Deployment Policy of End-To-End Network Slicing Based on Complex Network Theory[J]. IEEE Access, 2018, (6): 19691. DOI:10.1109/access.2018.2822398
- [3] Open Networking Foundation. Software-Defined Networking: The New Norm for Networks. ONF White Paper [EB/OL]. (2012-10-15)[2019-05-20]. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>
- [4] BANNOUR F, SOUHI S, MELLOUK A. Distributed SDN Control: Survey, Taxonomy, and Challenges[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 333. DOI: 10.1109/comst.2017.2782482
- [5] LI Y, CHEN M. Software-Defined Network Function Virtualization: A Survey[J]. IEEE Access, 2015, (3): 2542. DOI: 10.1109/ACCESS.2015.2499271
- [6] ETSI. Network functions virtualisation. NFV White Paper [EB/OL]. (2012-11)[2019-05-20]. http://portal.etsi.org/NFV/NFV_White_Paper.pdf
- [7] LI X, SAMAKA M, CHAN H A, et al. Network Slicing for 5G: Challenges and Opportunities [J]. IEEE Internet Computing, 2017, 21(5): 20. DOI:10.1109/mic.2017.3481355
- [8] 3GPP. Technical Specification Group Services and System Aspects; Telecommunication Management; Study on Management and Orchestration of Network Slicing for Next Generation Network (Rel 15): 3GPP TR 28.801 V15.1.0[S]. 2018
- [9] 3GPP. Technical Specification Group Services and System Aspects; Study on Security Aspects of 5G Network Slicing Management (Rel 15): 3GPP TR 33.811 V15.0.0[S]. 2018
- [10] 3GPP. Technical Specification Group Services and System Aspects; Study on Enhancement of Network Slicing (Rel 16): 3GPP TR 23.740 V0.5.0[S]. 2018
- [11] 3GPP. Technical Specification Group Services and System Aspects; Management and Orchestration; Concepts, Use Cases and Requirements (Rel 15): 3GPP TS 28.530 V15.1.0[S]. 2018
- [12] 3GPP. Technical Specification Group Services and System Aspects; Management and Orchestration; Provisioning (Rel 16): 3GPP TS 28.531 V16.1.0[S]. 2019
- [13] BACKMAN J, YRJOLA S, VALTANEN K, et al. Blockchain Network Slice Broker in 5G: Slice Leasing in Factory of the Future Use Case[C]//2017 Internet of Things Business Models, Users, and Networks. USA: IEEE, 2017. DOI: 10.1109/ctte.2017.8260929
- [14] HAN B, JI L H, SCHOTTEN H D. Slice as an Evolutionary Service: Genetic Optimization for Inter-Slice Resource Management in 5G Networks[J]. IEEE Access, 2018, (6): 33137. DOI:10.1109/access.2018.2846543
- [15] NIU B, YOU W, TANG H B, et al. 5G Network Slice Security Trust Degree Calculation Model [C]//2017 3rd IEEE International Conference on Computer and Communications (ICCC). USA: IEEE, 2017. DOI:10.1109/comppcomm.2017.8322724
- [16] SCHNEIDER P, MANNWEILER C, KERBOEUF S. Providing Strong 5G Mobile Network Slice Isolation for Highly Sensitive Third-Party Services[C]//2018 IEEE Wireless Communications and Networking Conference (WCNC) 2018. USA: IEEE, 2018. DOI: 10.1109/wcnc.2018.8377166
- [17] ZHANG Y, ZHAO J, ZHENG D. Efficient and Privacy-Aware Power Injection over AMI and Smart Grid Slice in Future 5G Networks[J]. Mobile Information Systems, 2017: 1-11. DOI: 10.1155/2017/3680671
- [18] ZHANG Y H, ZHENG D, ZHAO Q L, et al. PADA: Privacy-Aware Data Aggregation with Efficient Communication for Power Injection in 5G Smart Grid Slice[C]//2017 International Conference on Networking and Network Applications (NaNA). USA: IEEE, 2017. DOI: 10.1109/nana.2017.26
- [19] ZHANG Y H, LI J, ZHENG D, et al. Privacy-Preserving Communication and Power Injection over Vehicle Networks and 5G Smart Grid Slice[J]. Journal of Network and Computer Applications, 2018, (122): 50. DOI: 10.1016/j.jnca.2018.07.017
- [20] NI J, LIN X., 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. DOI: 10.1109/JSAC.2018.2815418

作者简介



罗珂榕, 西安电子科技大学网络与信息学院在读博士; 主要研究领域为无线网络安全、安全协议设计与分析; 参与多项国家重点研发计划及国家自然科学基金重点项目; 目前发表国际会议论文1篇, 公开国家发明专利1项。



曹进, 西安电子科技大学网络与信息学院副教授、硕士生导师; 主要研究领域为无线网络安全、应用密码学、安全协议设计与分析; 参与或主持国家自然科学基金项目、“863”项目、国家重点研发计划以及国家自然科学基金重点项目; 获省部级一等奖1项; 已发表论文24篇, 公开国家发明专利19项, 其中授权8项。



李晖, 西安电子科技大学网络与信息学院执行院长、教授、博士生导师; 主要研究领域为云计算中的密码理论与安全协议、移动互联网的隐私保护以及信息论与编码理论; 担任国家重点研发计划项目负责人, 主持“863”计划、国家科技支撑计划、新一代宽带移动通信国家重大专项、国家自然科学基金重点与面上项目、国防预研等项目15项; 获得国家级教学成果二等奖2项, 省部级科技进步奖一等奖2项、二等奖3项、三等奖1项, 获得2003年陕西省青年科技奖、2010年陕西省教学名师奖、2017年中央网信办网络安全优秀教师奖, 2018年入选陕西省特支计划教学名师项目; 发表论文170余篇, 获发明专利授权60余项。