



信息通信领域产学研合作特色期刊 | 十佳皖刊
第三届全国期刊奖百种重点期刊 | 中国科技核心期刊

ISSN 1009-6868

CN 34-1228/TN

中兴通讯技术

ZTE TECHNOLOGY JOURNAL

<http://tech.zte.com.cn>

2019年8月 • 第4期

专题：5G 通信安全技术



《中兴通讯技术》第8届编辑委员会成员名单

- 顾问

侯为贵（中兴通讯股份有限公司创始人） | 钟义信（北京邮电大学教授） | 陈锡生（南京邮电大学教授）
- 主任

陆建华（中国科学院院士）
- 副主任

徐子阳（中兴通讯股份有限公司总裁） | 糜正琨（南京邮电大学教授）

编委（按姓名拼音排序）

- 陈建平

上海交通大学教授
- 陈前斌

重庆邮电大学副校长
- 葛建华

西安电子科技大学教授
- 管海兵

上海交通大学教授
- 郭庆

哈尔滨工业大学教授
- 洪波

中兴发展股份有限公司总裁
- 洪伟

东南大学教授
- 纪越峰

北京邮电大学教授
- 蒋林涛

中国信息通信研究院科技委主任
- 李尔平

浙江大学教授
- 李红滨

北京大学教授
- 李建东

合肥工业大学副校长
- 李军

清华大学教授
- 李乐民

中国工程院院士
- 李融林

华南理工大学教授
- 李少谦

电子科技大学教授
- 林晓东

中兴通讯股份有限公司副总裁
- 刘健

中兴通讯股份有限公司高级副总裁
- 刘建伟

北京航空航天大学教授
- 陆建华

中国科学院院士
- 马建国

广东工业大学教授
- 孟洛明

北京邮电大学教授
- 糜正琨

南京邮电大学教授
- 任品毅

西安交通大学教授
- 孙知信

南京邮电大学教授
- 谈振辉

北京交通大学教授
- 唐雄燕

中国联通网络技术研究院首席科学家
- 王文博

北京邮电大学副校长
- 王文东

北京邮电大学教授
- 王喜瑜

中兴通讯股份有限公司执行副总裁
- 王翔

中兴通讯股份有限公司高级副总裁
- 卫国

中国科学技术大学教授
- 吴春明

浙江大学教授
- 邬贺铨

中国工程院院士
- 徐安士

北京大学教授
- 徐子阳

中兴通讯股份有限公司总裁
- 续合元

中国信息通信研究院副总工
- 薛一波

清华大学教授
- 杨义先

北京邮电大学教授
- 杨震

原南京邮电大学校长
- 易芝玲

中国移动研究院首席科学家
- 张宏科

北京交通大学教授
- 张平

北京邮电大学教授
- 张云勇

中国联通研究院院长
- 赵慧玲

工业和信息化部科技委信息网络专家组组长
- 郑纬民

清华大学教授
- 钟章队

北京交通大学教授
- 周亮

南京邮电大学教授
- 朱近康

中国科学技术大学教授
- 祝宁华

中国科学院半导体研究所副所长

目次

中兴通讯技术 (ZHONGXING TONGXUN JISHU)
总第147期 第25卷 第4期 2019年8月

专题:5G通信安全技术

5G 安全风险分析及标准进展 02

杨红梅, 赵勇

5G 典型应用场景安全需求及安全防护对策 06

闫新成, 毛玉欣, 赵红勋

5G 网络的认证体系 14

齐旻鹏, 彭晋

5G 网络的设备及其接入安全 19

陆海涛, 李刚, 高旭昇

基于软件定义的 5G 网络安全能力架构 25

张鉴, 唐洪玉, 侯云晓

软件定义 5G 通信网络的虚拟化与切片安全 30

罗巧榕, 曹进, 李晖

36 5G 时代大容量光接入网的安全技术

张宏熙

43 5G 物理层安全技术——以通信促安全

黄开枝, 金梁, 钟州

50 基于 5G 的垂直行业安全新特征与对策

汤凯

专家论坛

56 网络安全——5G 的基石

苏洲

企业视界

59 5G 网络设计与规划优化探讨

韩玮, 江海, 李晓彤

2019 年第 1—6 期专题计划及策划人

1. 5G 商用支撑理论及关键技术

中兴通讯股份有限公司执行副总裁 王喜瑜
中兴通讯股份有限公司首席科学家 向际鹰

2. 云网一体化技术

中国联通网络技术研究院首席科学家 唐雄燕

3. 边缘计算技术及其应用

清华大学教授 郑纬民
乔治亚州立大学教授 潘毅
韦恩州立大学教授 施巍松

4. 5G 通信安全技术

清华大学教授 李军

5. 新型光互连与光接入技术

北京大学教授 李红滨

6. 5G 通信系统示范应用

中国信息通信研究院科技委主任 蒋林涛

CONTENTS

ZTE TECHNOLOGY JOURNAL Vol. 25 No. 4 Aug. 2019

Special Topic: Technologies of 5G Communication Security

Risk Analysis and Specification Progress **02**

Security of 5G

YANG Hongmei, ZHAO Yong

Security Requirements and Protection **06** Countermeasures for Typical 5G Application

Scenarios

YAN Xincheng, MAO Yuxin, ZHAO Hongxun

Authentication Framework of 5G Network **14**

QI Minpeng, PENG Jin

Security of 5G Network Elements and Access Control **19**

LU Haitao, LI Gang, GAO Xusheng

Security Capability Architecture of **25** Software-Defined 5G Network

ZHANG Jian, TANG Hongyu, HOU Yunxiao

Virtualization and Slice Security of **30** Software-Defined 5G Communication Network

LUO Yurong, CAO Jin, LI Hui

36 Security Technology of Large Capacity Optical Access Network in 5G Era

ZHANG Hongxi

43 5G Physical Layer Security Technology: Enhancing Security by Communication

HUANG Kaizhi, JIN Liang, ZHONG Zhou

50 New Characteristics and Countermeasures for Vertical Industries Security in 5G

TANG Kai

Expert Forum

56 Keystone for 5G: Network Security

SU Zhou

Enterprise View

59 Optimization of 5G Network Design and Planning

HAN Wei, JIANG Hai, LI Xiaotong

期刊基本参数: CN 34-1228/TN*1995*b*16*68*zh*P* ¥ 20.00*15000*11*2019-08

敬告读者

本刊享有所发表文章的版权,包括英文版、电子版、网络版和优先数字出版版权,所支付的稿酬已经包含上述各版本的费用。未经本刊许可,不得以任何形式全文转载本刊内容;如部分引用本刊内容,须注明该内容出自本刊。

专题:5G 通信安全技术

专题策划人 李军



清华大学信息技术研究院研究员、博士生导师,中国电子学会计算机工程与应用分会副主任委员;主要从事网络与网络安全等领域的教学和研究工作;主持了多个“863”、国家重点研发计划和自然科学基金等项目;作为第一完成人荣获2014年中国电子学会科学技术奖二等奖;著译中外教材3部,发表学术论文100余篇,获得美国专利2项,中国发明专利20余项,且多数成果已商用。

内容导读

5G无疑是当前产业界最为热门的话题。这不仅是因为5G已经开始了商用进程,设备商、运营商纷纷进入白热化市场竞争,而且也因为5G被视为深刻影响国家利益的战略要害,受到国际经济、政治格局演变的巨大影响。但事实上,无论在技术与标准层面,还是在运营和应用层面,5G都还有很多亟待通过广泛国际合作共同解决的问题。在5G落地之际,迫切需要进一步凝聚产业共识,完善解决方案,而5G通信安全技术正是其中关键之一。

本期专题中,我们邀请长期从事通信安全并深度介入5G安全研究的一批专家、学者撰写了系列文章,从多个角度和多个层面倾力对5G通信安全技术进行较为全面的综述和探讨。5G通信安全技术必须立足于5G通信标准的基本框架,面向5G三大目标应用场景的真实需求,结合5G通信体系的技术和应用特点,既要为多种形态的终端和设备提供统一的认证、鉴权以及安全能力开放服务,又要能基于服务化架构(SBA)等标准实现差异化、个性化服务,并同时达成隐私保护和数据安全。5G网络与固网和其他无线网络密不可分,因而同样面临随着软件定义网络(SDN)/网络功能虚拟化(NFV)而来的网络虚拟化与网络切片等技术对安全的双面影响:新的安全能力与新的安全威胁,也同样面临着云计算和边缘计算引起的网络结构变化及安全解决方案的相应重构。当然,研究5G通信安全技术,还必然涉及到物理层等底层相关前沿技术

的研究、光接入网等相关基础设施的研究,更离不开结合物联网、自动驾驶等垂直行业特殊环境和演变态势的分析。5G通信安全内容庞杂繁复,本期的专题文章虽经认真布局,仍恐挂一漏万,有些安全需求和体系也只有随着5G应用模式的展开而逐步明晰。同时,为保持各篇的独立、完整成文,部分专题文章的内容(特别是场景交代)难免会有稍许交叠,敬请读者谅解。

专题的策划和组稿得到了编辑部和作者们的鼎力支持、慷慨赐稿,特此衷心感谢。5G将使全球社会肌体更加气血通畅,让机器计算与智能的能量更加快速有效地转变为价值,给人类生产与生活带来崭新可能,催生巨大变化。期望这个专题的文章能够有助于梳理5G通信安全技术脉络,引起更多关注和讨论,从而推动业界共识的形成和技术的成熟,为5G保驾护航。

李军

2019年7月11日

5G 安全风险分析及标准进展

Risk Analysis and Specification Progress of 5G Security

杨红梅/YANG Hongmei¹, 赵勇/ZHAO Yong²

(1. 中国信息通信研究院, 北京 100191;

2. 中国电信股份有限公司北京分公司, 北京 100010)

(1. China Academy of Information and Communications Technology, Beijing 100191, China;

2. China Telecom Co., Ltd. Beijing Branch, Beijing 100010, China)



摘要: 5G 网络新技术、新特征带来了新的安全风险与挑战, 主要体现在虚拟化设备安全边界模糊, 数据泄露风险有所增加, 海量多样化终端容易成为新的攻击目标以及新业务场景下安全责任主体划分难度加大等方面。5G 安全相关标准重点研究 5G 安全关键技术、5G 系统安全架构和流程相关要求、设备安全保障等, 目前已完成第 1 版本(R15)的标准制定工作, 预计 2019 年底完成第 2 阶段(R16)5G 安全的标准制定工作。

关键词: 5G; 基础设施; 关键技术; 安全风险; 供应链风险; 标准

Abstract: New technologies and features of 5G network bring new security risks and challenges. It is mainly reflected in the blurred security boundary of virtualization equipment, the increased risk of data leakage, massive diversified terminals which are vulnerable to attack, and the increased difficulty in the division of security responsibility subjects in new business scenarios. The 5G security specifications focus on the key technologies of 5G security, the security architecture and process, security assurance, etc. At present, the first phase (R15) of 5G security specifications has been published, and the second phase (R16) is expected to be completed by the end of 2019.

Key words: 5G; infrastructure; key technology; security risk; supply chain security risk; specification

DOI: 10.12142/ZTETJ.201904001

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.tn.20190704.1915.002.html>

网络出版日期: 2019-07-05

收稿日期: 2019-06-13

5G 时代, 移动通信将大幅提升移动互联网业务的使用体验, 进一步满足海量物联网应用的多样化需求, 与工业、医疗、交通、金融等行业深度融合, 实现“无处不在, 万物互联”。5G 网络与垂直行业深度融合的特点导致 5G 安全问题不仅影响人和人之间的通信, 还将会影响到各行各业, 有些场景甚至可能威胁到人们的生命财产安全乃至国家安全; 因此, 世界主要国家均将 5G 作

为优先发展的战略性领域, 5G 安全问题成为世界各国关注的焦点。

近期, 部分组织或国家(如欧盟、美国、捷克等)在 5G 安全领域发布了多个 5G 安全相关报告, 这些报告所表达的观点主要涵盖 2 个方面: 一是 5G 安全意义重大, 5G 网络的安全性对于国家安全、经济安全和其他国家利益以及全球稳定性至关重要; 二是 5G 将面临新的安全风险, 有必要开展 5G 安全风险评估,

并倡导将供应链安全及非技术因素纳入 5G 安全评估范畴。中国在 2016 年 12 月发布《国家网络空间安全战略》, 提出要统筹网络发展和安全 2 件大事, 认为安全是发展的保障, 发展是安全的目的。

1 5G 网络的主要特点

5G 是新一代信息通信技术的主要发展方向, 业务应用从移动互联网扩展到移动物联网领域, 服务

对象从人与人通信拓展到人与物、物与物通信,并将与经济社会各领域深度融合,引发人们生产、生活方式的深刻变革。国际电信联盟无线电通信组(ITU-R)定义了5G的3类典型业务场景:增强移动宽带(eMBB)、海量机器类通信(mMTC)、高可靠低时延通信(uRLLC),它们的应用需求以及对网络的性能要求各不相同。

与4G相比,5G网络整体架构延续4G特点,仍采用接入层、核心网层和应用层3层架构。不过,为了应对5G需求和场景对网络提出的挑战,并满足更加灵活、更加智能的发展趋势,5G网络进行了创新和变革。5G网络有以下几个主要特征:采用新型基础设施平台和新型核心网架构;比4G支持更多样化的业务场景;支持更高的性能指标并提供更强、更灵活的通信安全能力。下面我们从网络和安全2方面分别阐述。

(1)5G网络方面。基于网络功能虚拟化(NFV)和软件定义网络(SDN)技术实现基于通用硬件的新型基础设施平台。新型核心网基于统一基础设施平台进行云化部署,具有硬件平台通用化、软件功能模块化的特点:能够重构网络控制和转发机制,进一步实现控制和转发分离,改变单一管道和固化的服务模式;利用友好开放的基础设施环境,可为不同用户和垂直行业提供定制化的网络服务,构建资源全共享、功能易编排、业务紧耦合的综合信息化服务使能平台;利用服务化架构、网络切片、边缘计算、5G网络

能力开放等技术满足各行业需求。

(2)5G安全方面。5G网络采用统一的认证框架来融合不同的接入认证方式,并优化现有的安全认证协议(如安全上下文的传输、密钥更新管理等);采用差异化身份管理机制以及匿名化技术来保护用户隐私;为不同应用场景提供按需的安全保护,可满足业务多样化的时延要求、终端设备的使用寿命要求;采用更加灵活的安全机制保障网络安全。总体来说,5G可提供更健壮的业务安全性、更严密的数据保护以及更强的用户隐私性,可提供比4G系统更强大的通信安全能力。

2 5G 安全风险分析

相比于传统3G/4G网络,5G核心网基于NFV等新技术,在架构和功能上提供更泛在的接入支持、更灵活的控制和转发机制,以及更友好的能力开放方式,打破了传统电信网络的封闭性,同时能与云化基础设施结合,为普通消费者、应用提供商和垂直行业提供网络切片、边缘计算等新型业务能力。5G网络新技术新业务带来便利性的同时,也带来了安全风险和挑战。

2.1 5G 新技术新特性带来的安全风险与挑战

5G面临的新安全风险和挑战主要包括:实体网元变为虚拟化软件,物理资源共享,设备安全边界模糊,开放端口成为数据泄露的脆弱点,多样化终端的安全能力差异大,容易成为新的攻击目标以及新业务场景下安全责任归属问题等。

(1)基础设施虚拟化云化。

基础设施虚拟化云化给网络安全带来了突出挑战,具体表现在以下几个方面:虚拟化服务化架构模糊了传统网络边界,给虚拟化软件及虚拟机间的通信安全带来风险;集中的控制点容易成为网络攻击的“重灾区”;分层解耦、多厂商集成导致安全问题快速定位和溯源困难;开源软件的脆弱性及安全漏洞,给自动化安全评估和修复带来挑战,同时新型网络架构对安全运维人员的经验、技能提出了新的挑战。

(2)边缘计算。

边缘计算是指在网络边缘、靠近用户的位置上提供信息技术(IT)的服务、环境和云计算的能力,边缘计算节点可根据应用服务的需求部署于移动网络的边缘,提供超低时延的同时也能够降低高带宽业务的数据流对核心网的压力。但是,边缘计算带来便利的同时也带来了安全风险和挑战:一方面,移动边缘计算(MEC)基础设施通常部署在网络边缘,客观缩短了攻击者与MEC物理设施之间的距离,使得攻击者更容易接触到MEC网络基础设施,被攻击后可能会造成物理设备毁坏、服务中断、用户隐私和数据泄露等严重后果;另一方面,由于性能、成本、部署灵活性要求等多种因素制约,MEC节点的安全能力不够完善,可抵御的攻击种类和抵御单个攻击的强度不够,容易被攻击,使5G网络面临风险;另外,MEC服务不仅可由网络运营商提供,也可由第三方服务商提供,当MEC服务由第三方提供时,在接入网络的时候

如果没有调用认证与鉴权接口,则面临恶意第三方接入网络提供非法服务的风险等。

(3)网络切片。

5G 网络切片是在统一基础设施上,为用户提供专用服务。网络切片为不同业务提供差异化安全服务的同时,也面临一定的安全风险:不同的网络切片承载不同的 5G 业务,但网络切片共享网络基础设施,这就对切片的安全隔离能力带来挑战。若网络切片的认证和授权能力不足,则可能造成敏感信息和/或隐私信息泄漏,并且被攻击者所利用。另外,在 5G 新业务场景下,运营商可能会以网络切片的模式向第三方企业、用户提供网络服务,对于此种服务中涉及的运营商、虚拟运营商、用户等不同层和不同域的安全责任主体划分问题面临挑战。

(4)网络能力开放。

5G 网络基于网络能力开放技术,与垂直行业深度融合,使得垂直行业可以充分利用网络能力的同时灵活开发新业务,但也带来新的风险和挑战:5G 网络能力开放架构可能会面临网络能力的非授权访问和使用、数据泄露、用户和网络敏感信息泄露等安全风险,同时攻击者还可以利用 5G 网络能力开放架构提供的应用程序编程接口(API)对网络进行拒绝服务攻击;随着跨行业应用的开展,需要开放共享相应的用户个人信息、网络数据和业务数据,这些信息和数据从运营商内部的封闭平台开放共享到垂直行业企业的开放平台上,运营商对数据的控制力减弱,数据泄露的风险增

大。另外,跨行业数据共享过程中一旦发生用户数据泄露等安全事件,将面临主体间的责任划分不清的风险。

(5)海量多样化终端。

5G 支持多种接入技术,终端类型复杂多样,终端的安全能力差异巨大,终端设备分散不便统一管理,应用需求复杂难以部署强有力安全防护。因此,5G 时代海量多样化终端会给 5G 网络带来安全风险。

巨量化、泛在化的智能终端易被利用成为新攻击源。一方面在 mMTC 场景下,未来将有数以百亿计的终端接入物联网,一旦这些终端被入侵利用,形成规模化的设备僵尸网络,将成为新型高容量分布式拒绝服务(DDoS)攻击源,进而对用户应用、后台系统等发起攻击;另一方面,物联网终端提供的数据信息量巨大,分类众多,应用场景多元化,但缺乏统一的安全标识和认证管理机制,这也增加了网络管理的难度。

另外,终端上日趋开放的用户应用生态环境将加大安全管理挑战。在 5G 的泛在连接场景下,生产类、生活类应用可能同时安装在一台用户终端上,开放的应用生态环境在带来生产和生活便利的同时,也加剧了恶意应用威胁其他应用安全、终端安全以及后台生产系统安全的风险。

2.2 5G 融合应用面临的安全风险与挑战

5G 融合应用基于 5G 网络开展业务,因此也面临 5G 新技术、新特

性带来的安全风险与挑战,并具有各自业务本身的特点。同时,5G 新应用迭代速度快,5G 规模商用对经济社会带来的影响有待持续评估,安全风险呈现动态演进、持续变化的特点。具体表现为:(1)eMBB 场景下个人信息泄漏风险加大;(2)uRLLC 场景下数据保护风险加大;(3)mMTC 场景下多种终端形态导致海量终端被攻击的风险增大。

另外,5G 融合应用业务发展模式尚不明朗,其面临的风险可能在相当长一段时间之后才会逐步显现,有待持续跟踪研究。

2.3 应对举措

针对 5G 网络和业务面临的安全风险,可以从以下几个方面来应对:完善 5G 安全相关政策和管理制度,确保 5G 安全能力建设和业务发展同步推进;加大 5G 安全研发投入,在 5G 网络建设过程中,将安全需求纳入到业务设计、网络和网元动态部署的各个环节中,形成针对 5G 网络特点的主动防御体系;构建 5G 安全标准体系,加强 5G 网络安全新技术研究,制定完善 5G 安全技术标准,提升国际标准话语权。

3 5G 安全标准进展

3.1 国际标准

5G 相关国际标准主要由第 3 代合作伙伴计划(3GPP)研究制定,分为 R15 和 R16 2 个版本来满足 ITU IMT-2020 的全部需求:R15 为 5G 基础版本,重点支持 eMBB 业务和基础的 uRLLC 业务;R16 为 5G 增

强版本,将支持更多类型的业务。目前,3GPP已完成了R15独立组网5G标准,并将于2019年底发布R16标准。R16标准在R15的基础上,进一步增强网络支持eMBB的能力和效率,重点提升对垂直行业应用的支持,特别是对uRLLC类业务以及mMTC类业务的支持。

5G安全研究及标准制定与5G总体架构相关工作保持同步。3GPP于2018年6月完成了第1阶段(R15)5G安全标准,重点研究5G系统安全架构和流程相关要求,包括安全框架、接入安全、用户数据的机密性和完整性保护、移动性和会话管理安全、用户身份的隐私保护以及演进的分组系统(EPS)的互通等相关内容。预计2019年底将可以完成第2阶段(R16)5G安全标准的工作,将重点推进uRLLC安全、切片安全、5G蜂窝物联网(CIoT)安全、增强的服务化架构(eSBA)安全、位置业务安全增强等工作。

5G安全相关的主要国际标准如下:

- 5G系统安全架构和流程(3GPP TS 33.501)^[1];
- 3GPP系统架构演进(SAE)安全架构(3GPP TS 33.401)^[2];
- 安全保障通用要求(3GPP TS 33.117)^[3];
- 5G安全保障规范 NR Node B(gNB)(3GPP TS 33.511)^[4];
- 5G安全保障规范接入与移动管理功能(AMF)、用户平面功能(UPF)、统一数据管理(UDM)、会话管理功能(SMF)、认证服务器功能

(AUSF)、安全边界保护代理(SEPP)、网络存储功能(NRF)、网络开放功能(NEF)(3GPP TS 33.512~519)^{[5]~[12]}。

其中,《5G系统安全架构和流程》和《3GPP系统架构演进(SAE)安全架构》主要规定独立组网(SA)架构和非独立组网(NSA)架构下的5G网络架构及安全机制相关内容;安全保障系列规范主要规定5G网元的基线要求(数据和信息保护、可用性和完整性保护、认证和授权、会话保护、日志等)、抗攻击能力、端口扫描、漏洞扫描等的技术要求和测试方法等。

3.2 中国标准

中国5G安全标准分为行业标准和国家标准2大类,主要研究5G安全关键技术、架构和流程、虚拟化安全技术、设备安全保障等。行业标准在中国通信标准化协会(CCSA)研究制定,预计在2020年完成大部分标准;国家标准在国家标准化管理委员会制定,正在陆续立项。

目前正在研究制定的中国标准如下:

- 5G移动通信网安全技术要求(2018-2367T-YD);
- NFV安全技术要求(H-2019009066);
- 移动通信网络设备安全保障要求 5G基站(gNB)(H-2019008972);
- 5G移动通信网络设备安全保障要求核心网网络功能(H-2018008666);

• NFV环境下移动通信核心网安全需求研究(B-2018008682);

• 5G网络切片安全技术要求(B-2017006541);

• 5G边缘计算安全技术研究(B-2019008981)。

目前正立项的国家标准如下:

• 5G移动通信网通信安全技术要求(G-2019009101);

• 5G移动通信网络设备安全保障要求核心网网络功能(G-2019009031);

• 5G移动通信网络设备安全保障要求 5G基站(G-2019009031)。

以上行业和国家标准的主要内容基本与对应的国际标准一致,旨在指导5G移动通信网络设备的研发,并为运营商和监管机构在5G安全方面开展工作提供技术参考。

4 结束语

在当前5G发展的关键时期,中国应进一步加快5G技术创新,提升产业竞争优势,打造5G精品网络,构建新型基础设施,坚持5G产品全球化路线,继续推动5G产业快速发展。同时,为了应对5G面临的安全风险和挑战,应进一步加强国际交流合作,提升中国在5G安全领域的话语权;加大5G安全研发投入,突破5G安全关键技术研究,提升中国5G网络和设备的安全性可靠性;加强5G与垂直行业的融合创新研究,构建支撑行业发展的具有灵活高效安全属性的5G网络,并积极推动5G安全的全球标准以及后续产业

►下转第18页

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/km² 增大到 100 万台/km²^[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。

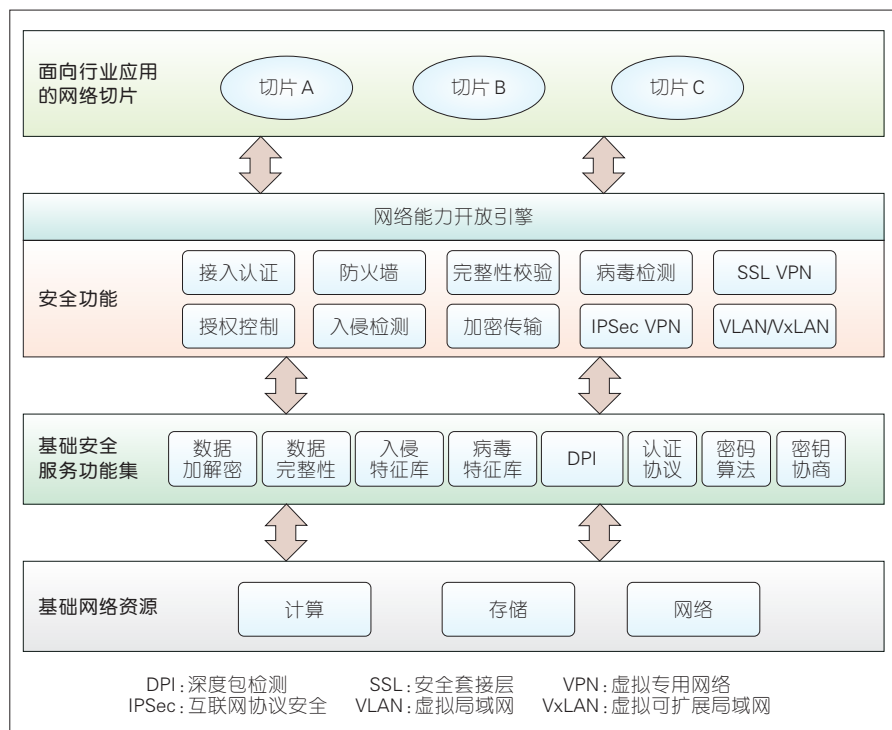
(2)网络安全功能按需重构。

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

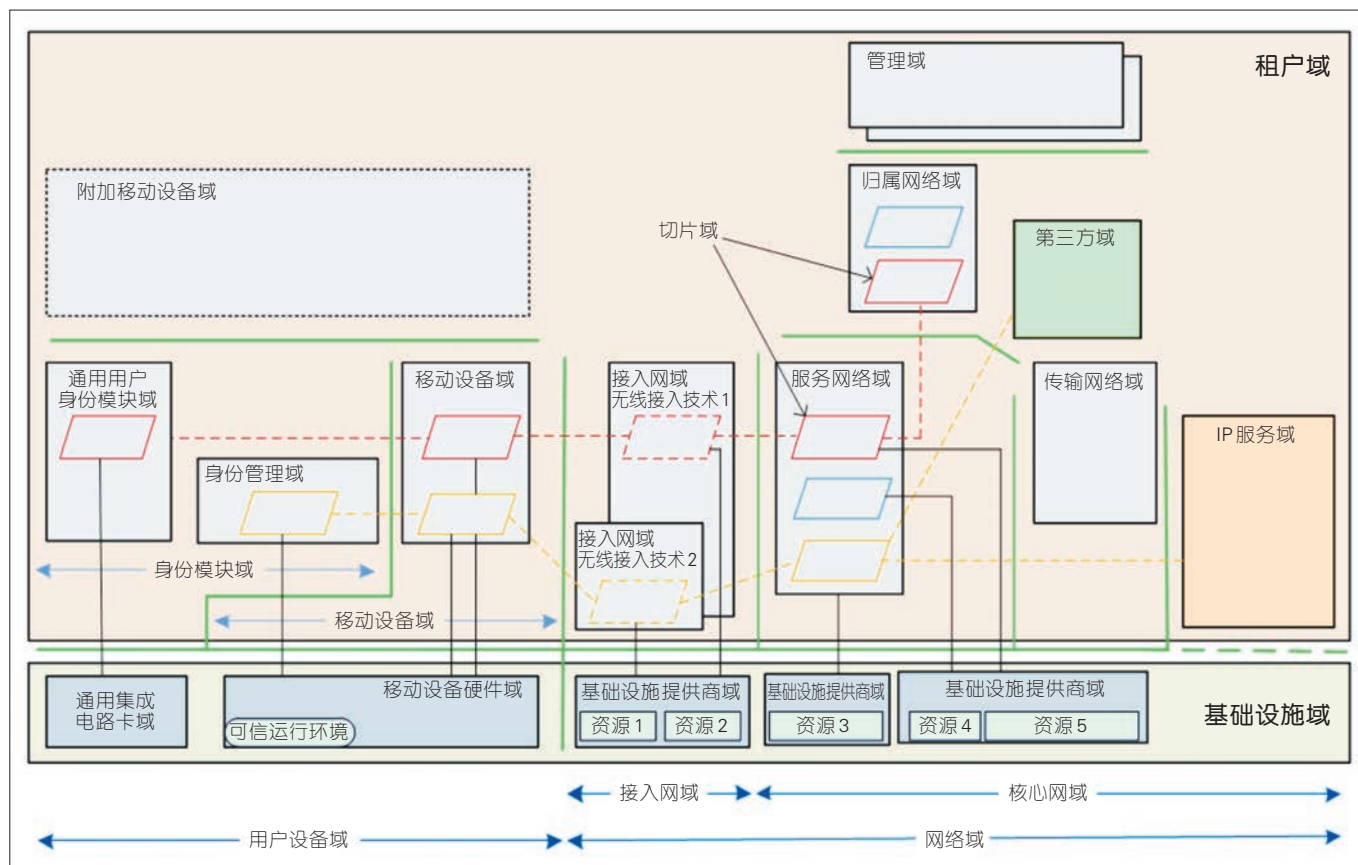
的安全服务也是差异化的。在实现网络安全服务功能虚拟化后，可以为服务于不同行业的网络切片提供网络安全功能的按需重构。例如，服务于车联网 (V2X) 的低时延网络切片，需要在网络边缘节点实例化一些必要的网络功能，选择适应低时延要求的认证方法、加密算法和密钥长度，以便在时延约束下提供对应的安全防护，更好地支持第三方的垂直应用；对于服务于 mMTC 的网络切片，仅需配置基本的控制面接入认证功能，而诸如移动性相关的网络功能则无需配置。我们还可以考虑在切片内部署虚拟的物联网网关以及安全态势感知系统，来防止 DDoS 攻击和威胁横向扩散。

(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 网络进行合理地域分；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。

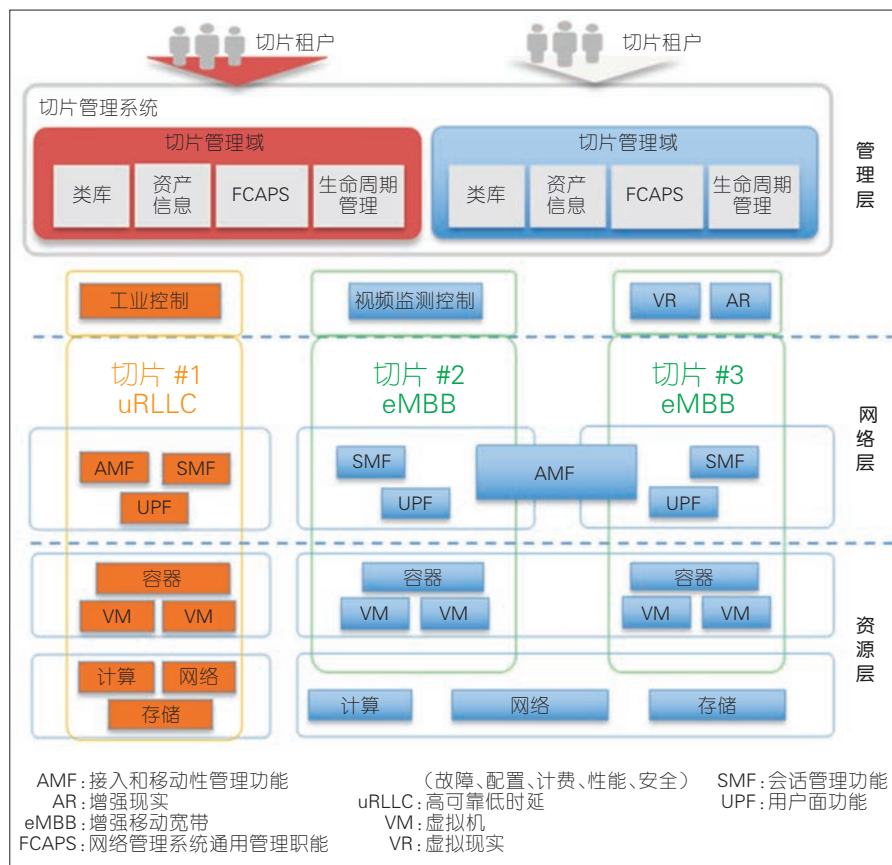
网络切片是5G提供网络服务的主要形态。5G可以在相同的网络基础设施上同时构建多个网络切片,为多个应用提供差异化网络服务。网络切片使得5G组网更加灵活,网络服务更贴合应用需求;但由于共享网络基础资源,如果管理不当就会引发切片数据泄露、切片间资源竞争、非法用户接入切片等安全威胁,因此需要提供切片安全隔离技术、切片接入控制等技术。

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(如视频监控控制、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。

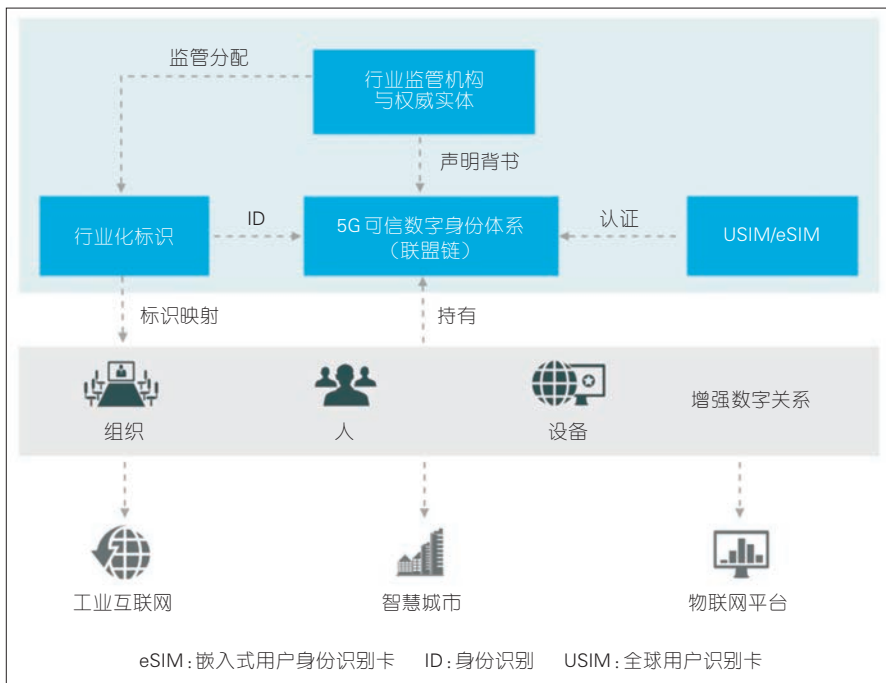
5G面向垂直行业的半封闭特征,以及众多不同类型新参与者的加入(例如新行业、新商业主体、新业务类型、新机器连接等),使得基础设施提供商、运营商、第三方服务提供商、网络用户等参与者之间的信任关系变得复杂,因而需要构建用户、终端、网络、服务之间的多元信任模型,以应对不同应用场景的

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,还是实现网络和服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。

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



▲图4 统一信任服务框架

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

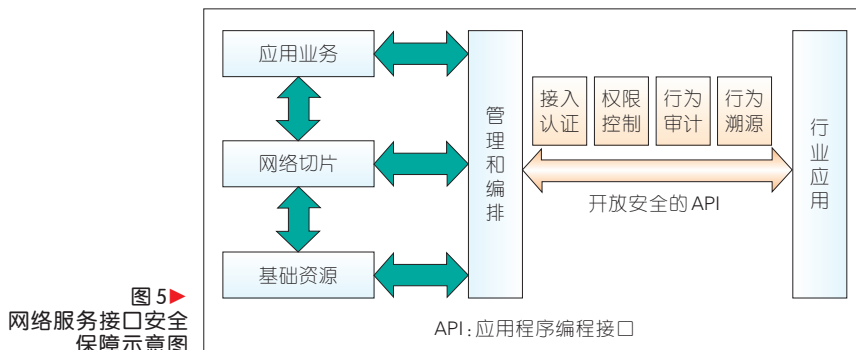


图5 网络服务接口安全保障示意图

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,采用全新安全防务理念构建全新的5G安全架构,以实现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,重视工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的电信网络安全技术白皮书[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。

5G 网络的认证体系

Authentication Framework of 5G Network



齐旻鹏/QI Minpeng, 彭晋/PENG Jin

(中国移动通信研究院, 北京 100053)
(China Mobile Research Institute, Beijing 100053, China)

摘要: 接入认证是保障网络安全的基础。随着网络变得越来越复杂, 认证机制逐步地将不同的参数分发、密钥产生、网络接入场景等各方面纳入统一考虑, 最终在 5G 中呈现出统一的认证框架。这使得 5G 网络可以为各种不同类型的终端提供安全的认证机制和流程。

关键词: 5G; 安全; 认证

Abstract: Access authentication is the basis of network security. While network grows more and more complex, consideration for authentication is also wider to involve different aspects like parameter distribution, key generation, network type and access scenarios. As a result, a unified authentication framework is proposed for 5G, which enables the 5G network to provide secure authentication mechanisms and process networks for different types of terminals.

Key words: 5G; security; authentication

DOI: 10.12142/ZTETJ.201904003

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.tn.20190709.1528.002.html>

网络出版日期: 2019-07-09

收稿日期: 2019-05-20

1 概述

移动通信网络作为国家重要基础设施, 承载着网络通信任务, 为用户提供语音、网络浏览, 乃至多媒体业务等多种服务, 已经深刻地融入至人们日常的生产生活过程中。随着 5G 的到来, 移动通信网络不仅影响个人生活的方方面面, 同时也进一步地对社会生活产生重大影响。同时, 移动通信网络也成为攻击者的目标。攻击者会针对用户和网络发起假冒、伪造、篡改、重放等主动攻击, 也会通过窃听、跟踪

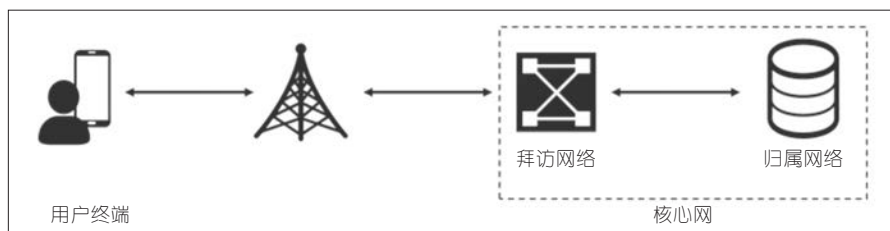
等方式发起被动攻击。因此, 为了保证移动通信网的安全和运营商、用户的权益, 鉴权认证机制成为保护移动通信网的第一道防线^[1]。

移动通信网通常由 3 部分组成, 即核心网(CN)、无线接入网(RAN)和用户设备(UE)。其中, 移动用户设备通常属于用户个人^[1], 由用户直接控制; 而接入网与核心网属于运营商, 由运营商直接控制。考虑到用户漫游的需求, 运营商被进一步分为保存用户信息的归属网络运营商, 以及直接为用户提供接入服务的拜访网络运营商, 具

体如图 1 所示。

当用户尝试接入网络时, 用户与网络需要确认真实身份, 以避免攻击者冒充真实用户或者提供虚假网络服务, 造成非法网络接入或者骗取用户的个人信息。因此, 用户接入网络时首先需要进行认证。

移动通信网络的认证采用经典的“挑战-响应”机制进行, 即用户与网络之间共享一个秘密信息, 然后网络侧根据该信息产生一个挑战信息并发送给用户, 用户根据挑战基于同样的秘密信息产生一个响应发回网络, 网络再判断响应是否符合



▲图1 用户与网络的连接示意图

合要求,从而判定用户是否为合法用户。该认证的流程如图2所示。

2 移动通信网络中的认证技术演进

移动通信网络从2G的全球移动通信系统(GSM)时代引入认证技术,发展到今天的第5G,经历了一系列的技术进步和换代。

2.1 2G 认证

在GSM时代,人们对安全的期望是能够跟有线电话一样安全。GSM在设计时,仅考虑对用户身份的识别,防止非法的用户接入,而未考虑用户对网络的身份校验。因此,GSM中的认证,只是一种单向的认证方式。出于对移动性的考虑,GSM的认证被设计成由直接为用户提供接入服务、拜访地运营商的拜访位置寄存器(VLR),对用户进行相关的认证;而负责维护用户签约信息、归属地的归属位置寄存器(HLR)只负责提供用户认证的安全参数。GSM认证如图3所示。

随着技术的发展,分组传送方式也被引入至移动通信网络中,形成通用分组无线服务技术(GPRS)网络,并引入了数据服务节点(SGSN)。SGSN既然负责对用户进行移动性管理,也就负责对终端的

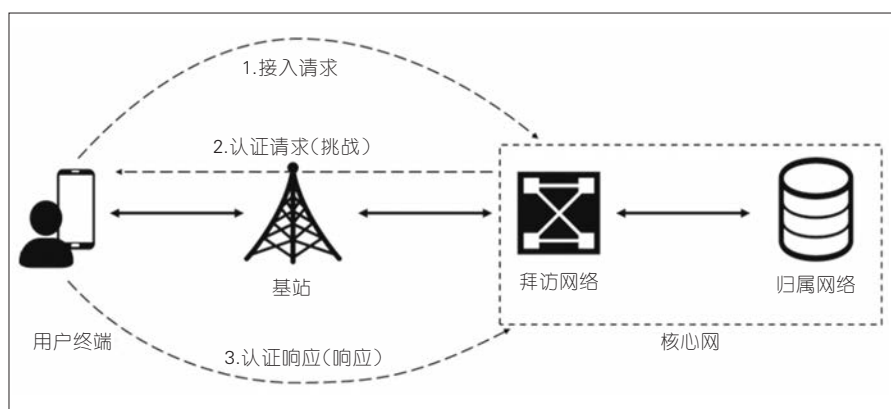
接入认证。用户认证信息同样来自于负责维护用户数据签约信息的归属地HLR;因此,为了便于在GPRS中对用户进行管理,由拜访地SGSN为用户进行认证,由归属地HLR提供认证参数,从而实现了GSM/GPRS在认证参数分发上的统一。GSM/GPRS的技术的认证,具体如图4所示。

2.2 3G 认证

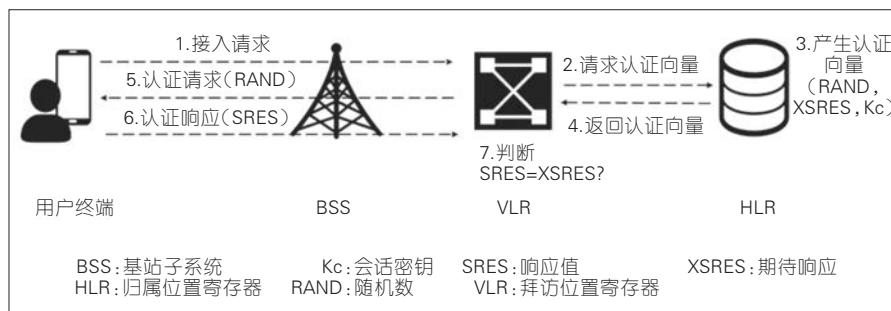
到了3G时代,人们意识到在

GSM/GPRS认证过程中可能存在伪装网络和重放等风险,如攻击者通过伪装网络的方式,诱骗用户接入虚假网络,进而可以通过构造虚假号码向用户推送垃圾信息甚至诈骗信息,使得用户遭受侵害。因此,3G引入双向认证机制,增加了用户对网络的认证能力,如图5所示^[2]。

更为重要的是,GSM/GPRS认证所对应的响应值(RES)和会话密钥Kc之间是相互独立的。当时仅是为了方便计算和传送,便在推荐实施方案中将相关参数同时产生并由HLR一并传递给VLR。但从3G认证开始,认证机制在设计时就将认证与后续通信所需要使用的会话密钥绑定在了一起,认证参数的产生与会话密钥的产生过程不可分割。这就使得攻击者无法通过分割



▲图2 认证示意图



▲图3 全球移动通信系统认证

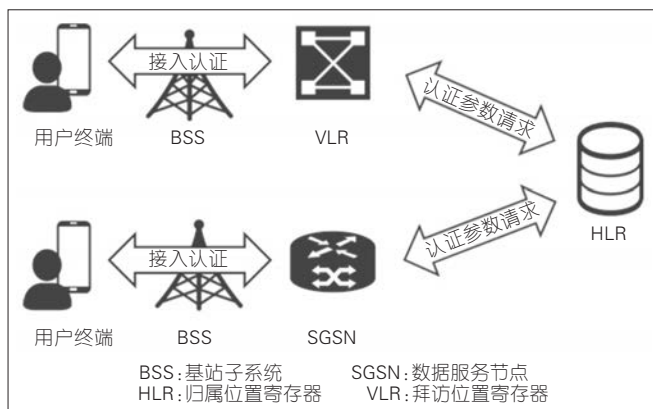


图4 全球移动通信系统/分组无线服务技术认证

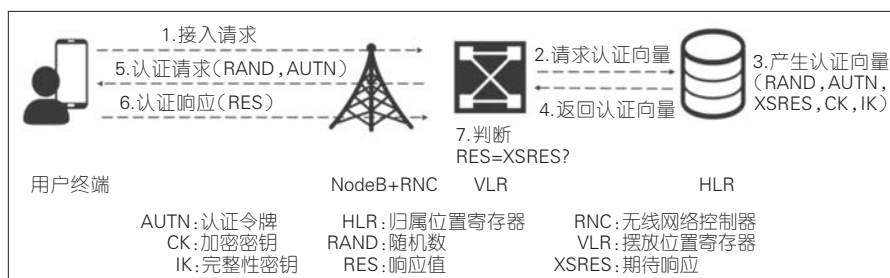


图5 3G认证

认证参数和会话密钥参数的方式实现对用户或网络身份的替代。所以,3G认证机制被叫做认证与密钥协商机制(AKA),该机制实现了认证参数与会话密钥参数之间的统一考虑。认证与密钥的产生具体如图6所示^[2]。

2.3 4G 认证

到了4G时代,认证机制又得到了进一步扩展。一方面,2G/3G时代的认证参数由归属网络产生,所以用户认证的实际上是归属网络。但与用户直接进行双向认证的是拜访网络的网元,这就导致用户无法对拜访网络进行认证,而只能间接地依赖于归属网络对拜访网络的完全信任对拜访网络进行认证。例如,中国用户漫游至其他国家时,认证参数仍由中国运营商提供,用户

认证的仍是中国运营商网络;但此时双向认证发生在中国用户和其他国家的网络运营商之间,中国用户无法认证接入的其他国家网络的身份。这种做法在4G时得到了一定程度的纠正。在4G的认证过程中,拜访网络需要将其网络标识(ID)发送给归属网络,归属网络在产生认证所需参数时将拜访网络的ID作为生成参数之一引入,从而使得用户也可以在认证时对拜访网络的身

份进行验证。

另一方面,随着蜂窝接入和无线局域网(WLAN)技术的长期并行,4G开始考虑用户通过WLAN等非蜂窝方式接入4G核心网的场景。对应地,在认证方面,4G也设计了面向非蜂窝接入的认证体系,第一次引入了基于EAP的认证框架,具体如图7所示。

3 5G 网络中的认证机制

随着通信网络技术的发展,第5代移动通信网络被提上日程。5G通信网络的设计目标面向3大场景:增强型移动宽带(eMBB)、高可靠低时延(uRLLC)以及海量机器类通信(mMTC)。因此,5G通信不仅考虑人与人之间的通信,还将考虑人与物、物与物之间的通信,进入万物互联的状态。

这种情况下,5G认证面临着新的安全需求。一方面,为了适应多种类型的通信终端,并使得它们能够接入通信网络,5G系统将进一步地扩展非蜂窝技术的接入场景。例如,电表、水表、摄像头等物联网设备通常采用蓝牙、WLAN等技术与网络相连,这类设备采用5G系统通信时仍倾向于使用原有的连接方

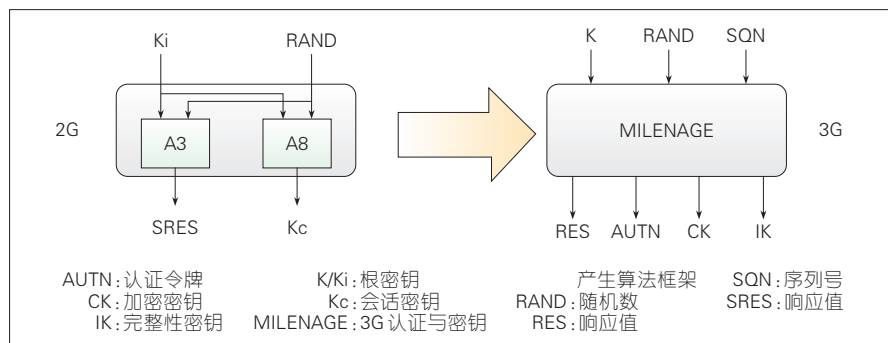
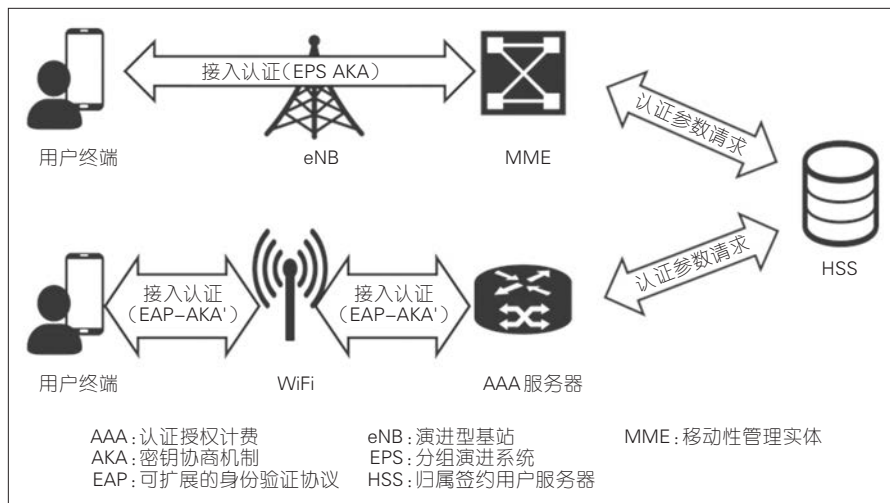


图6 认证与密钥产生



▲图7 4G不同接入方式下的认证统一

式。这就导致传统面向蜂窝接入的认证机制需要进一步地向非蜂窝接入的方式扩展。另一方面,传统认证机制下,拜访地/归属地的两级移动网络架构下的认证机制要求归属网络无条件信任拜访网络的认证结果。但随着网络的发展,出现了越来越多的安全隐患,拜访网络和归属网络之间的信任程度在不断降低。例如,拜访地运营商可以声称其为某运营商的用户提供了接入服务而实际未提供,导致计费纠纷。对于5G的通信来说,相比于人与人之间的语音通信和数据交互,万物互联下的移动通信将会承载更多的设备测控类信息,因此对接入安全的要求更高。例如,当5G系统被垂直行业用于传递远程操控的控制消息。这使得5G认证还需要加强归属网络对用户终端的认证能力,使其摆脱对拜访网络的依赖,实现用户在归属地和拜访地等不同地点间的认证机制统一。5G还引入了对用户身份的进一步增强保护,使得用户的永久身份不在空中接口上进

行传输,拜访网络还需要从归属网络获得用户的身份信息。这就导致拜访网络和用户终端之间无法直接对身份信息进行确认。因此,为了简化设计,5G认证过程中对用户的认证信息也需要进行确认。

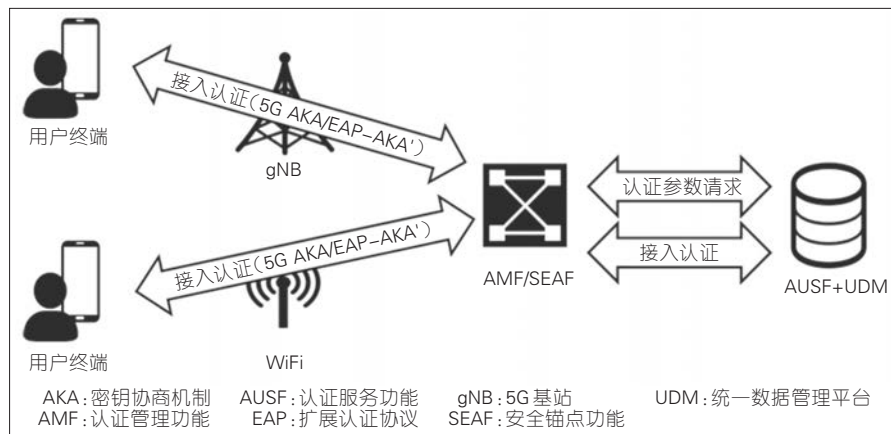
基于上述需求,5G提供了2种认证框架,分别被称为5G-AKA和EAP-AKA',如图8所示。

此外,5G网络将更多地垂直行业提供服务,而垂直行业对5G网络提出了更多的需求。例如,需要通过5G新增的网络切片特性来为垂直行业提供定制化的服务,包括

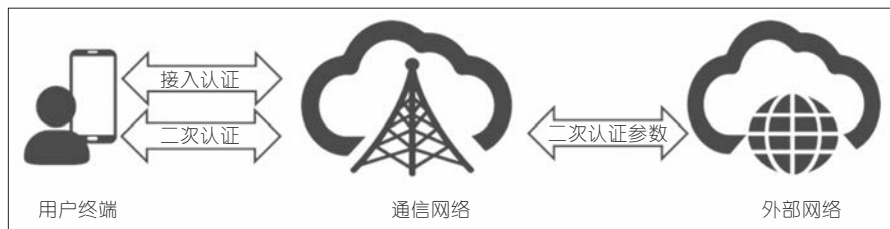
为特定的业务提供数据通道建立前的认证机制^[3]。因此,5G系统引入了二次认证的概念,即在用户接入网络时所做认证之后为接入特定业务建立数据通道而进行的认证。在该认证过程中,第一次使用了非运营商控制的信任状要求。例如,当5G网络用于为高保障业务系统提供通信时,用户通过接入认证后并不能直接与业务系统建立连接,而是利用业务相关的信任状与用户终端进行认证,并在认证通过的情况下才允许5G网络为用户建立与业务系统间的通信链路,从而提升对业务系统的保护,具体如图9所示。

4 结束语

随着移动通信技术的不断发展,移动通信系统对于人们的生产生活影响越来越大,所需要面对的需求也越来越多,故而网络变得越来越复杂,这使得对应的认证机制也需要考虑越来越多的因素和场景。在认证机制的演进过程中,逐步实现了对认证参数分发形式的统一、对认证参数和密钥参数产生的统一、对拜访网络和归属网络的统



▲图8 5G的认证示意图



▲图9 二次认证的示意图

一、对不同接入场景的统一,以及对认证框架的统一。正是有了这些不同角度和层面的统一,使得5G网络可以为各种不同类型的终端提供安全的认证机制和流程,并为后续安全保护打下了坚实的基础。

但同时我们也要看到,5G的认证仍然面临着诸多挑战,例如学术界通过形式化分析方法对5G认证机制进行评估^[4-5],发现了一些潜在的风险点并促使网络协议改进。在通信网络的演进过程中,考虑网络的后向兼容性,无线通信系统始终坚持以对称密钥作为认证的基础,并因此衍生出一系列的安全参数。因此,基于对称密钥的信任状是整

个网络认证和后续安全保障的基础。但对于5G及后续的网络,需要考虑更多的应用场景,并需要与垂直行业做更深入的结合。这些条件下,可能产生新形态的信任状需求。因此,如何做到不同形态的信任状的统一,将会是后续认证演进的考虑方向。此外,对于轻量级的物联网应用,如何充分发挥无线通信网络已有的安全优势,实现通信网络和业务之间认证的统一,降低物联网终端的能耗,提升安全保障效率,也是目前5G标准正在研究制定的内容之一。

参考文献

[1] 胡鑫鑫,刘彩霞,刘树新,等. 移动通信网鉴权认

证综述[J]. 网络与信息安全学报, 2018, 4(12): 1-15

[2] 3GPP. 3G Security; Security Architecture: 3GPP TS33.102[S]. 2013

[3] 栗栗,彭晋,齐旻鹏,等.移动通信网中的密码算法演进之三——认证篇[EB/OL].[2019-05-20]. https://mp.weixin.qq.com/s/SoA1bY4AZtbGbUkMj_U_X17Q

[4] BASIN D, DREIER J, HIRSCHI L, et al. A Formal Analysis of 5G Authentication[J]. 2018, (2):22-25. DOI:10.1145/3243734.3243846

[5] BASIN D, DREIER J, HIRSCHI J, RADOMIROVIC L, S, et al. A Formal Analysis of 5G Authentication[C] //25th ACM Conference on Computer and Communications Security. USA: ACM, 2018: 1383-1396. DOI: 10.1145/3243734.3243846

作者简介



齐旻鹏, 中国移动通信研究院安全所项目经理、中国移动3GPP安全与隐私小组代表等;长期从事LTE、5G等基础网络通信安全研究,并参与物联网、车联网等系统安全设计工作,目前主要负责5G系统安全架构与协议研究;申请并获得授权专利10余项,发表10余篇论文。



彭晋, 中国移动通信研究院安全所所长,曾担任ITU-T SG13 报告人、3GPP SA1 UDC子组主席等;研究方向为电信核心网、电信网安全、云计算安全、大数据安全等;曾负责多项国家科研项目,并参与ITU-T、3GPP、GSMA等国际标准工作。

◀上接第5页

发展,实现5G技术发展与技术安全相统一。

参考文献

- [1] 3GPP. Security architecture and Procedures for 5G System (Release 15): 3GPP TS 33.501 [S]. 2019
- [2] 3GPP. 3GPP System Architecture Evolution (SAE); Security Architecture: 3GPP TS 33.401 [S]. 2012
- [3] 3GPP. Catalogue of General Security Assurance Requirements: 3GPP TS 33.117[S]. 2017
- [4] 3GPP. 5G Security Assurance Specification (SCAS); NR Node B (gNB): 3GPP TS 33.511[S]. 2019
- [5] 3GPP. 5G Security Assurance Specification (SCAS); Access and Mobility Management

- Function (AMF): 3GPP TS 33.512[S]. 2018
- [6] 3GPP. 5G Security Assurance Specification (SCAS); User Plane Function (UPF): 3GPP TS 33.513[S]. 2018
- [7] 3GPP. 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) Network Product Class: 3GPP TS 33.514[S]. 2018
- [8] 3GPP. 5G Security Assurance Specification (SCAS); Session Management Function (SMF): 3GPP TS 33.515[S]. 2018
- [9] 3GPP. 5G Security Assurance Specification (SCAS); Authentication Server Function (AUSF): 3GPP TS 33.516[S]. 2017
- [10] 3GPP. 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) Network Product Class: 3GPP TS 33.517[S]. 2018
- [11] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class: 3GPP TS 33.518 [S]. 2018
- [12] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) Network Product Class: 3GPP TS 33.519[S]. 2018

作者简介



杨红梅, 中国信息通信研究院主任工程师、CCSA TC5 WG12 副组长;主要研究领域为移动通信3G、4G、5G核心网及安全;负责并完成4项国家重大专项课题,牵头制定了移动通信核心网和安全领域多项行业标准,多次获得CCSA科学技术奖;发表文章30余篇,主编专著《演进分组系统(EPS)业务应用技术》。



赵勇, 中国电信股份有限公司北京分公司高级工程师;研究领域为移动通信核心网及业务;牵头负责并完成了多个业务平台的云化工作;发表文章10余篇。

5G 网络的设备及其接入安全

Security of 5G Network Elements and Access Control

陆海涛/LU Haitao, 李刚/LI Gang, 高旭昇/GAO Xusheng

(中兴通讯股份有限公司, 广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)



摘要: 分析了 5G 基站在自身的硬件和软件资源、无线空口、传输接口和管理接口等方面所面临的安全威胁, 以及针对这些安全威胁的安全解决方案。认为安全对 5G 产品来说非常重要, 也是 5G 技术能够切实推广应用的重要基础。5G 网络的设备及其接入所面临的安全威胁随着技术的演进不断更新变化, 需要人们采取相应的安全技术来应对。

关键词: 安全威胁; 加密; 认证; 授权

Abstract: The security threats faced by 5G base station in its own hardware and software resources, wireless air interface, transmission interface and management interface are analyzed in this paper, as well as the security solutions to these security threats. It is considered that security is very important for 5G products and is an important basis for the practical application of 5G technology. With the evolution of technology, security threats are constantly changing. It is necessary to adopt appropriate security technology to ensure product safety.

Key words: security threats; encryption; authentication; authorization

DOI: 10.12142/ZTETJ.201904004

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1701.006.html>

网络出版日期: 2019-07-17

收稿日期: 2019-05-25

随着物联网的大规模应用, 越来越多的设备接入到 5G 网络, 并要求提供大容量、大连接和高可靠低时延的移动通信。2018 年 6 月 13 日, 第 3 代合作伙伴(3GPP)正式发布 5G 新空口(NR)标准方案, 完成了 5G 全功能的标准化工作。3GPP 定义了 5G 的 3 大应用场景分别为: 增强移动宽带(eMBB)、高可靠低时延通信(uRLLC)以及海量机器类通信(mMTC), 支持诸如物联网、触觉互联网等更高数据速率、更低时延和更大规模的设备连接, 对

安全提出挑战。

5G 网络的新架构如图 1^[1]所示, 主要由用户设备(UE)、无线接入网络(RAN)、5G 核心网(5GC)功能组件和数据网络(DN)组成。

其中 RAN 是 5G 基站(gNB)设备, 用来连接所有终端用户; UE 提供对用户服务的访问; 接入及移动性管理功能(AMF)提供核心网控制面功能; 用户面功能(UPF)提供核心网用户面功能; 鉴权服务器功能(AUSF)提供认证服务器功能, 用于归属网络的 5G 安全过程。

本文中, 我们讨论的 5G 网络设备和接入安全主要是针对 5G 基站设备。安全的核心关注点就在 gNB 的外部接口和 gNB 的内部互联安全需求, 通常安全攻击点都是在系统的外部接口发起。RAN 的核心在于如何保证 UE 与 gNB 空口上传输信息的安全性、5G 基站本身操作维护的网管系统的接口安全性等。

1 5G 网络设备的接入安全威胁

5G 基站设备, 是无线通信网络

中的一部分,存在于UE和核心网间,实现无线接入技术。如图1所示,5G基站设备的安全威胁,主要有4个方面:一是构成gNB的硬件、软件及网络的基础设施的安全威胁;二是针对连接NG-UE的空口上发送信息的空口安全威胁;三是针对连接到5GC的N2和N3参考点的传输网络安全和信息的的安全威胁;四是对基站连接到网管的管理平面的安全威胁,具体如图2所示。

(1)基础设施的安全威胁。

基站设备的基础设备包括部署环境、硬件设备以及基站内部的软件版本、数据、文件等。对于部署环境和硬件,其面临的安全威胁是损坏设备周围环境,如温度、烟雾等,或直接破坏设备的硬件。对于基站内的软件,其面临的安全威胁是非授权登录基站或普通账户登录基站后执行非授权的访问,从而破坏基站的数据、文件等,导致基站功能不可用。

(2)空口的安全威胁。

空口指用户终端和基站设备间的空中无线信号传播。空口的安全威胁主要表现为3方面:信息泄露,在基站发射信号的覆盖区域,非法用户也能接收,并通过侦听、嗅探、暴力破解等手段获取基站的转发数据,造成信息泄露;数据欺骗,例如伪造虚假的基站发射无线信号,骗取合法用户接入,然后盗取用户数据或实施欺诈;攻击设备发射强干扰信号,破坏正常用户和基站的无线连接,从而造成正常基站的业务中断。

(3)核心网接口的安全威胁。

基站的核心网接口包括基站与核心网、基站与基站间的用户面数据和信令面数据接口,通过以太网传输。因此也会面临与一般IP网络相同的安全威胁,包括不安全的网络传输协议引起的数据泄露,针对网络可用性的攻击(例如拒绝服务(DOS)攻击、广播包攻击,缓冲区溢出等造成基站不能提供正常服务),以及对传输数据篡改破坏数据完整性。

(4)网管接口的安全威胁。

网管接口是后台网管设备与前台基站的管理面数据接口,也通过以太网传输。网管接口的安全威胁首先是网络传输协议。一些不安全的网络传输协议,例如Telnet、文件传输协议(FTP)、超文本传输协议(HTTP)、简单网络管理协议(SNMP)v1/v2等不进行加密处理,很容易受到嗅探攻击,导致数据泄露;第2个威胁是账户和密码管理的健壮性,例如密码较弱,就很容易受到字典攻击或暴力破解,基站被非法登录攻击;第3个威胁是权限控制管理,如果账户的分级权限控制不好,也会造成非授权用户或授权用户的非授权访问,破坏数据的

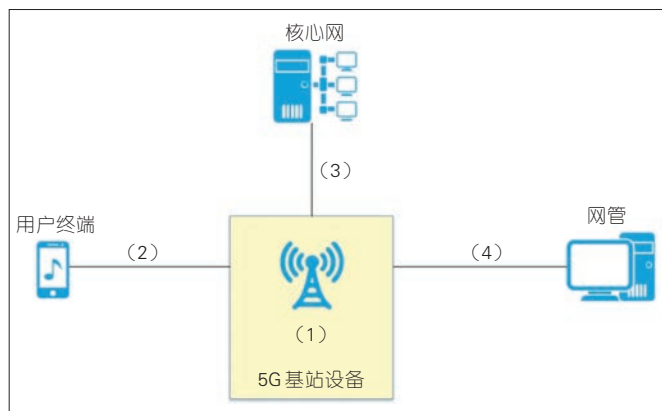


图2
5G基站设备接口

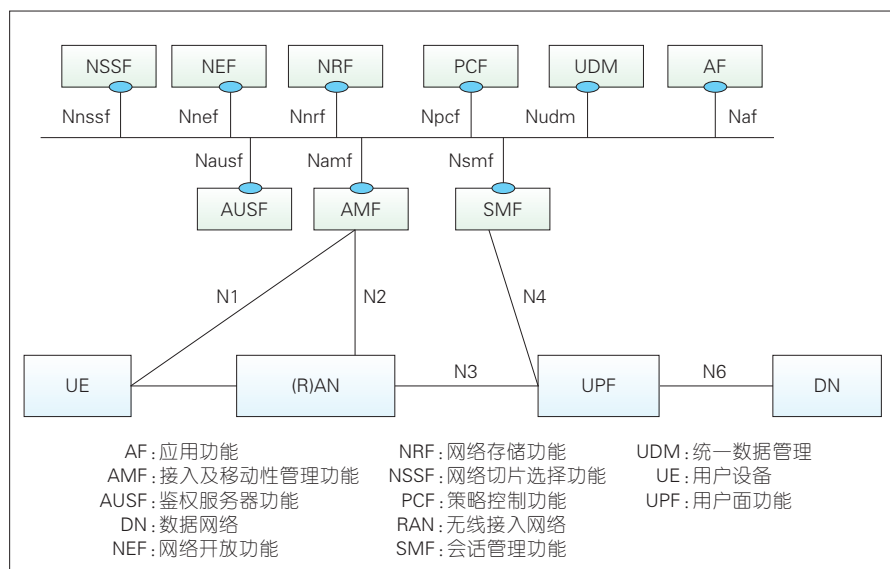


图1 5G的网络架构

机密性和完整性;还有就是会话管理控制,例如缺乏最大会话连接数限制,就容易遭受DOS攻击,导致系统资源耗尽等。

2 5G 网络设备及接入的安全方案

相比于2G/3G/4G在网络上存在的安全弱点,5G在网络定义和标准还建立过程中,安全性是一个核心问题。5G的应用场景和网络架构要复杂许多,包括eMBB场景下的大容量用户通信保证、uRLLC场景下的大量物联网设备接入、云化的集中单元(CU)部署、虚拟化的网络架构等,对安全性都有着很大的挑战。

3GPP 33.501^[2]提出5G网络安全整体架构,具体如图3所示。

图3中,(I)是网络访问安全,表示一组安全功能,使UE能够安

全地通过网络验证和访问服务,包括3GPP访问和非3GPP访问;(II)是网络域安全,表示一组安全功能,使网络节点能够安全地交换信令数据和用户平面数据;(III)是用户域安全,表示保护用户访问移动设备的一组安全功能;(IV)是应用域安全,表示一组安全性功能,使用户和供应商中的应用程序能够安全地交换消息。

5G协议引入了用户永久标识符(SUPI)和用户隐藏标识符(SUCI)的概念。更重要的是,5G规范中引入了基于公钥基础设施(PKI)的安全体系结构,允许验证和鉴别源自5GC的控制面消息(CPM)。

这是3GPP协议在5G体系架构上的安全考虑。具体地,针对5G基站设备及其接入,并根据图2所示的4个方面的安全威胁,我们分别

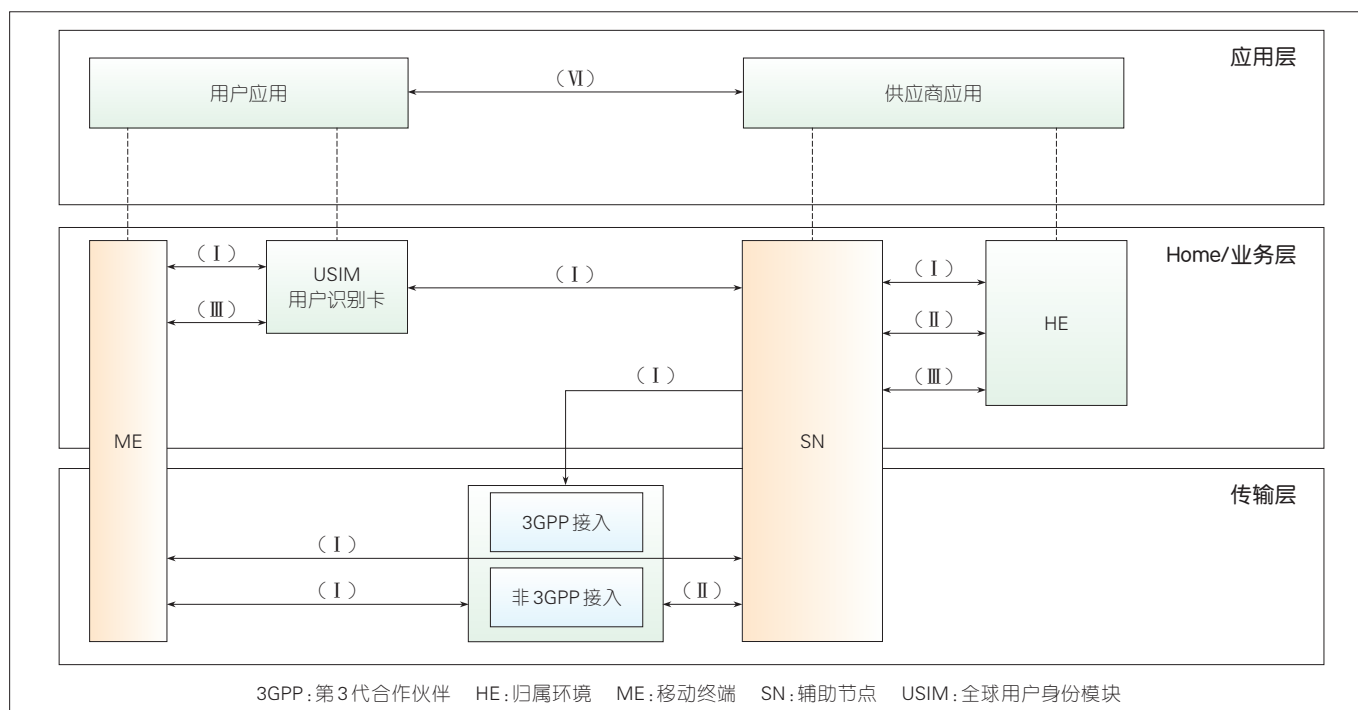
采用了不同的安全解决方案。

2.1 基础设施的安全方案

基站基础设施的安全,首先要确保对基站设备本身及周围组网设施的物理安全,如设置门禁、监测控制、配备烟雾、温度传感器等,有异常及时通知管理员。

同时,还要做好防火墙配置。基站设备在系统组网中通过IP协议连接核心网、网管服务器等网络设备,很容易遭受IP网络的攻击,如DoS、广播包、缓冲区溢出攻击等。通过配置防火墙过滤规则,只提供对外开放的端口/协议列表,不使用的端口缺省拒绝。另外,还可以配置入侵检测系统(IDS),对网络攻击行为及时检测并警报,以尽快采取响应措施。

除了基站硬件和组网环境,基站软件资源具体包括操作系统、软



▲图3 5G安全体系结构

件版本、数据存储文件也是重要的基础设施。攻击者会利用操作系统和数据库等漏洞攻击设备,因此需要定期对设备软硬件进行安全威胁分析和评估。每发布一个软件版本,都需要经过第三方软件的安全扫描和评估,以将发现的漏洞和风险及时解决。通过对版本的数字签名来检验版本的合法性,防止被篡改。数据存储文件的安全是通过设置安全存储区,对数据分类(不同分类的数据存储在不同的存储区),并

进行严格的访问控制,以确保机密性。例如,基站的机密信息要加密存储,存放在安全存储区,只有管理员权限才能访问。

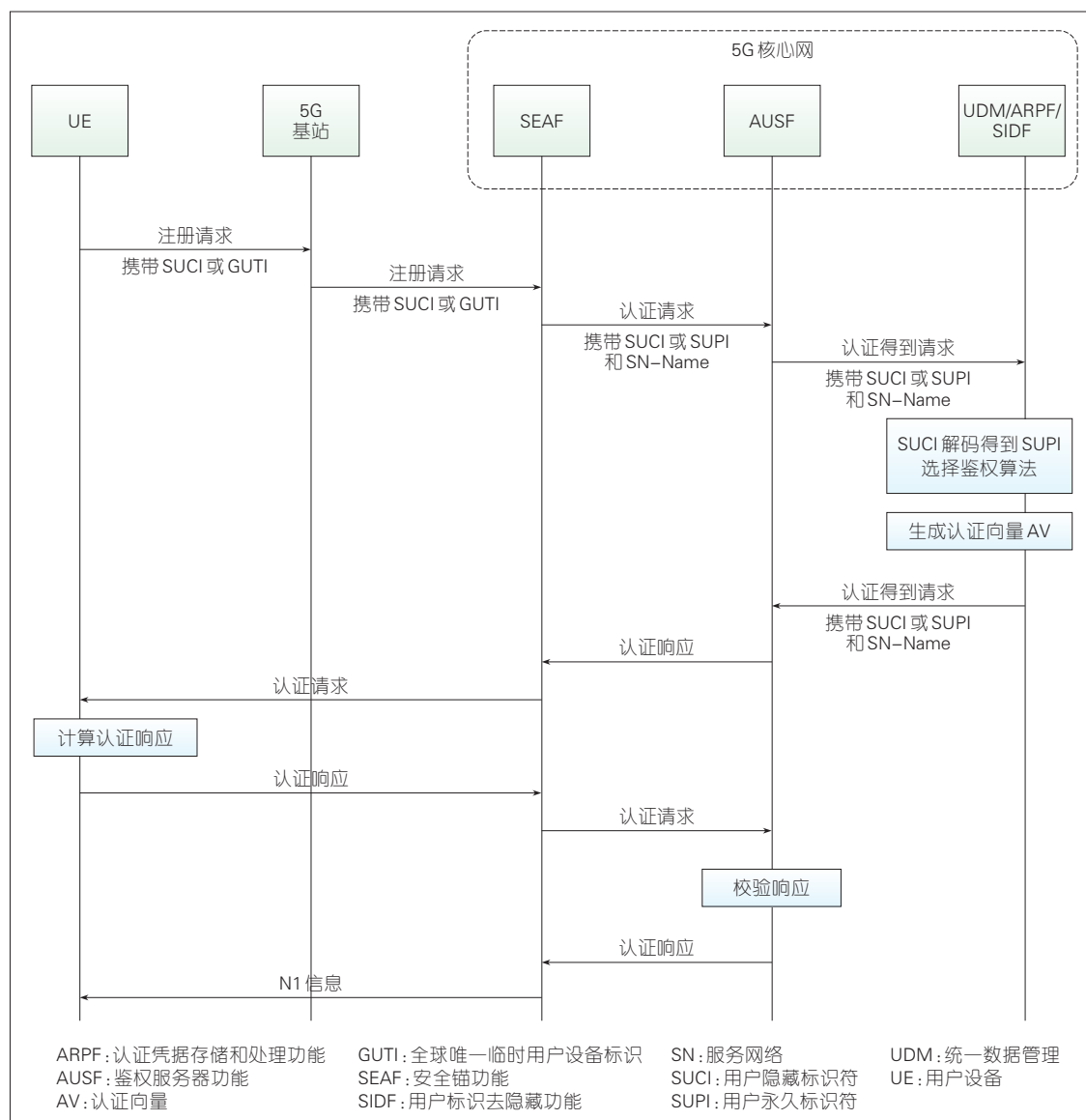
2.2 空口的安全方案

(1) 支持双向认证。

在2G时代,移动终端使用普通用户身份识别卡(SIM),只支持可扩展身份认证协议(EAP)-SIM单向鉴权,即网络对SIM卡进行身份合法性认证,而没有用户终端对网

络的认证,这就造成“伪基站”。长期演进(LTE)使用了全新的双向认证方式,使用配置用户识别模块(UIM)的USIM卡,只有都完成网络对终端认证和终端对网络认证后才接入网络。

5G的双向认证流程和LTE变化不大,可以不用换卡,不用换号,并且使用EAP-认证与密钥协商协议(AKA),支持统一框架下的双向认证。EAP-AKA的认证流程^[2]如图4。增加5G-AKA认证,是通过向归



属网络提供 UE 从访客网络成功认证的证明,来进一步增强 EPS-AKA 的安全性。

(2)支持数据机密性。

数据加密指发送方通过加密算法将明文数据转换为密文数据,保证数据不被泄露。5G 基站根据 SMF 发送的安全策略激活用户数据的加密,支持 NEA0、128-NEA1、128-NEA2、128-NEA3 等加密算法,加密算法再由 5G 基站通过安全模式信令(RRC)指示给 UE。加密密钥由 UE 和 5G 基站分别生成。

(3)支持数据完整性。

支持数据完整性指发送方通过完整性算法计算出完整性消息认证码(MAC-I),接收方通过完整性算法进行计算(X-MAC),再比较 MAC-I 和 X-MAC 是否一致,以保证数据不被篡改。

5G 基站根据 SMF 发送的安全策略激活用户数据的完整性保护。完保算法由 5G 基站通过 RRC 信令指示给 UE。5G 基站支持 NEA0、128-NEA1、128-NEA2、128-NEA3 等完整性算法,发送方采用协商确定的某一完整性保护算法。完保密钥由 UE 和 5G 基站分别生成。

2.3 核心网接口的安全方案

5G 基站设备的传输安全主要包括 N2、N3 口的传输安全,并按照开放式系统互联(OSI)七层协议,在不同的协议层都有各自的安全解决方案。

(1)物理层安全。物理层通过线缆屏蔽传输信号,防止外部监测和干扰,同时支持多物理链路和多

物理端口冗余备份,提供系统的可用性。

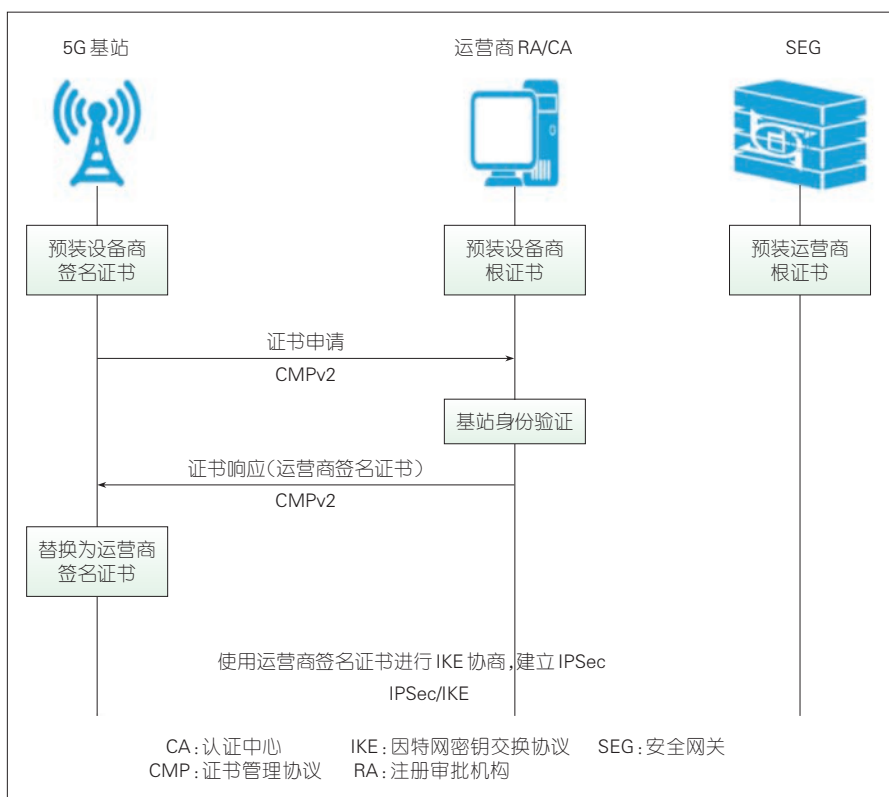
(2)链路层安全。对不同数据平面,链路层使用虚拟局域网(VLAN)隔离,防止 DoS 攻击和数据嗅探;支持 MACSec 加密,为用户提供安全的 MAC 层数据发送和接收服务,包括用户数据加密、数据帧完整性检查及数据源真实性校验;支持 802.1x 访问控制和认证协议,只有通过有效认证,基站才能接入运营商网络,网络物理端口才对基站开放,以限制未经授权的用户/设备通过接入端口访问局域网(LAN)/无线局域网(WLAN)。

(3)网络层安全。网络层支持 IPSec 安全隧道协议,提供端到端的加密和认证功能,保证数据的完整性和机密性。通信时和通信对象的

密钥交换方式使用 Internet 密钥交换协议(IKE)、RFC5996、数据传输使用封装安全载荷(ESP)报文格式、RFC4303。

5G 规范中引入了基于 PKI 的安全体系结构,3GPP 33.310 协议定义了基站数字证书的注册机制,以及应用数字证书与核心网安全网关(SEG)建立安全通信链路的过程^[3],具体如图 5 所示。

首先是准备阶段,基站由设备商预先提供出厂生成的公私钥对,并预装由设备商签名的数字证书、运营商的登记授权(RA)/证书授权(CA)服务器预装设备商的根证书、核心网 SEG 预装运营商根证书。然后基站向核心网注册使用 CMPv2 协议向 RA/CA 发起证书申请,RA/CA 则使用设备商根证书和



▲ 图 5 5G 公钥基础设施安全结构

设备商签名证书来对基站进行身份验证,验证通过后给基站签发运营商证书并返回证书响应,基站证书替换为运营商签名证书,完成基站注册。随后基站就使用运营商签名证书和核心网安全网关建立 IPSec 连接。

2.4 网管接口的安全方案

网管是对基站设备的管理系统完成基本的数据配置、监测控制、性能统计等功能。基站与网管系统通过 IP 网络连接,有可能暴露在公网,因此面临非法入侵、信息泄露、服务中断、物理破坏等安全威胁。和网管接口相关的安全解决方案如下几个方面。

(1) 账户管理。

基站系统支持集中账户管理和本地账户管理。集中账户是指由网管创建和管理并集中到网管进行认证的账户,本地账户是由网管创建但在基站本地进行认证的账户。账户管理支持常用的用户名密码方式认证,以及基于 PKI 的数字证书双因素认证方式。

对于使用用户密码认证方式,为避免密码易被破解,系统可以支持强制为系统配置高强度密码,如长度至少 8 位,密码必须至少包含数字、大写字母、小写字母、特殊字符中的 3 类。同时,系统支持检测密码强度是否满足要求,如果密码不满足规则,可以强制用户在登录时修改为高强度密码。

系统还可以根据不同的用户要求,为帐号设置对应的有效期,帐号到了有效期,将不允许再使用。为

了避免用户密码被暴力破解,系统支持对登录密码尝试次数做限定,超出尝试次数,用户会被锁定,锁定又支持按照用户来源锁定和按照用户锁定的锁定策略。

(2) 权限管理。

对接入系统的用户需要做身份认证,非授权用户不能接入系统。用户接入系统后,还需要进行权限控制,即用户能够读取/修改/执行系统文件是否在授权范围内。系统需要对用户分组,不同等级的用户分组有不同的权限。

登录用户通过身份验证后,可以对 5G 基站设备进行管理操作。基站需要根据用户的分组对用户操作进行授权控制,为用户授予相应的操作权限。系统遵循最小特权和职责分离的原则,为不同职能的用户创建出不同权限的角色。

同样,帐号信息类也有专门的权限控制,只有授予了帐号修改权限的安全管理员才能对帐号以及权限进行配置,避免帐号权限被恶意修改。

(3) 传输安全。

系统通过支持安全链路传输数据,使用安全通道协议(SSH)/安全文件传送协议(SFTP)/简单网络管理协议(SNMPv3)协议,以及基于这些协议实现的加密安全通道,确保数据在网络传输过程中难以被窃取和篡改。

采用 SSH/SFTP 协议可以有效地避免远程管理信息泄露问题,及上下层网络管理系统间的数据传输链路信息泄露问题。SSH/SFTP 协议提供的功能包括所有传输数据的

加密,防止域名系统(DNS)欺骗和 IP 欺骗,通过数据压缩加快数据传输,并替换 Telnet,为 FTP 提供安全通道^[4]。

采用 SNMP V3 协议对数据进行完整性检测,以保证数据不会在传输时被修改或者损坏,并且可以保证传输序列不会被故意修改。数据源的鉴别保证了传输数据和数据源对的一致性。数据加密确保了数据在传输时不会被窃取或者泄露。消息时间序列指的是超出制定时间窗生成的数据不会被接受。在消息重传和消息重新排序时,生成的消息可能会超出制定时间窗。SNMPV3 识别服务用来确定一个消息是否由消息实体识别的用户来发送,是否在传输中被编辑、重传或其传输方向被修改。SNMPV3 加密服务用来对消息实体加密以保证数据不会被直接读取^[5]。

(4) 敏感信息保护。

依据隐私保护原则,客户的隐私信息需要保密,也就是说没有权限的人不能查看,也无权传播。在必须要传播的某些数据中,如果携带了用户数据,则需要对用户数据做匿名化处理。

个人隐私数据指可以直接或者间接关联到用户个人的信息,如已知用户号码能反查到用户姓名,那么用户号码就是个人隐私。这种关联比较直接,称为直接个人信息。某些信息需要绕几个圈才能关联到用户信息的,称为间接个人信息。

所谓的匿名化指在任何有导出文件的地方,如果涉及到用户隐私

➡ 下转第 55 页



基于软件定义的 5G 网络安全能力架构

Security Capability Architecture of Software-Defined 5G Network

张鉴/ZHANG Jian, 唐洪玉/TANG Hongyu, 侯云晓/HOU Yunxiao

(中国电信股份有限公司网络与信息安全研究院, 上海 200000)
(China Telecom Corporation Limited Network and Information Security Research Institute, Shanghai 200000, China)

摘要: 基于 5G 网络“云化”和“软件定义化”的特点, 提出了基于软件定义的安全能力架构。认为该架构能够实现 5G 网络模块化的、可调用的、快速部署的内生安全能力, 能够更好地满足 5G 业务多样化和 5G 系统架构变迁所带来的安全新需求。

关键词: 5G 网络; 软件定义; 安全架构

Abstract: Based on the characteristics of "cloudification" and "software definition" of 5G network, a security capability architecture based on software-defined network is proposed. This architecture can realize the modular, invoked and rapidly deployed endogenous security capability of 5G network, which can better meet the new security requirements brought by the diversification of 5G service and the change of 5G system architecture.

Key words: 5G network; software defined; security architecture

DOI: 10.12142/ZTETJ.201904005
网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1059.004.html>

网络出版日期: 2019-07-16
收稿日期: 2019-05-22

5G 不仅是下一代移动通信网络基础设施, 而且是未来数字世界的使能者。5G 网络全新业务场景的出现和 5G 网络架构的变迁, 均对 5G 网络的安全能力提出了全新挑战。5G 网络需要具备模块化、可编排、可灵活调度的安全防御能力, 满足不同应用场景的动态、差异化的安全要求, 从而构建安全可信的网络空间。

软件定义的理念为建设 5G 安全能力提供了全新的思路, 随着 5G 网络系统架构“云化”和“软件定义化”的变革, 建设基于软件定义的安全能力体系成为可能。本文中, 我

们基于软件定义的理念, 提出了全新的 5G 网络安全能力架构, 并对该架构的部署方式、主要模块和接口功能, 以及带来的价值赋能进行了全面的阐述和分析, 为 5G 网络安全建设提供有借鉴性的参考。

1 5G 网络总体架构

未来的 5G 网络将更加灵活、智能、融合和开放。5G 目标网络逻辑架构简称“三朵云”架构, 包括接入云、控制云和转发云 3 个逻辑域, 如图 1 所示。

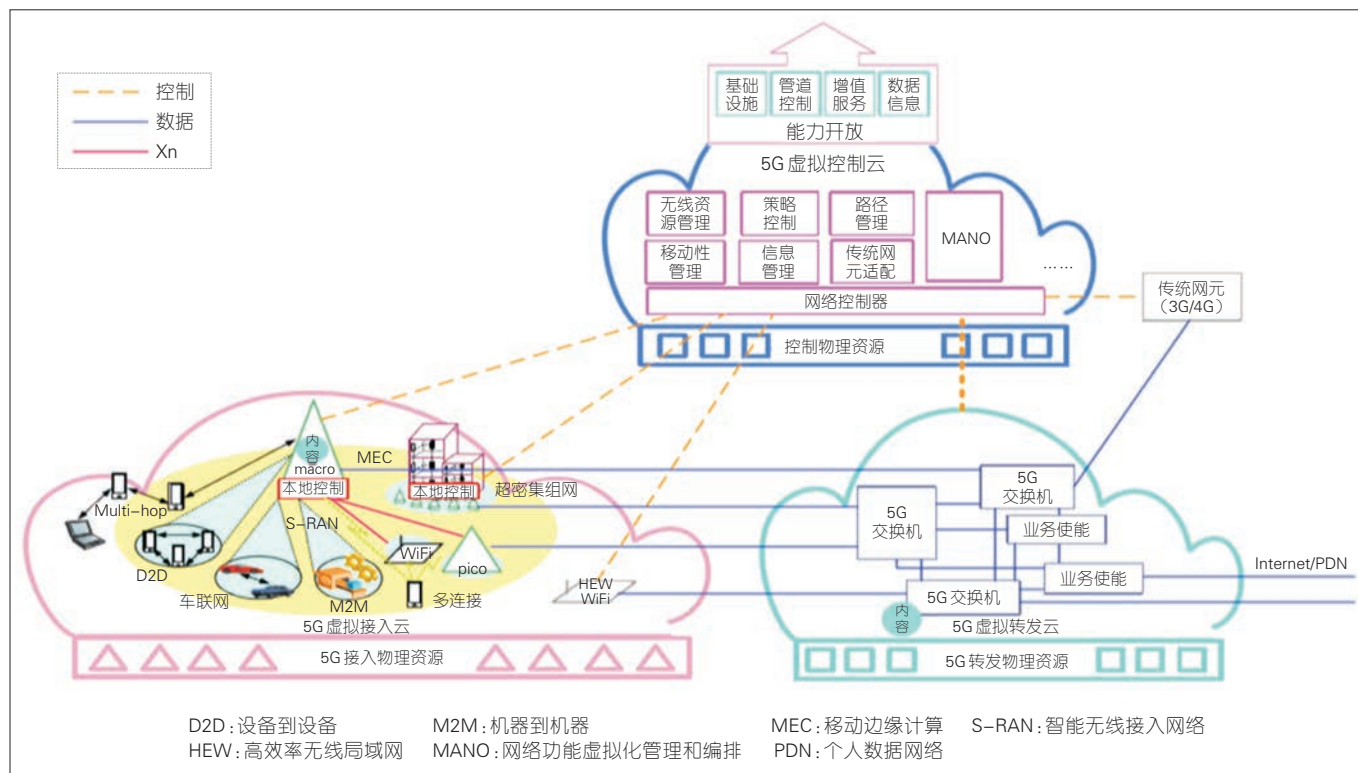
总体架构基于软件定义网络 (SDN)、网络功能虚拟化 (NFV)、云

计算等关键技术推动网络架构重构, 构建简洁、敏捷、集约、开放的网络新架构^[1]。

(1) 接入云: 支持接入控制和承载分离、接入资源的协同管理, 满足未来多种部署场景 (例如集中、分布、无线 Mesh), 并实现基站的即插即用。

(2) 控制云: 实现网络控制功能集中, 网元功能具备虚拟化、软件化以及重构性, 支持第三方的网络能力开放。

(3) 转发云: 将控制功能剥离, 使转发的功能靠近各个基站, 将不同的业务能力与转发能力融合。



▲图1 “三朵云”5G网络总体逻辑架构

在上述5G网络架构中,SDN技术是连接控制云和转发云的关键;NFV将转发云中的转发设备和多个控制云中的网元用通用设备来替代,从而节省成本;三朵云中的资源调度、弹性扩展和自动化管理都是依赖基础的云计算平台。

2 5G 网络安全需求分析

2.1 业务多样化需要差异化的安全能力

国际电信联盟(ITU)定义了5G的3大应用场景:增强移动宽带(eMBB)、海量机器类通信(mMTC)、高可靠低时延(uRLLC)。不同的业务会有差异化的需求,5G需要针对eMBB、mMTC和uRLLC 3种应用场景提供不同安

全需求的保护机制。eMBB聚焦对带宽和用户体验有极高需求的业务,不同业务的安全保护强度需求是有差异的,因此需要针对客户提供的安全能力具备可编排性和模块化;mMTC聚焦连接密度较高的场景,终端具有资源能耗受限、网络拓扑动态变化、以数据为中心等特点,因此需要轻量级的安全算法、简单高效的安全协议;uRLLC侧重于高安全低时延性的通信业务,需要既保证高级别的安全保护措施又不能额外增加通信时延,因此需要安全能力的敏捷快速部署^[2]。

2.2 新技术、新架构带来的安全挑战

5G新的网络架构引入了SDN、NFV技术,解耦了设备的控制面和

数据面。这为基于多厂家通用信息技术(IT)硬件平台建立新型的设备信任关系创造了有利条件,但是也给安全方面带来很多挑战。

首先是传统封闭管理模式下的安全边界和保障模式都在发生深刻的变化,业务的开放性、用户的自定义和资源的可视化应用给云平台的安全可信带来前所未有的挑战;其次,计算、存储及网络资源共享化,会引入虚拟机安全、虚拟化软件安全、数据安全等问题。5G网络中NFV虚拟化技术的应用,可进一步简化网络功能的部署和更新,使得部分功能网元以虚拟功能的形式部署在云化的基础设施上。5G需要考虑虚拟化基础设施的安全机制,从而保障其业务在虚拟化环境下能够安全运行;还需要定义更好的安

全隔离手段,增强虚拟功能网元之间的安全管理。基于虚拟网络的切片也需要安全机制,以保证切片的安全运营和用户的正常接入。

因此,传统的安全防护模式已不再适用,5G的发展迫切需要利用5G网络架构的有利条件,挖掘出5G网络的内生安全属性,建立基于软件定义的新型安全能力架构,实现构建高可信、高安全的5G网络的目标^[3]。

3 基于软件定义构建 5G 网络安全能力框架

3.1 软件定义安全逻辑架构

借鉴软件定义的理念和SDN架构,软件定义安全(SDS)逻辑架构包括3个层面,从下向上依次是:基础设施层、控制层、应用层,具体如图2所示。

(1)应用层:包括各种各样的安全应用及服务,实现安全业务的封装、编排和对外提供。

(2)控制层:核心是安全控制器,南向通过应用程序编程(API)接口和安全资源池进行互动,对安全资源池进行管理和调度;北向通过API对外提供封装后的安全能力甚至是安全业务;东西向和网络控制器、云等互通,实现安全流量的检测和安全策略的下发和控制。

(3)基础设施层:包括各种硬件、软件形态的安全设备、安全引擎,提供安全的原子功能,形成云化的安全资源池。

软件定义安全架构相应的接口包括北向接口(控制层与应用层接

口)和南向接口(控制层与基础设施层接口),具体如图3所示。

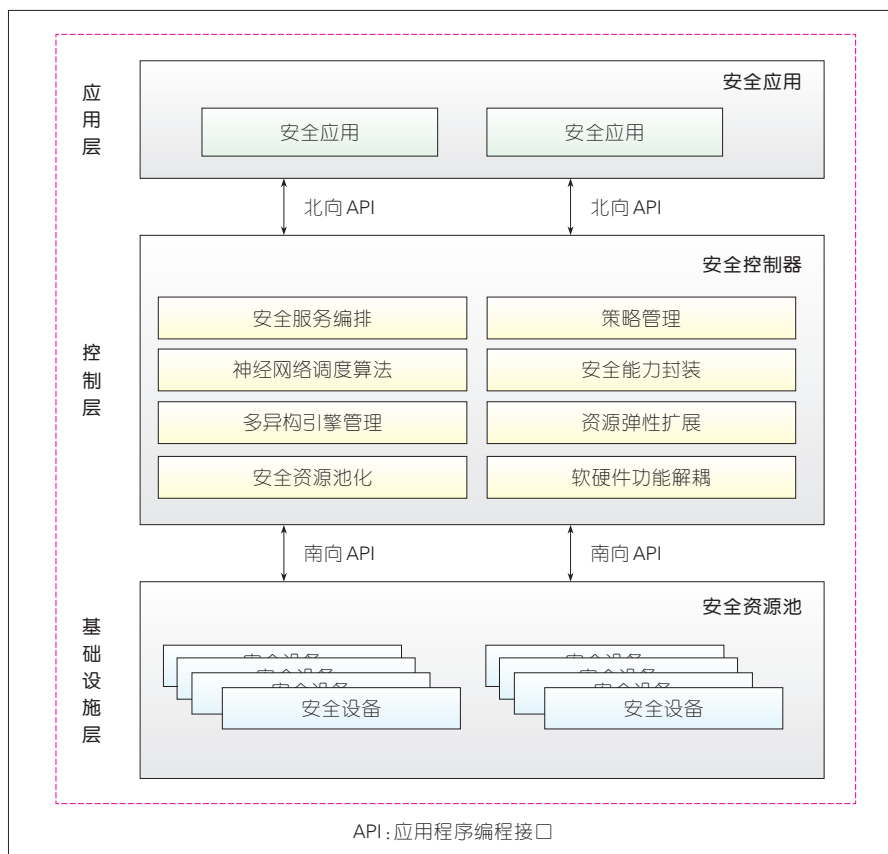
(1)北向接口:控制层与应用层接口(NBI)。

• 连接SDS控制器和用户应用

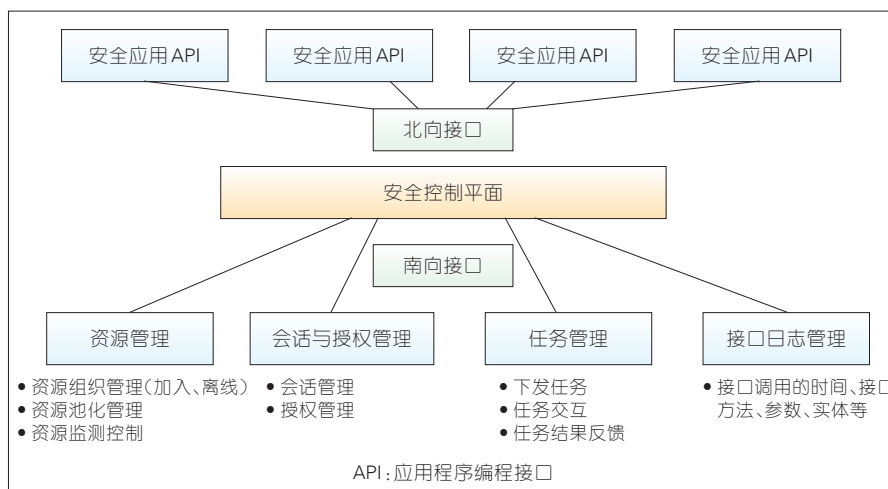
之间的重要纽带;

- 为应用平面提供安全能力,可用于上层应用开发和资源编排;
- 具有多样化的特征。

(2)南向接口:控制层与基础设



▲ 图2 软件定义安全逻辑架构



▲ 图3 软件定义安全南北向接口

施层接口(SBI)。

- 控制平面与基础设施平面交互安全策略以及设备信息等数据的信息;

- 将差异化的安全设备抽象成统一的安全资源池,集中管理,统一部署;

- 打破传统硬件资源的封闭性,为不同设备厂商、不同功能的安全设备提供了管理和部署方面的便利条件。

3.2 5G 网络软件定义安全防护框架

5G 网络增强了开放服务能力,

基于 SDN/NFV 的编排能力是 5G 网络的重要能力集;因此,基于 SDN/NFV 的统一编排能力,可以将软件定义安全的架构应用到 5G 网络安全防护体系中,从而保障 5G 网络具备保证各项业务安全的安全机制。基于软件定义的 5G 安全防护框架具体如图 4 所示^[4-5]。

基于软件定义的 5G 安全防护框架的主要有 6 个模块。

(1)安全服务层:向 5G 垂直行业和 5G 用户提供可定制化、可编程的安全服务。

(2)安全控制及编排层:根据来自安全服务层或安全数据分析层的

安全需求,将安全策略下发给相应的安全设备实现安全防护。

(3)安全分析器:使用大数据、人工智能等技术,将安全分析的结果转化为安全需求再发送给安全编排器。

(4)网络控制及资源编排层:包含 SDN 控制器和 MANO 系统。SDN 控制器根据来自安全控制层的策略,实现流量的编排、管理。MANO 系统实现对安全功能需要的虚拟化资源的编排、管理,以及虚拟安全网元的生命周期管理。

(5)资源池:包含硬件资源、安全资源池以及业务资源池。

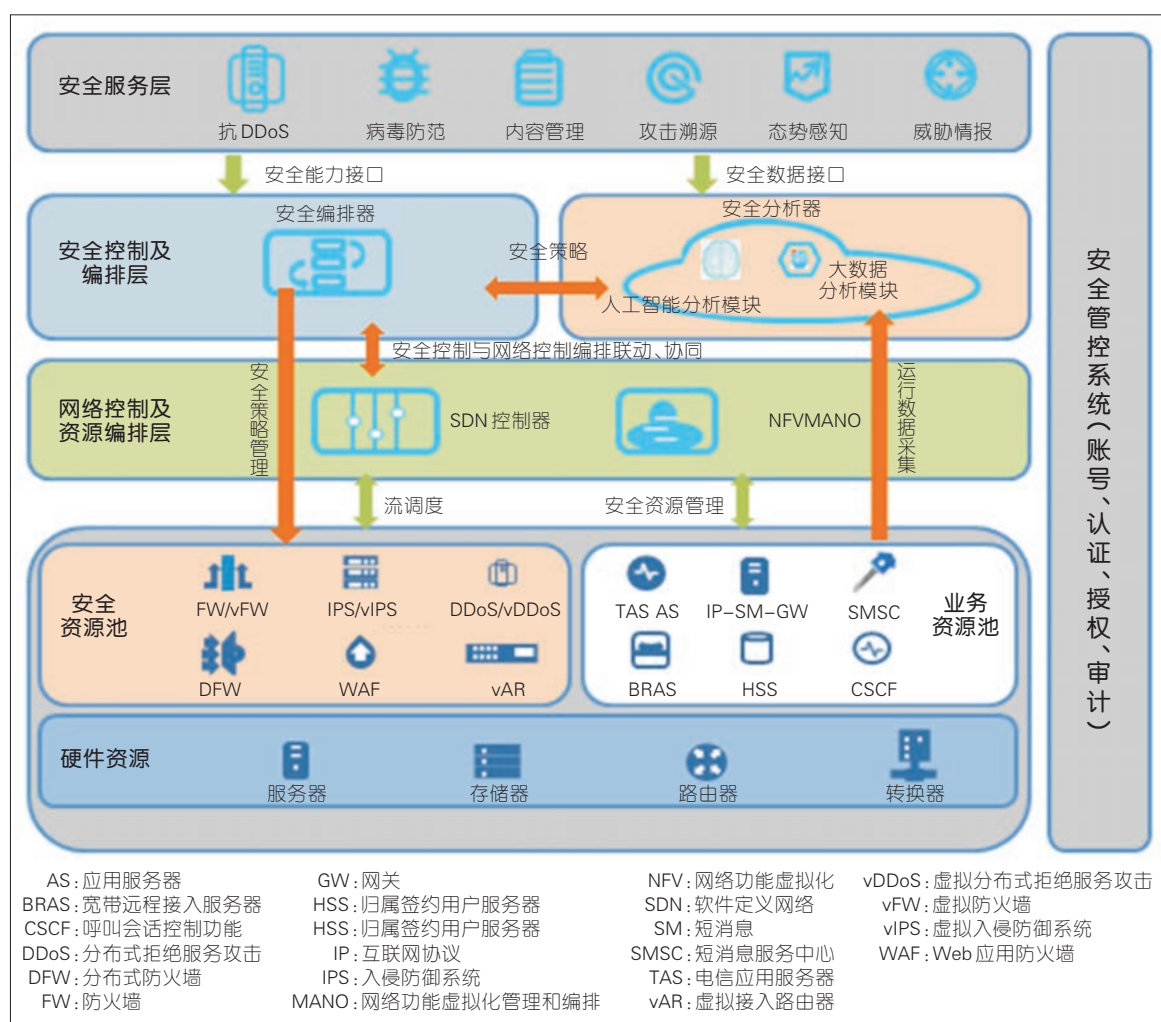


图 4
基于软件定义的
5G 安全防护框架

(6)安全管控系统:包含统一账号管理、认证管理、授权管理以及审计管理,可将安全控制器、智能分析与可视化工具等统一纳入至安全管控体系。

3.3 软件定义的 5G 网络安全能力架构优势

通过构建基于软件定义的 5G 安全能力架构,能够实现 5G 网络模块化的、可调用的、快速部署的内生安全能力,能够更好地满足 5G 业务多样化和 5G 系统架构变迁所带来的安全新需求。

(1)安全能力模块化管理,实现架构的可扩展和可编排。

基于软件定义的架构,可以将网络安全能力进行独立的服务化定义,封装为安全能力模块。其他功能在授权的基础上,可以调用此安全能力模块。这里安全能力包括用户身份管理、认证鉴权、密钥管理及安全上下文的管理等。安全能力的模块化增强了安全能力的精细灵活化管理,支持基于安全编排的弹性灵活调用,同时支持对调用安全能力的授权。5G 网络内的安全能力以模块化的方式部署,并能够通过相应接口方便调用。通过组合不同的安全功能,可以灵活地提供安全能力以满足多种业务的安全需求。

(2)安全功能的快速部署以及调用。

基于软件定义的架构,在安全能力模块化的、可调用的、可组合的基础之上,可实现安全功能自动化管理,包括安全功能的部署、编排、配置、调用等。相对于传统的人工配置的方式,该架构可以极大地提高效率,节省成本,使垂直行业可以直接安全地部署业务,从而降低了业务门槛并缩短部署时间。

(3)安全能力开放,实现价值的共赢。

基于软件定义的架构,垂直行业可以直接使用运营商开放的安全能力,降低了一些新型垂直行业的业务门槛和成本,缩短上市时间。通过安全能力开放,运营商可以盘活网络资产和基础设施,开创新的利益增长点;可以打破管道化运营和封闭网络模式,以电信网络为中心构建安全生态系统;可以提升差异化竞争力,形成运营商、垂直行业、安全厂商、个人用户的生态链,合作共赢共创商业价值。

4 结束语

5G 安全需要针对更加多样化的应用场景、差异化的网络服务方式以及新型网络架构,提供全方位的安全保障。目前,5G 试商用化工作正在全面启动,因此尽早明确 5G 网络安全需求,建设符合 5G 安全需求和网络特性的安全能力架构,是当前一项紧迫的重要工作。本文中

我们基于软件定义的理念,提出了全新的 5G 网络安全能力架构,希望能为 5G 网络安全建设提供有借鉴性的参考。

参考文献

- [1] 中国电信. 中国电信 5G 技术白皮书[R]. 2018
- [2] 3GPP. 5G Security Architecture and Procedures for 5G System: 3GPP TS 33.501 version 15.4.0 Release 15[S]. 2019
- [3] 3GPP. System Architecture for the 5G System: 3GPP TS 23.501 V16.0.2[S]. 2019
- [4] Open Networking Foundation. Software Defined Networking: the New Norm for Networks[EB/OL]. (2013-11-16)[2019-05-22]. https://www.techlib.com/en/view/shapcart/software-defined_networking_the_new_norm_for_networks
- [5] 华为. 华为 5G 安全架构白皮书[R]. 2017
- [6] ETSI. Network Functions Virtualization (NFV) Security and Trust Guidance: ETSI GR NFV-SEC 003 V1.2.1[S]. 2016

作者简介



张鉴, 中国电信股份有限公司网络与信息安全研究院云安全研究所高级工程师; 主要研究方向为云安全、5G 安全、安全攻防。



唐洪玉, 中国电信股份有限公司网络与信息安全研究院云安全研究所所长; 主要研究方向为云安全、态势感知、威胁情报。



侯云晓, 中国电信股份有限公司网络与信息安全研究院云安全研究所工程师; 主要研究方向为威胁情报、云安全、5G 安全。

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

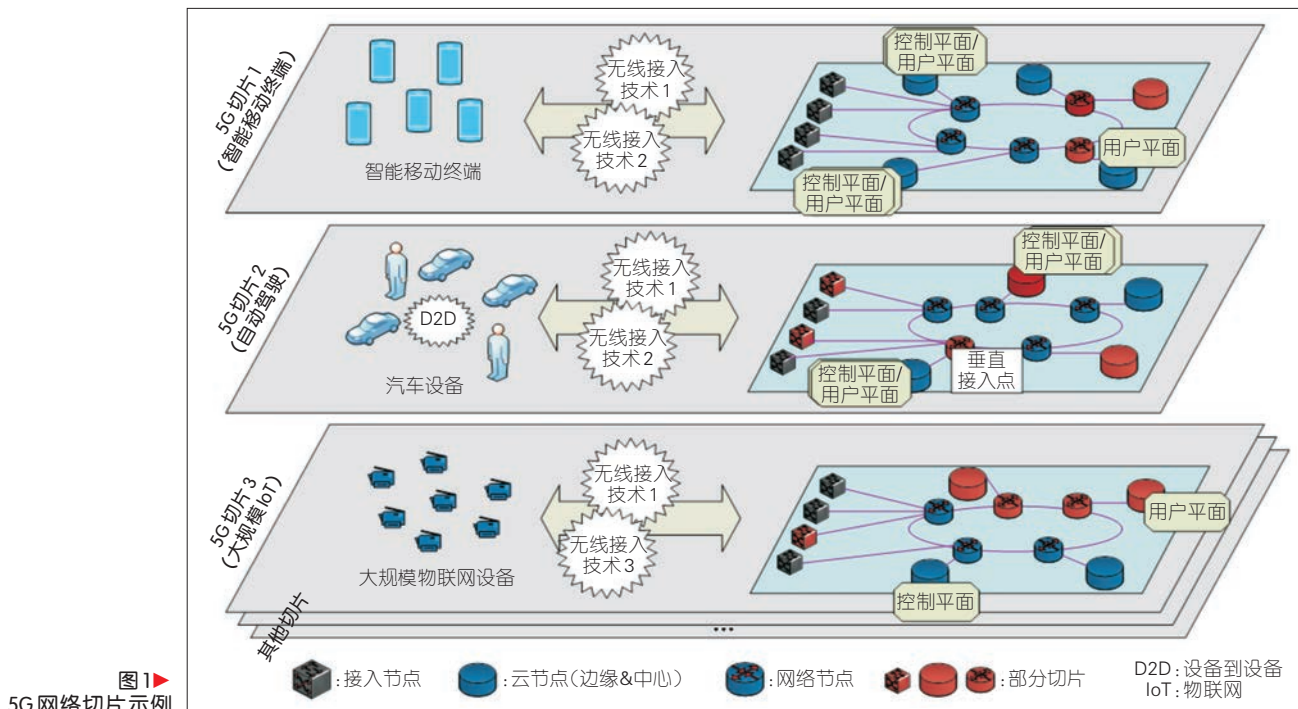
形成整体统一管理,再进一步分割实现网络切片。资源的统一和网络的分割是基于软件定义网络(SDN)和网络功能虚拟化(NFV)实现的。网络切片包括横向切片和纵向切片,首先横向分为不同的虚拟网络功能,然后根据服务需求对这些虚拟网络功能进行纵向切片以得到不同的网络子切片^[2]。网络切片在5G网络中部署示例如图1所示,其中控制平面(CP)是传送控制信令的通道,用户平面(UP)是传送用户数据的通道。网络切片由服务实例层、网络实例层及资源层组成,每种服务由一个服务实例表示。服务运营商利用切片规划生成网络切片实例,切片实例则可以被多个服务实例所共享。网络切片可以为5G环境下差异化需求的应用场景提供灵活的适应方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



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。

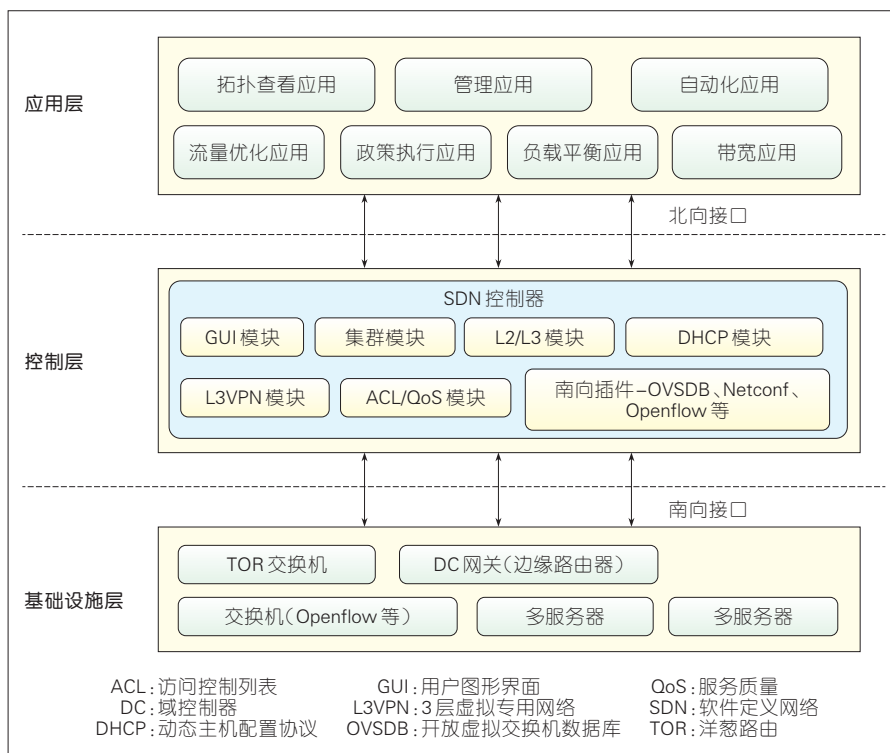
SDN 的目标是集中网络控制,提供更高的可视性和灵活性来管理网络并优化其性能^[4]。与覆盖网络方案相比,SDN 不仅能够控制选定的一组节点,还能够使用公共网络

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

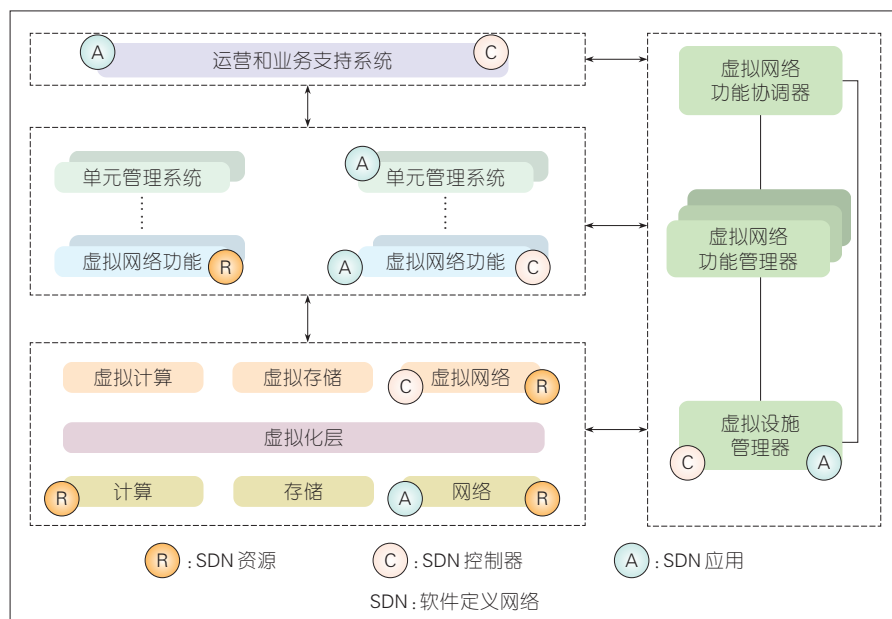
3.1 安全问题概述

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安全学院在读博士; 主要研究领域为无线网络安全、安全协议设计与分析; 参与多项国家自然科学基金重点项目及国家自然科学基金重点基金项目; 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安全学院副教授、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基金项目; 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安全学院执行院长、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。

5G时代大容量光接入网的安全技术

Security Technology of Large Capacity Optical Access Network in 5G Era

张宏熙/ZHANG Hongxi

(中兴通讯股份有限公司, 广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)



摘要: 5G时代,光接入网会逐步承载5G应用,并向固移融合(FMC)的方向不断演进。在这种应用场景下,光接入网的安全将面临更多的威胁和挑战。无源光纤网络(PON)在演进到下一代PON2(NGPON2)的过程中,安全能力也逐步加强。5G网络面向垂直行业的安全应用使得光接入网面临着切片化的变革。光接入网必将融入到5G网络中,和5G网络一起为用户构建端到端的安全防护网。

关键词: 光接入网;无源光网络;安全;5G技术

Abstract: In the 5G era, optical access network will gradually carry 5G applications and evolve to fixed-mobile convergence (FMC). The security of the optical access network will face more threats and challenges. In the process of the evolution from passive optical fiber network (PON) to the next generation PON2 (NGPON2), the security of PON is also gradually strengthened. At the same time, the security requirements of 5G network for vertical industry make the optical access network face the revolution of slicing. It is considered that optical access network will be integrated into 5G network, which can build the end-to-end security protection network.

Key words: optical access network; passive optical network; security; 5G technology

DOI: 10.12142/ZTETJ.201904007

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1006.002.html>

网络出版日期: 2019-07-19

收稿日期: 2019-05-26

1 5G时代光接入网的发展趋势

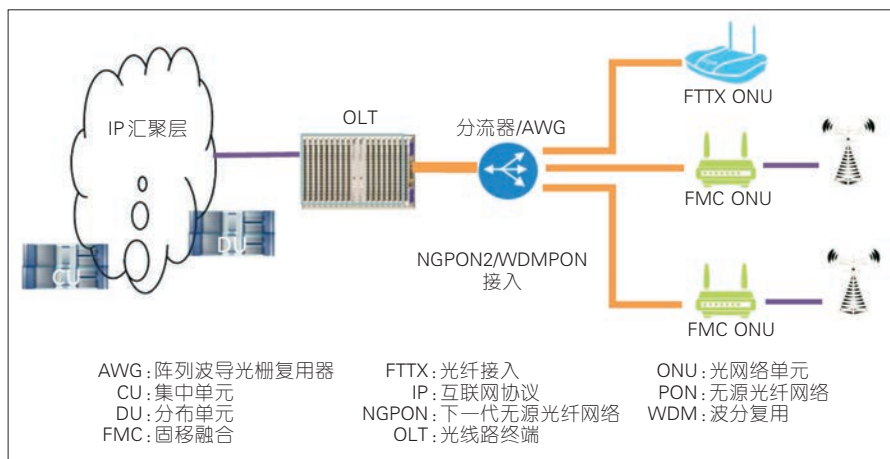
光纤接入网络经过十几年的高速发展,经历了光进铜退、光纤到小区,目前已经进入光纤到户的阶段。随着高清视频业务的不断兴起,以及移动网络从4G往5G的成熟演进,光接入网必将逐步承载大视频以及5G相关的业务,并伴随着虚拟化、云化的变革,朝着固移融合(FMC)(具体如图1所示)的方向

发展。

因此,5G光接入网在承载传统接入业务的基础上,还将承载着更多的大视频业务以及移动业务,包括5G前传及中传业务。4K/8K高清视频业务的发展,对用户带宽的提升提出新的需求,目前光接入网的带宽从100M、1G逐步过渡到10G。因此,光纤接入(FTTX)技术从1G无源光纤网络(PON)演进到10G PON,并向下一代(NG)PON演进。在高带宽提升的同时,5G移动

前传或中传的承载,对光接入段的时钟精度要求在20ns以下,时延要求500μs以下。波分技术更适合传递低时延的业务,国际电信联盟电信标准化部门(ITU-T)G.989已经对NGPON2技术定义出了标准规范。另外,IEEE 1588技术会更多地应用在光接入的相关领域,并从IEEE 1588V2升级到IEEE 1588V3,以更好地保证时钟及时间的高质量传递。

FMC要求网络提供者给不同



▲图1 光接入网络固移融合的场景

服务等级(QoS)的业务或不同运营商的业务提供一个共享的接入平台,或者说在承载5G网络后,5G时代各垂直行业多样化的业务需求会间接反映到光接入网络上面。网络切片正是满足这类需求的重要技术,目前已经在各大运营商中开始部署。

视频业务的发展对网络带宽的优化提出了新的需求,通过光线路终端(OLT)的内置刀片部署边缘内容分发网络(CDN)节点是一个有效的解决方案。该方案可以降低视频业务的时延,增强边缘处理能力,让OLT成为边缘云计算平台的节点。同时,基于网络扁平化和虚拟化的要求,将宽带网络网关(BNG)下移以和OLT的转发面融合,同时控制面上移云端,电信网络软件定义网络(SDN)/网络功能虚拟化(NFV)化给业务的快速部署带来优势。

中兴通讯的大容量光接入平台(TITAN)支持未来NGPON2的大带宽接入,也支持5G前传和中传;内置刀片技术支持边缘计算处理能力,也支持切片技术、SDN/NFV的

虚拟化演进。

2 5G时代光接入网的安全挑战

5G网络对于增强移动宽带(eMBB)、海量机器类通信(mMTC)、高可靠低时延(uRLLC)这3大应用场景和相关安全要求都有明确规划。5G网络是一个大容量的网络,在承载5G后,光接入网的光网络单元(ONU)从光纤到户(FTTH)的一个用户或少量用户转变为5G和FTTH融合的FMC接入,尤其是5G网络支持广连接、高覆盖的物联网接入,容量的提升要求其安全性也要上一个台阶。另外,5G是一个开放的网络,海量的设备会暴露在更靠近用户的区域,更易被黑客控制或攻击。一旦遭到安全攻击,影响面会非常大。如何避免受到网络攻击,如何避免敏感信息不被泄露,如何保证设备的可用性不受影响,如何在受到安全攻击的情况下又如何把损失降低到最小,都是需要我们持续研究的课题。本文中,我们将重点探讨5G安全挑战下

的PON网络安全技术。

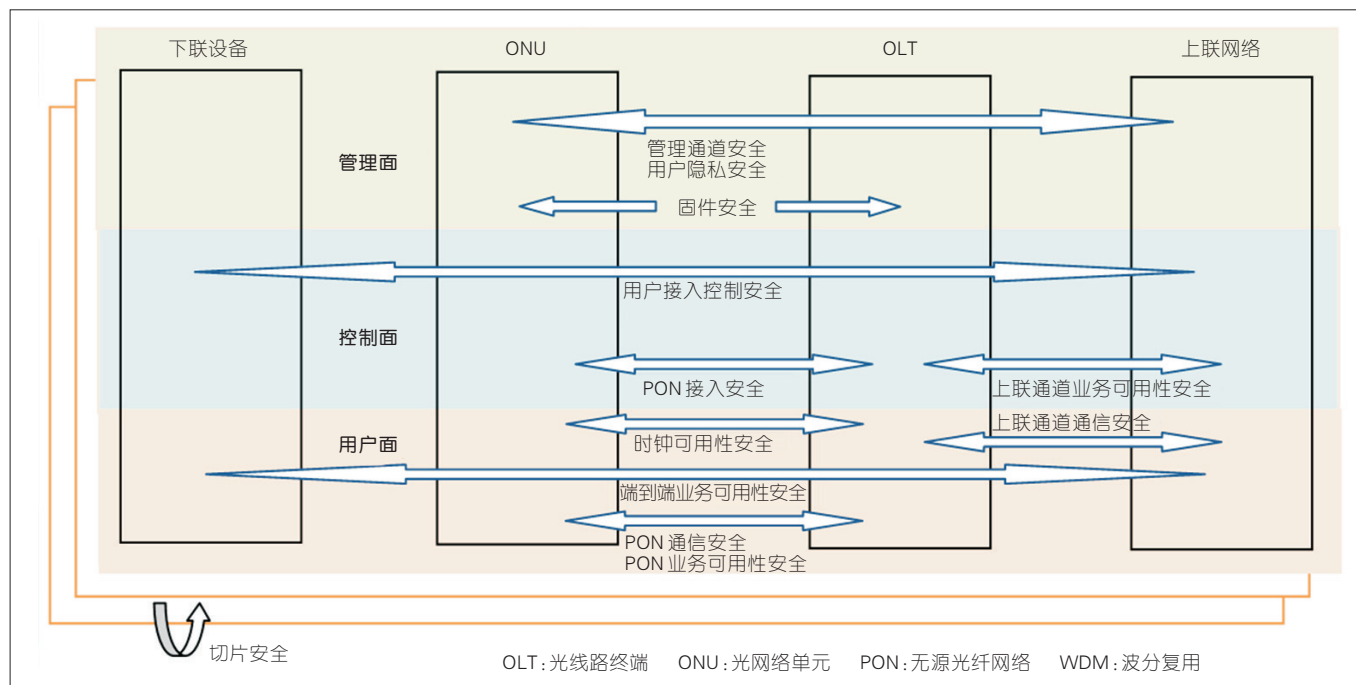
5G网络的承载,必然让光接入网络的架构产生重大变革。边缘节点的下沉,对接入网络的安全级别要求提高,原有针对核心网络的攻击模型需要引入接入层;为了支持切片功能,软件架构会进行重构,以便支持切片的快速部署、差异化服务及可剪裁等特性;为了提高通信系统的灵活性、可扩展性,提升业务的部署速度,还会考虑引入信息技术(IT)。

对于5G安全架构,NFV/SDN化和微服务化是其发展的必然趋势。5G安全架构会面临新的挑战,其安全功能也会和其他的功能一样在新架构里灵活地进行编排和部署。虚拟化、云化相关的云安全联盟已经在这方面进行了深入研究。本文中,我们会基于切片技术引入的光接入网架构变化做探讨。

3 光接入网的安全架构

参照ITU-T X.805的标准建议,我们对光接入网的安全架构进行分析。ITU-T X.805建议的安全架构分为3层(应用安全层、业务安全层、基础设施安全层)、3面(端用户平面、控制平面、管理平面)。针对3层3面的资产,我们定义了8个安全维度(接入控制、认证、不可否认、数据保密性、数据完整性、通信安全、可用性、隐私性)、5类安全威胁(摧毁、破坏、移除、泄露、中断)。

图2是光接入网的安全架构,包括基础设施层的3个平面(用户面、管理面、控制面)相关的安全模型。其中,光接入网络主要涉及



▲图2 光接入网的安全架构

基础设施层,少量位于服务层。文章中,我们重点探讨基础设施层的安全。

(1)用户面。主要涉及PON层的通信安全、PON业务可用性安全、端到端业务可用性安全、时钟可用性安全、切片安全等。

(2)控制面。主要涉及PON ONU接入安全以及用户接入控制安全等。

(3)管理面。主要涉及管理通道安全、用户隐私安全,以及固件安全等。

对于各层的安全,我们分别做如下考虑:针对PON层通信安全,主要考虑应用PON层加密技术;针对PON ONU接入安全,主要考虑应用PON接入认证技术;针对PON接入业务可用性安全,主要考虑应用PON保护技术;针对端到端业务可用性安全,主要考虑分布式的防拒

绝服务(DoS)攻击技术;针对时钟同步安全,主要考虑时钟和时间传递的保护和备份技术;针对切片安全,主要考虑切片隔离和权限控制技术;针对用户隐私安全,主要考虑数据保护技术和脱敏技术;针对固件安全,主要考虑数字证书技术。

4 关键安全技术

4.1 PON网络通信安全技术

通过建模分析,我们可以发现PON网络的通信安全主要存在以下威胁:

(1)在PON系统中,下行数据向PON上所有ONU进行广播。如果有恶意用户对ONU进行更换或重新编程,那他就能分析出所有用户的所有下行数据。这是PON安全系统会遇到的“窃听”威胁。

(2)上行数据可以来源于接入

特定ODN的所有ONU。如果有恶意用户对ONU进行更换或重新编程,那他就可以通过伪造报文的方式来仿冒其他的ONU。

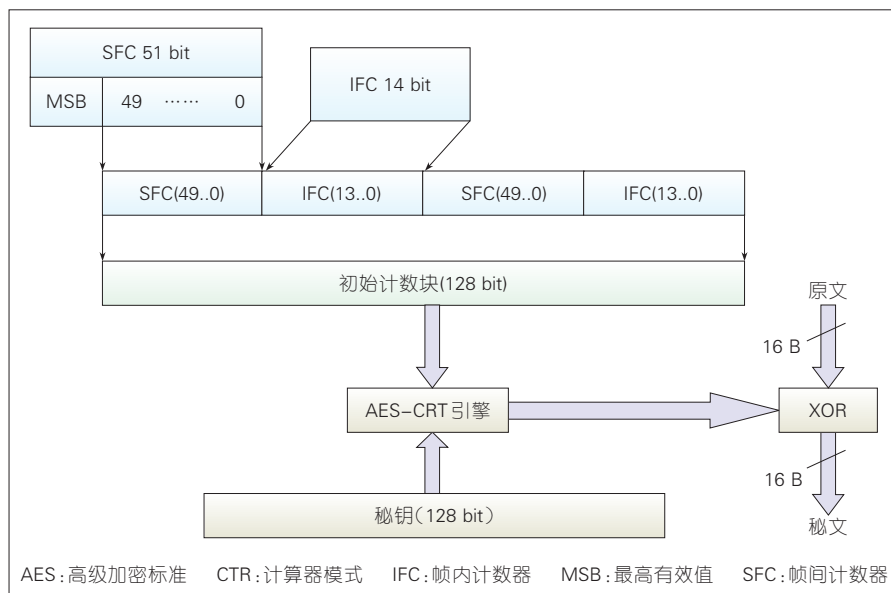
(3)攻击者还可以在基础设施上的不同点连接恶意设备(例如通过篡改街道机柜、备用端口或光纤电缆),以拦截或产生流量。根据不同位置,设备可以模仿OLT的行为,或可以模仿ONU的行为。

当然,点对点(PtP)模式的波分复用(WDM)-PON相对于传统的PON网络或时分波分复用(TWDM)-PON网络,安全威胁要弱一些,因为这种模式下不同用户通过波长进行了隔离。其主要的威胁来源于恶意破坏物理设备以模仿OLT或ONU设备的行为,或由于阵列波导光栅复用器(AWG)的性能问题或恶意干扰导致的不同波长间的串扰。对于物理设备的恶意破

坏,则需要加强其管理,提升 AWG 的抗干扰性能,并且强化 ONU 的认证机制。

针对加密技术,吉比特无源光网络(GPON)可采用 ITU-T G.984.3 建议的高级加密标准(AES)技术,它以 16 字节(128 bit)为单位进行操作,可以使用 128,192 或 256 bit 的密钥。AES 加密采用计数器(CTR)模式,计数器宽度为 46 bit,由 16 bit 的帧内计数器和 30 bit 的帧间计数器组合而成。46 bit 的计数器复制 3 次后保留并使用最低的 128 bit,按照 AES 算法生成密码进行数据加密。加密密钥则由 ONU 产生,并定期和 OLT 进行交互,OLT 收到密钥后,和 ONU 同步进行切换。这些交互的具体过程借助 PON 物理层的维护管理(PLOAM)通道来完成。

ITU-T G.984.3 仅要求下行的加密,而 ITU-T G.984.3 以后的标准(XGPON 开始,包括 ITU-T G.987、ITU-T G.9807^[4]和 ITU-T G.989^[5]等)则要求了双向加密。双向加密中,这 64 bit 是由 14 bit 的帧内计数器和 51 bit 的帧间计数器的低 50 位组合而成(如图 3 所示)。另外,密钥交互过程也更复杂,由 OLT 发起的多次交互来完成。密钥交互和切换通过 PLOAM 通道完成。另外,ITU-T G.984 仅规范了下行单播数据的加密,而 ITU-T G.987 以后的标准则规范了上下行的单播,以及下行组播通道的加密。下行组播通道的加密密钥由 OLT 生成,并通过光网络单元管理控制接口(OMCI)通道传递给 ONU。



▲ 图3 下一代无源光网络的网络加密方法

在管理通道完整性安全方面,ITU-T G.984.3 仅要求 PLOAM 通道和 OMCI 通道采用循环冗余查核(CRC)校验,而 ITU-T G.987 以后的标准则要求这 2 个通道采用基于 AES 加密方式的消息认证码(AES-CMAC)的方式进行加密。

其他方面的加密技术,还包括 ITU-T G.983.1 定义的搅动(Churning)算法、中国电信在基于以太网的无源光网络(EPON)技术规范中要求的三重搅动技术等。PON 系统采用 CTR 模式的 AES 加密技术,相当于一次一密,安全性相对比较高,其薄弱环节在于密钥(图 3 中的密钥)从 ONU 到 OLT 的传递过程。从 ITU-T G.987 开始,各个标准均对密钥的加密传送进行了规范,并要求采用电子密码本模式(ECB)的 AES 方法,但是其使用的密钥是加密密钥(KEK),存在一定的安全风险。在不考虑 PON 互通性的前提下,采用非对称的加密方

式进行密钥管理将能够较大幅度地提升安全性。

针对 PtP 类型的 WDM-PON 系统,加密技术没有在标准里被定义。针对移动前传和中传,尤其是仅针对接口进行透传处理的场景,加密可主要依靠基站和分布单元(DU)/集中单元(CU)间的数据进行,如 MACSec 技术等。

在接入认证方面,ITU-T G.984 定义了 ONU 序列号和密码 2 种认证方式。序列号或密码通过 ONU 经由 PLOAM 通道上报,OLT 会将其和预设置的序列号或密码进行关联判断。ITU-T G.987 以后的标准定义了基于 Register ID 的认证方式,可以经由 OMCI 通道进行双向认证,也可以通过 IEEE 802.1X 进行双向认证。

未来的 PON 网络认证技术,应在已有标准化的认证技术基础上,增加对 ONU 的许可证(license)控制、数字证书校验等新技术,即在

OLT上增加对ONU的许可控制,限制PON口下接入的终端型号,以及对应型号的接入数量。此外,如果在OLT上增加数字证书认证技术,针对ONU的固件进行基于数字证书的认证,可以最大程度地防止对ONU固件的篡改。可行的一种方式是在ONU上线的过程中对OLT和ONU上存放的数字证书进行比较。对于不一致的情况,则不允许上线。

4.2 PON网络流氓ONU防护技术

在PON网络里,存在这样一种威胁:由于某个ONU工作异常或攻击者通过ONU进行更换或重新编程,不依据OLT下发的授权时隙发送上行数据,或不依据OLT分配的逻辑通道ID发送上行数据。这样会影响到其他ONU的正常工作。由于上行时隙的重叠或逻辑通道的冲突,会导致其他ONU产生误码甚至业务中断,引起可用性问题。

我们可以从3个方面来应对该威胁:

(1)检测。

针对连续长发光型的流氓ONU,可以通过PON口的告警来识别。出现这种情况时,PON口会出现严重的误码,甚至上行突发丢失、出现信号丢失告警或ONU掉线告警。更严格的识别方法包括定期在非授权时隙进行检测,看能否发现从ONU送上的连续光信号。

针对瞬间长发光型的流氓ONU,也可以通过PON口的告警来识别。出现这种情况时,PON口会出现误码,某些ONU的窗口漂移告

警、上行突发丢失及ONU的掉线告警(一般是和流氓ONU相邻的ONU)。更严格的识别方法具体包括定期在非授权时隙进行检测,看是否有可能检测到非授权时隙瞬间发光。

针对逻辑通道非法抢占的情况,一般体现为某些逻辑通道业务异常或告警,辨识上会更困难一些。

(2)定位。

针对连续长发光型的流氓ONU,可以通过OLT对ONU顺序下发关光的指令或顺序物理断开ONU的方式。如果某个ONU关光后,长发光异常消失,则流氓ONU得到定位;如果某个ONU开电前后系统由正常进入异常状态,则流氓ONU也可得到定位。

针对瞬间长发光型的流氓ONU,可以通过检查动态带宽分配(DBA)列表中出现告警的ONU位置统计信息,得到流氓ONU及受影响ONU清单;通过和连续长发光型的流氓ONU类似的方式,进行该清单中ONU的关光或物理断开的方式,最终定位出流氓ONU。

针对逻辑通道非法抢占的情况,可以通过检测ONU上线时间,结合逻辑通道相关业务异常的时间,对非法强占逻辑通道的流氓ONU进行初步定位,并依次得到流氓ONU及受影响ONU清单,再通过类似连续长发光型的流氓ONU类似的方式,进行该清单中ONU的关光或物理断开,最终定位出流氓ONU。

(3)隔离或防护。

针对定位出的流氓ONU,可以

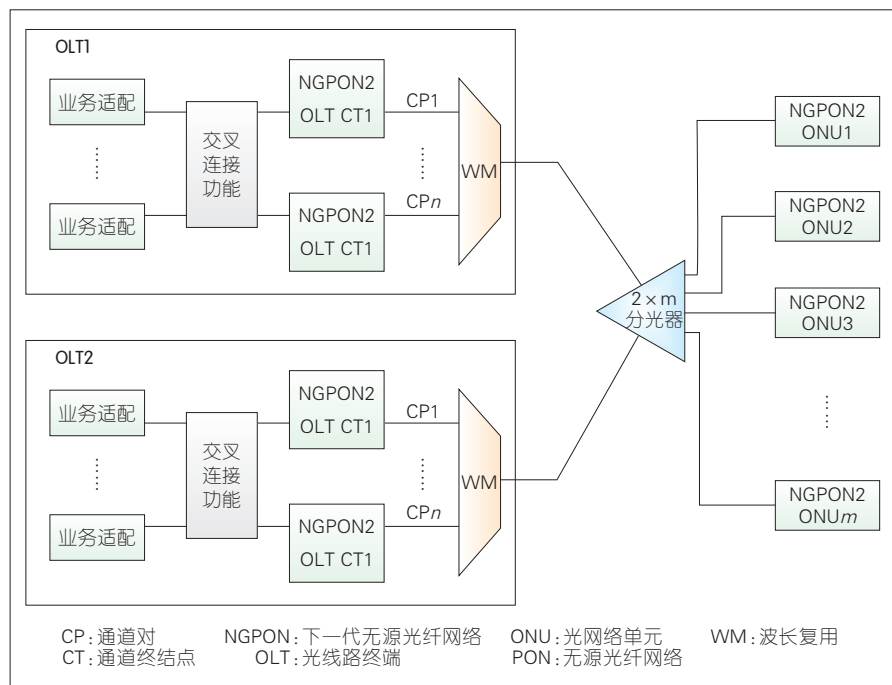
远程发送下线指令,或采用人工关电来进行隔离。对于非法抢占逻辑通道的流氓ONU,也可以采用逻辑通道编号和ONU认证信息绑定的方式进行防护。上行的非法逻辑通道的业务无法匹配绑定清单中的条目,OLT会对该业务进行忽略。

以上的方法适用于普通的PON网络和NGPON2的网络。针对多波长的场景,在每个可能的波长中都需要进行检测和防护。但是,从某种意义上说,以上的方法仅能防范部分的流氓ONU,对于非常恶意的光层的干扰,还需要做进一步的研究。

4.3 PON保护技术

PON网络在应用时,一个比较严重的可用性风险是光路的故障,包括PON接口或OLT节点的故障。为应对这方面的可用性风险,做到失效时安全,PON网络标准定义了4类保护方式:Type A、Type B、Type C、Type D,最常用的是Type B保护。以上保护类型,针对OLT上的PON口,需要进行冗余设计。一般主备端口位于不同的板卡或不同的OLT节点。针对5G接入,考虑到接入用户量比较大,之后将会越来越多地应用跨OLT的保护方案,而且由于基站距离短、密度大,所以更多使用Type B保护,即主要保护主干光纤和OLT节点。针对AWG设备,则主要是依赖于物理方面的安全保护。图4为典型的Type B类型的PON的保护方案(定义在ITU-T G.989中)。

和普通PON类似,NGPON2可



▲图4 PON网络典型的Type B保护技术

以实现同一波长对之间的保护,即在这种情况下,不管是单波长的ONU或多波长的ONU都可以达到保护的效果。这主要是通过检测某个特定波长的光信号的告警来实现的。对于多波长的ONU,如果各波长之间是负荷分担的,则可以定义多个波长组合成的一个逻辑链路,那么Type B则实现的是多波长的逻辑链路组间的保护。这种情况下可以定义为仅有一个波长出现故障即实现保护,或者只有所有的波长都出现故障了再进行业务保护。不论是TWDM PON还是PiP WDM PON,保护的流程都是类似的。ONU也可以采用不同的波长分别连接主备OLT端口。特别是在跨OLT保护的场景中,实现起来较为方便,可以减少OLT节点间的协议交互。当然,ONU可以采用波长调谐方式实现在主备波长之间的切

换,这在ONU支持可调谐或无色的情况下是非常适用的。

4.4 时钟安全技术

5G前传和中传的承载,依赖于时钟传递和IEEE 1588时间传递技术。时间或时钟方面的信号劣化或中断,对基站的工作是致命的。

在时钟传递方面,OLT需要支持多种或多路时钟源,包括外部大楼综合定时供给设备(BITS)时钟、同步以太网时钟源、全球定位系统(GPS)时钟源、IEEE 1588时钟源等。在运营过程中,根据时钟源定义的优先级,需要优选出质量最好、优先级最高的时钟源。在主用时钟信号发生质量劣化或出现丢失告警时,可以马上切换到下一优先级的时钟。如果系统可以同时同步2路以上的时钟源,则可以使备选时钟质量得到较好的保证,同时切换过

程可以做到基本无损。PON光线路的时钟需同步于OLT的系统时钟源,可保证时钟信号在PON链路上的有效传递。对于PiP类型的WDM-PON网络,则只要OLT和ONU间特定的一个波长进行同步以太网信息的传递即可。

在时间传递方面,OLT上也需支持多种或多路时间同步信号源,包括GPS时间、1秒脉冲(PPS)+日期时间(TOD)信号、1588协议端口等。精确时钟协议(PTP)模块进行时间信号的同步及时间源的优选。在运营过程中,根据时间源定义的优先级,优选质量最好、优先级最高的时间源。在主用时间信号发生质量劣化或者出现丢失告警的时候,可以马上切换到下一优先级的时间源。如果系统可以同时同步2路以上的时间源,则可以使备选时钟质量得到较好的保证,同时切换过程可以做到基本无损。时间信息在PON链路上传递,主要依靠超帧信息作为基准,而且靠OMCI信令进行定期校准。对于PiP类型的WDM-PON网络,则只要OLT和ONU间特定的一个波长进行IEEE 1588协议的传递即可。

针对时钟的锁相环以及时间的PTP模块,系统需要考虑冗余备份,以便在发现故障的情况下可以自动切换到备用的模块。主备模块可以位于专用的时钟板卡上,也可以位于业务控制板上。如果位于业务控制板上,应结合业务板卡的运行情况综合进行板卡切换。不同的模块间应考虑主备时钟及时间信号的跟踪机制,以确保在主模块故障后可

以做到无损切换。

4.5 切片安全技术

光接入网络目前已经引入切片技术,但是主要应用在 OLT 侧,以面向不同的运营商共享同一物理设备的方式为主,主要有基于板卡、基于 PON 口、基于 ONU 等方式划分切片的应用。引入 5G 承载后,场景会有革命性的变化。以垂直行业应用为基础将会是切片划分的主要场景。因此,切片将会是从基站到核心网络的端到端的隔离,即切片经由光接入网时,ONU 会按照业务切分,在 OLT 上,将会在 PON 口内部按照不同的业务颗粒度进行切分。这种场景下,切片间的安全攻击、切片内业务可用性威胁都要基于光接入网络的特性来应对。

为了达到切片隔离的效果,首先需要保证切片内的业务调度。仅靠逻辑的隔离是不够的,需要在 QoS 层面对业务进行保证。不同的切片应用在转发面上不同的 QoS 单元中,例如 PON 接入层面,需要给不同的切片业务分配不同的逻辑通道,以对业务进行专门控制。在上行方向,需要能基于 Tcont 或 Tcont 组进行切片划分,不同的 Tcont 或 Tcont 组需要能保证 QoS 的调度等级,以达到某个切片被攻击但不会扩散到其他切片的效果。当然,对于 PiP 的 WDMPON 的场景,隔离就相对容易一些,可以采用不同波长或波长组为单位进行切片划分。

另外,在管理层面,切片的安全功能需要纳入端到端切片的场景中进行统一编排,从基础设施层、业务

层到应用层都需要做到隔离。因此,管理面上的用户接入及业务控制是非常重要的。对于切片间的互相访问要进行严格地鉴权,禁止非法的跨切片互访。特别地,为防止跨切片的攻击,如果涉及不同的切片采用相同的虚拟网络的场景,应该在切片间配置防火墙进行隔离。

4.6 端到端业务可用性安全技术

端到端的业务安全是依据纵深防御的安全原则进行部署的。从 PON 接入层到切片层,再到用户业务管道,都需要进行部署。在防 DoS 攻击技术上,可以从接入节点到 ONU、OLT 再到核心网络建立起端到端追踪监测系统。通过各个设备的联动,在某个节点发现疑似 Dos 攻击的情况下,可以快速定位到攻击源头。同时,这也体现了一个分布式的网络防御架构,在接入网络复杂的情况下,可以在更靠近攻击源头的地方及早发现并遏制。完备的入侵检测系统(IDS)正是构筑在这样的分布式系统基础上的。

4.7 CDN 下沉相关安全技术

在可用性安全方面,需要考虑 CDN 设备和其他模块的隔离。在这方面,防火墙技术、防 Dos 攻击技术是非常重要的技术。来自于合法用户的仿冒核心网设备的攻击会是识别的难点,因此防火墙技术需要防止来自用户侧的攻击,也需要防止来自网络侧的攻击。根据 CDN 设备归属的业务,将 CDN 设备划入对应的切片也是必须的措施。另外,数据安全也非常重要,必须识别

关键的隐私数据,并对该数据部署加密的存储和传输,以及分析使用方面的脱敏等措施。

5 结束语

光接入网络安全技术的部署对 5G 时代的光接入网的应用能起到一定的防护作用。当然,随着 5G 技术的发展和应用的深入,相关的安全继续也需要不断演进。光接入网必将融入到 5G 网络中,和 5G 网络一起,为用户构建端到端的安全防护网。

参考文献

- [1] ITU-T. Gigabit-Capable Passive Optical Networks (GPON): Transmission Convergence Layer Specification: ITU-T G.984.3[S]. 2009
- [2] ITU-T. 10-Gigabit-Capable Passive Optical Networks (XG-PON): Transmission Convergence (TC) Layer Specification: ITU-T G.987.3[S]. 2009
- [3] ITU-T. 10-Gigabit-capable symmetric passive optical network (XGS-PON): ITU-T G.9807.1 [S]. 2016
- [4] ITU-T. 40-Gigabit-Capable Passive Optical Networks (NG-PON2): Transmission Convergence Layer Specification: ITU-T G.989.3[S]. 2015
- [5] ITU-T. T. Security Architecture for Systems Providing End-to-End Communications: ITU-T X.805 [S]. 2003
- [6] National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2[R/OL]. [2019-05-25]. <https://aisel.aisnet.org/amcis2017/TREOs/Presentations/51/>
- [7] 任建勇. 光接入网的安全技术研究[J]. 信息网络安全, 2009, (10): 61. DOI:10.3969/j.issn.1671-1122.2009.10.022
- [8] 张位. 光接入网的安全性及其增强技术研究[D]. 成都: 电子科技大学, 2017
- [9] 乔婧, 潘武, 杨静. 全光网络的安全及防范分析[J]. 光通信技术, 2008, 32(3): 10. DOI:10.3969/j.issn.1002-5561.2008.03.003

作者简介



张宏熙, 中兴通讯股份有限公司上海研发中心总工; 主要研究领域为光接入网、光线路终端系统、通信产品安全等; 先后主持及参与过多个光接入项目的研发; 已申请专利 10 余项。

5G 物理层安全技术 ——以通信促安全

5G Physical Layer Security Technology: Enhancing Security by Communication

黄开枝/HUANG Kaizhi, 金梁/JIN Liang, 钟州/ZHONG Zhou

(中国人民解放军战略支援部队信息工程大学, 河南 郑州 450002)
(PLA Strategic Support Force Information Engineering University, Zhengzhou 450002, China)



摘要: 作为无线安全的颠覆性革命技术,物理层安全技术是实现安全与通信一体化的关键手段。物理层安全技术的本质是利用无线信道特性的内生安全机制,为“一次一密”提供一种可行思路。源于通信能力的提升,无线物理层安全在 5G 高速率数据传输加密、5G 鉴权认证、增强型移动宽带(eMBB)场景信令、业务数据完整性保护和 5G 物联网场景轻量级加密等方面有着重要的应用前景。为了进一步实现物理层安全在 5G 中的应用,还提出了一种可行的物理层安全 5G 工程实现框架。

关键词: 5G 通信; 物理层安全技术; 安全与通信共生

Abstract: As a wireless security disruptive revolutionary technology, physical layer security technology is the key means to achieve security and communication integration. The built-in security mechanism based on the characteristics of wireless channel provides a feasible idea for the realization of "one secret at a time". Due to the improvement of communication capabilities, wireless physical layer security has important application prospects in 5G high-rate data transmission encryption, 5G authentication, integrity protection of enhance mobile broadband (eMBB) scenario signaling and service data, and 5G Internet of things (IoT) lightweight encryption. Specifically, in order to further realize the application of physical layer security in 5G, a feasible physical layer security 5G engineering implementation framework is proposed.

Key words: 5G communication; physical layer security; communication security integration

DOI: 10.12142/ZTETJ.201904008

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.TN.20190720.1036.002.html>

网络出版日期: 2019-07-22

收稿日期: 2019-05-26

无线通信自诞生的那一刻起,其安全问题就如同幽灵一般无处不在、无时不在,成为挥之不去的梦魇。与传统有线通信网络相比,无线通信以电磁波取代线缆作为信息传输的载体,具有在空间中

以光速进行自由、开放传播的物理特性,一定程度上模糊了通信边界的约束。这种特性既是区别于有线通信的一个标志性特点,同时也为攻击者实施恶意攻击提供了天然的条件,是引发无线安全问题的根源所在。

1948年,C. E. SHANNON 的第 1 篇文章——《通信里的数学理论》^[1]用数学刻画通信;1949年,他的第

2 篇文章——《安全里的通信理论》用信息论刻画安全^[2]。其中,他给出了完美安全的必要条件——“一次一密”,指出“完美安全需要以密钥的本身安全和传递安全为基础”,并定义了完美加密模型,提出达到完美安全需要实现一次一密,要满足以下 3 个条件:(1)合法通信双方总能获得一致的密钥,且该密钥是随机、不可预测、不可重现的;(2)密

基金项目: 国家自然科学基金项目 (No.61501516, 61701538, 61871404, 61801435, 61601514)、国家科技重大专项“新一代宽带无线移动通信网”(2018ZX03002002)

钥的长度不小于需要加密信息的长度,即密钥的生成速率不小于信息速率;(3)生成的密钥具有最大熵分布。一次一密是理论上的完美加密方法,同时也是工程上最为轻量级的加密算法,可以直接利用密钥与明文进行模2加生成密文^[3]。

现代密码学通过密码机算法的私密性和初始分发密钥的私密性,利用计算复杂度,保证密码流的安全性,是逼近 C. E. SHANNON 完美安全的一种尝试。例如,流密码加密技术^[4],先由种子密钥生成一个密钥流。然后利用加密算法把明文流和密钥流进行加密,产生密文流,如图1所示。由于每一个明文都对应一个随机的加密密钥,所以流密码在绝对理想的条件下应该是一种无条件安全的一次一密密码。但是,绝对安全的私密信道在无线通信工程实现上是不存在的,因此密码学从根本上仍是逼近 C. E. SHANNON 完美安全的一种妥协,随着 KASUMI^[5]、高级加密标准(AES)128^[6]、AES 256^[7]以及信息摘要(MD)5^[8]等数据加密和完整性保护算法被破解,SS7 信令漏洞被利用等一系列安全问题的披露,暴露

出依靠补丁式的安全演进策略所建立的被动防御体系具有脆弱性。量子计算机的提出以及计算能力的不断提高,基于计算理论的安全手段将会面临更大的挑战。

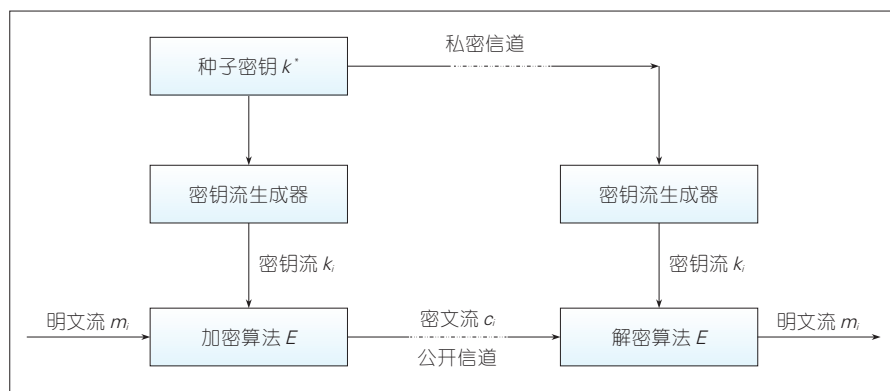
尽管 C. E. SHANNON 信息安全理论的私密信道物理上是不存在的;但是从实现角度出发,其涵义可以进一步理解为通信双方之间存在一种可观侧的、具有封闭私密特性、时变特性的随机源。因此,密钥的传递在工程中可以转化为基于共同随机源的密钥生成。

量子密钥分发就是 C. E. SHANNON 信息安全理论的一种实现方法。量子密钥分发利用量子的纠缠态分发密钥^[9],通信的双方分别持有纠缠的量子,而量子状态能够创建某种联系,使得它们无论距离多远依然能随着对方的改变而改变。通过随机改变量子的状态,通信双方通过对量子状态的测量产生并分享一个随机的密钥。另外,基于量子的测不准原理或者不可克隆特性,任意一个未知的量子态进行完全相同的复制过程是不可实现的。因为复制的前提是测量,而测量一般会改变该量子的状态,并且

第三方的存在(以及他截获的数量)能被检测到,这保证了通信双方之间密钥分发的私密性。量子密钥分发,利用量子的纠缠态和测不准特性,在通信双方之间等效实现了通信双方私密的密钥信道,理论上提供了一次一密的可能性。目前量子通信技术已经发展得比较成熟,但它的现实应用并不广泛,这主要取决于2个因素:成本和需求^[10]。量子通信对单光子的制备要求高,应用成本高,只能应用到军队、银行、政府机关等保密性需求较高的特殊领域。而且,单光子的制备存在诸多困难,不仅严重降低了量子密码通信通道的传输效率,而且还增大了量子密码通信通道传递量子密码编码的误码率。

从密码学到量子安全手段,与无线通信均是割裂开的。安全的定位一直是服务于通信,依托于通信,跟随于通信,不能有效地解决无线通信安全问题。因此,亟待革命性的、颠覆性的理念和技术从无线通信根源上解决安全问题。无线物理层安全,利用无线信道的多样性和时变性以及合法通信双方信道的唯一性和互易性,从无线信号传播的客观规律入手,挖掘无线信道的内生安全元素。这些安全元素天然寄生于通信流程与信号处理技术中,可以和新空口技术同步演进、融合发展,促进安全与通信一体化。

本文中,我们重新审视了无线物理层安全的本质,即物理层安全利用无线信道内生安全增量,是无线通信与生俱来的安全手段。从安全与通信的辩证关系入手,阐述了



▲图1 流密码加解密模型

物理层安全引领通信促进安全、通信与安全共生的重要意义。紧接着,针对5G高速率数据传输加密、5G鉴权认证、增强型移动宽带(eMBB)场景信令、业务数据完整性保护和5G物联网场景轻量级加密等方面存在的问题,提出了无线物理层安全解决方案。最后,从5G应用角度出发,进一步设计了物理层安全5G工程实现框架,将物理层安全作为一种可选服务模块,以独立功能模块的方式嵌入到无线接入网(RAN)中,实现分等级的多层多域安全功能。

1 物理层安全——无线通信与生俱来的安全手段

无线通信亟需与其传输特性、传播机理相契合的安全防护手段。其实,在无线通信原始的内涵中,就带着安全的设计理念与痕迹,尤以预均衡和波束形成技术最为典型。预均衡^[11]作为信号通过信道之前的滤波处理,目的是让信道透明掉,在特定的合法接收位置上纠正信道对信号的恶化。因此,预均衡对于其他位置的用户来说,相当于乘性噪声。这意味着只有合法接收端能接收到最好的信号质量。这样一来,会导频资源分配越多信道估计越准,同时预均衡就越彻底,合法用户越安全。波束形成^[12]是一种经典的多天线技术,通过调整发送天线权重系数,使天线主瓣对准合法接收用户,以减少信号泄露给其他用户,也减小被窃听的概率。只要天线够多,孔径够大,主瓣够窄,就能实现点聚焦传输。从安全角度来看,只

要主瓣足够窄,点聚焦足够好,就能实现特定位置的安全传输,任何其他位置均接收不到信号。这2种技术在实现通信的同时也提高了系统的安全性能。为了获得足够好的安全效果,往往需要更精确的信道估计。这导频资源分配越多信道估计越准,同时主瓣越窄,从而安全效果就越好。

无线物理层安全^[13](PLS),来源于但同时又高于无线通信本身的安全理念。它从无线信号传播特点入手,利用无线信道的不可测量、不可复制的内生安全属性,从物理层探索无线通信内生安全机制,促进安全与通信一体化。物理层安全技术的2大分支为:物理层安全传输技术和物理层密钥生成技术。物理层安全传输技术的实质是利用无线信道的差异设计与位置强关联的信号传输和处理机制,使得只有在期望位置上的用户才能正确解调信号,而在其他位置上的信号是置乱加扰、污损残缺、不可恢复的;物理层密钥生成技术的实质是利用通信双方私有的信道特征,提取无线信道“指纹”特征,提供实时生成、无需分发的快速密钥更新手段,逼近一次一密的完美加密效果。物理层安全技术本质上利用无线信道的物理特性实现基于用户位置的安全,不同位置的用户对合法信道不可测量、不可复制,所依赖的科学规律与量子密钥分发利用量子特性具有异曲同工之处,而其充分利用了无线信道的内生安全属性,与无线通信是一体的,因此称为“无线通信中的量子密码通信”。而且,物理层安全技

术与无线信道的“绑定”关系,使得物理层安全技术在无线通信中的应用具有得天独厚的优势。

物理层安全能够挖掘无线信道的内生安全属性,并利用无线信道本身的特性,实现C. E. SHANNON安全理论中的私密信道,是该安全理论的发展,它为实现安全模型提供了一种可行思路。从物理层安全角度出发,无线信道的内生安全属性将安全与通信绑定在一起,安全实现的流程兼容于、内嵌于、衍生于通信之中。因此,物理层安全技术的引入,使得通信与安全不再割裂开来,有通信就有安全,两者是共生的关系。从安全与通信共生的思路出发,物理层安全能力的提升不需要像密码机制一样提高计算复杂度。任何有助于提高通信容量的手段,都能够提升安全性能。无线通信安全问题转化为通信资源分配和发掘问题,即安全能力的增强来自于通信能力的提升和通信资源的有效利用。这一结论也表明:物理层安全机制寄生于通信中,可以和下一代无线通信新空口技术同步演进、融合发展,实现安全与通信一体化发展的愿景。

2 PLS在5G中的应用前景

5G、B5G以及未来的6G通信,将会采用大规模天线、高频段、大带宽等空口技术,极大地提高信道空间分辨率,数百倍地提高信道信息量,而且随着频段提升、波长缩短,绝对距离的信道差异性更剧烈。这使得无线内生安全元素更丰富、提取更便利,易于实现并且增强具有

无线内生安全属性的物理层安全技术。因此,在5G通信关键性能指标(KPI)呈数量级提升的背景下,物理层安全技术提供一种不同于计算复杂度安全的、负荷灵活调控的、适用于多场景的、与通信共生的新型安全机制。

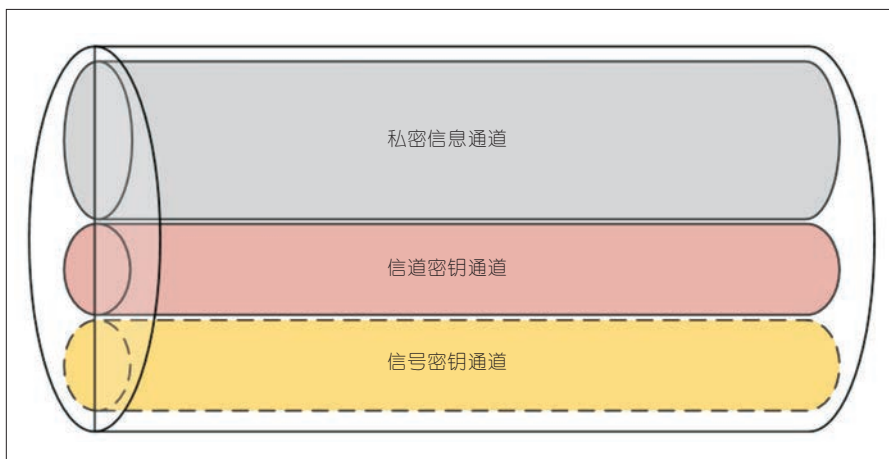
针对信号开放性带来的安全问题,物理层安全利用无线信道特征差异,通过信号处理方法实现基于用户位置的安全。基于无线信道的内在属性实现安全,物理层安全机制将通信与安全绑定在一起,在工程实现上和5G新空口技术的较好兼容,并通过叠加信号处理技术实现空口安全增强。物理层安全应该成为5G安全中具有代差效应的核心技术,与传统安全机制相结合能够进一步拓展安全维度,在高速率数据传输、鉴权认证、信令业务数据完整性保护和物联网场景轻量级加密等方面为5G安全提供特色增量。

2.1 物理层密钥能够解决 5G

高速率数据传输的加密难题

传统密码算法中,复杂的密钥生成与分发流程难以保障5G的千兆量级通信速率的安全防护,物理层密钥生成技术的密钥生成速率上限为无线信道容量,这无疑为5G高速率数据传输的加密提供了革命性思路。在5G通信中,通过合理分配信息通信资源和密钥生成资源,保证密钥容量大于等于私密信息容量,能够实现一次一密的绝对安全愿景。

如图2所示,为了保证5G高速率数据传输的加密,在发送私密信



▲图2 信道+随机信号的密钥生成

息的同时,发送随机信号、合法通信双方将随机信号和信道本身作为共享随机源,并从中提取密钥。如果满足信道密钥+信号密钥容量大于等于私密信息容量,就能够实现一次一密。相比单一信道密钥,信号密钥通道的增加,就是通信资源的再分配,能够有效地解决高数据速率传输情况下信道密钥源熵不足的相关问题。

接收信号的随机性来自于发送信号与信道的叠加,这使得接收信号熵包含信道熵和信号熵,而且其中发送信号是自主可控的,这样一来就可以通过提高随机源本身的随机性提高密钥容量,可以有效地解决高数据传输速率的密钥生成速率需求。在密钥生成过程中,接收方直接从接收信号中量化提取密钥,而将信道估计工作放在发送方。这是一种非对称的密钥生成方案,便于实现接收方的轻量级密钥生成。信道+随机信号的密钥生成方案,本质上是通过通信资源的合理分配,将整个无线通信“管道”资源分配给私密信息通道、信道密钥通道

和信号密钥通道,满足信道密钥+信号密钥容量大于等于私密信息容量,为保证5G高速率数据传输加密提供了解决方案^[14]。

2.2 物理层安全能够拓展认证维度,增强5G鉴权认证

针对以无线信号为载体对信息内容篡改、假冒,以及以转发和重放等形式的无线接入攻击等,传统的2G、3G和4G鉴权认证方案本质上是对基于身份索引的密钥打上包含用户身份信息的标签。一旦根密钥泄露,认证参数将失效,通过窃听认证的过程即可推导出后续保护密钥,威胁网络安全。

针对上述问题,物理层安全认证手段利用动态、时变的无线信道元素拓展认证维度^[15],将对数据和信令的认证转移到对无线信道的认证。通过终端侧融合身份密钥K和传统认证参数rand,映射出基站进行信道参数估计的初始反向训练序列,基站侧结合安全传输辅助的密钥生成方案可以生成与终端一致的密钥K_H,并根据 $f(K, K_H, rand)$

更新反向训练序列。身份密钥K和传统认证参数rand保证了初始反向训练序列的私密性,K_H保证了反向训练序列在通信过程中可以不断更新。这一过程既保证参与密钥生成的双方均为合法用户,又保证了信道测量过程的安全性。K_H的生成过程本质上是利用信道特征对信道加盖“位置戳”,实现对合法通信信道的认证。

上述方法将物理层安全与传统安全融合,形成双加固的新型安全机制。该方法能提取与位置强耦合的无线信道特征作为新的内生认证元素,在信号层面增加对承载身份的信号认证,通过与现有认证机制结合,增加认证维度,构建5G新型内生安全防御体系,可以检测、发现,并能有效抵御来自于异常位置的无线攻击。

2.3 物理层密钥能够解决eMBB场景信令、业务数据完整性保护的问题

与认证相似,传统的信令、数据完整性保护方案,本质上是对信令和数据打上包含用户身份信息的标签。随着移动通信数据速率的提高,并受制于速率与计算复杂度之间的矛盾,目前移动通信系统中针对业务数据的完整性保护尚未有合适的解决方案。毫无疑问,eMBB通信场景高速率业务数据亟待有效的、轻量级的完整性保护。

针对上述问题,基于无线信道的信令、数据完整性保护方案在基站侧结合安全传输辅助的密钥生成方案可以生成与终端一致的无线信

道密钥K_H。将无线信道密钥K_H与信令、业务数据按比特或按块对应模2加,并利用循环冗余校验(CRC)纠正错误比特,最终生成介质访问控制(MAC)标签。基于无线信道的信令、数据完整性保护方案的实质是利用信道特征为业务数据加盖位置戳。

基于无线信道唯一性、复杂性和时变性的密钥生成,等效实现了C. E. SHANNON信息安全理论中密钥在私密信道的传递,而且密钥速率与信息传输速率的可适配,保证了只要利用密钥K_H与业务数据按比特或按块模2加就可以实现一次一密绝对安全,为实现eMBB通信场景高速率业务数据完整性保护提供了轻量级解决方案。

2.4 物理层安全能够解决物联网场景轻量级加密的问题

在海量机器类通信(mMTC)和高可靠低时延通信(uRLLC)2大物联网典型场景中,节点不仅受到计算资源、体积、功耗的约束,还将不断动态加入或退出网络。因此,节点侧需要针对小数据设计高效和轻量级的安全机制,对信令与数据进行完整性、机密性和隐私保护;网络侧面对海量密钥的分发与管理问题,需要降低安全信令开销与时延。仅依靠传统密码算法和密码管理的优化设计,难以实现节点侧轻量级的安全通信机制以及海量通信终端和节点的密钥分发与管理。对现有密码算法进行适应性的裁剪,必然以牺牲安全性能为代价。

在基于无线信道特性的物理层

密钥生成技术中,无线通信双方可以随时通过信道估计安全地获取时变的随机密钥,由此解决密钥分发问题。物联网中数据速率低、数据量小,物理层生成的密钥可直接对信令和敏感数据等低速率敏感信息通过模2加实现一次一密的轻量级绝对安全。针对物联网场景下的物理层密钥生成技术受限于准静态信道密钥生成速率低的问题,可以通过基于中继辅助的密钥生成方案,引入中继信道作为额外的密钥源,以提高密钥生成速率。此外,还可以利用物联网中节点之间多条传输链路的优势,通过提取多条传输路径上的随机信道的信息,来增加合法通信双方用于生成密钥的密钥源的熵。

2.5 物理层安全的5G工程实现框架

物理层安全应用于RAN的愿景为:天然寄生于通信流程和信号处理技术中,实现安全与通信的融合和一体化设计,将安全作为服务推送给不同安全需求的垂直行业 and 用户。因此,物理层安全技术最佳的实现方式应该是作为一种可选服务模块。接入网利用物理层安全技术研制专用高等级安全功能模块,通过设备内部接口嵌入基站和终端中,实现安全与通信的融合和一体化设计以及分等级的多层多域安全功能。

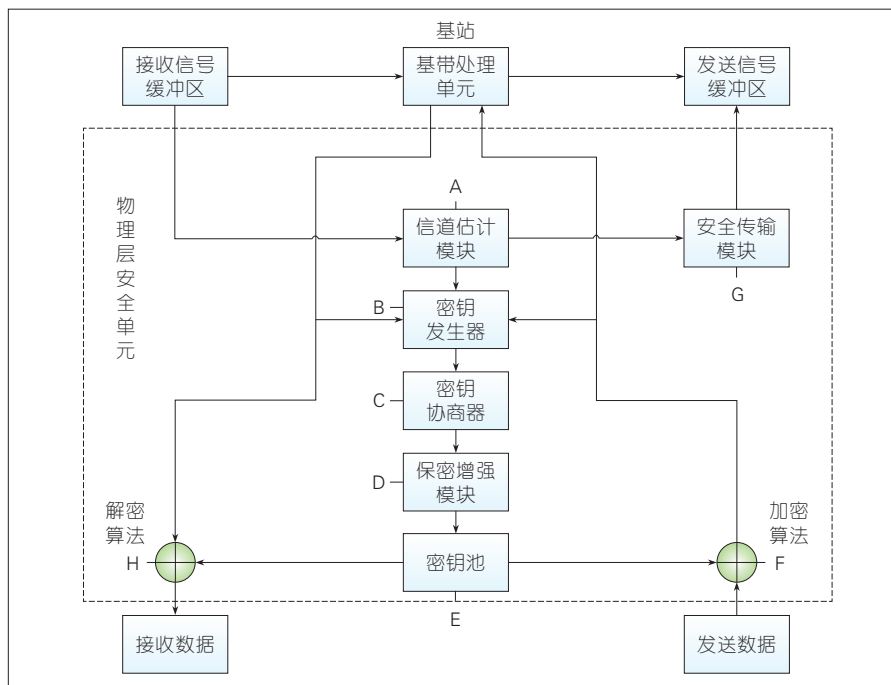
集中化处理无线接入网(C-RAN)是一种利用集中式基带处理单元(BBU)基带池和分布式射频拉远单元(RRU)结合的部署方式。

该部署方式结合开放、统一的平台,可以实现灵活的多标准支持和未来先进技术扩展的5G网络架构关键技术。中国移动针对C-RAN定义了下一代前传网络接口(NGFI)以及BBU和RRU的基带/射频划分方案^[16]。基带池内的BBU协作化和基站的软化方案,使得无线处理资源云化在C-RAN里,基带计算资源不再单独属于某个BBU,而是属于整个资源池。

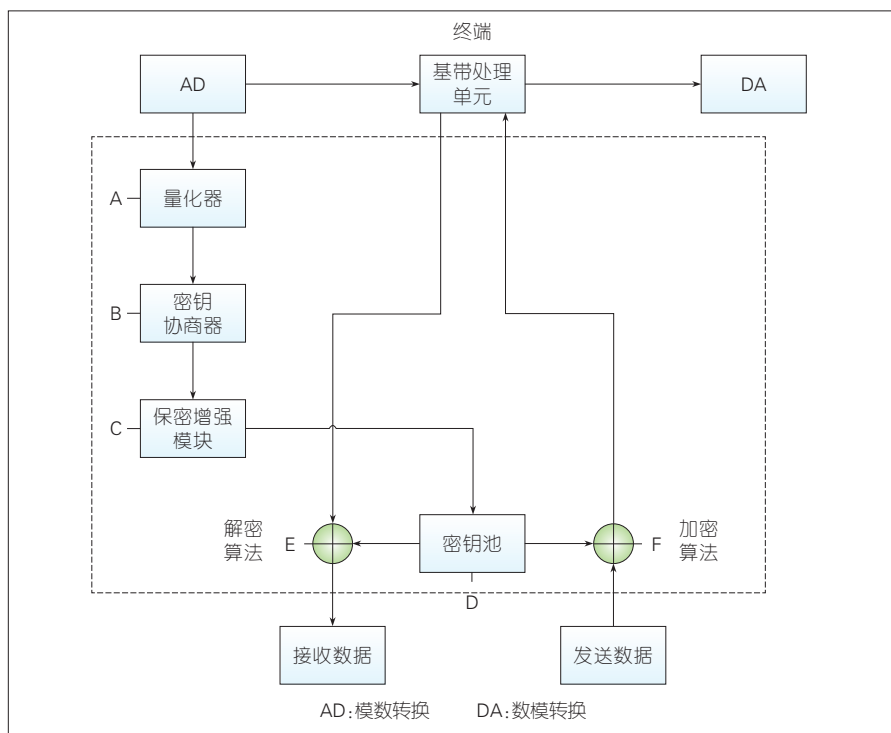
如图3所示,在现有C-RAN架构的基带处理池中增加物理层安全单元(PLSU),实现物理层密钥生成与安全传输,使物理层安全技术能够作为一个功能模块嵌入接入云架构之中。

其中,基站侧的PLSU串接在收发数据与BBU之间,同时PLSU接入接收信号缓冲区与发送信号缓冲区。利用PLSU中的信道估计模块从接收信号缓冲区中获取终端发送的导频信号估计当前信道,并将信道估计结果送入密钥发生器与安全传输模块。安全传输模块利用信道估计结果生成安全传输辅助信号并送入发送信号缓冲区。密钥发生器将物理层生成的密钥序列经协商和保密增强后送入密钥池,用于发送和接收数据的加密和解密。发送数据时,密钥池中的密钥流与待加密数据运算生成密文,送入BBU中完成后续信号处理,并可用于完成下一次密钥生成。

相应地,如图4所示,终端侧接收时提取数模转换(AD)输出信号进行量化,生成私密序列经协商和保密增强后送入密钥池完成对数据



▲图3 面向集中化处理无线接入网的物理层安全单元在基站侧的实现框图



▲图4 物理层安全单元在终端侧的实现框图

的解密;发送数据时,密钥池中的密钥流与待加密数据运算生成密文,送入基带处理模块中完成后续的相关处理。

关处理。

在基于上述架构的物理层密钥生成方法中,终端侧物理层安全单

元串接在基带处理器与信源之间,利用接收信号提取随机序列,并与基站的物理层安全单元相配合,使两端生成的随机序列保持一致。物理层安全单元生成的共享随机序列,可用于通信过程中的物理层认证及信号加扰,实现高性能空口安全增强目标。终端侧实现的硬件资源小,与现有通信系统耦合程度较低,无须对现有通信架构进行较大更改,仅增加独立功能模块就能提升整个系统的安全性。从接收信号提取物理层密钥的流程与通信流程相一致,能促进安全与通信一体化。另外,因为采用非对称的实现方式,将主要负荷集中在基站端,降低了终端的开销,便于实现终端的轻量级安全。

3 结束语

本文中,我们阐述了物理层安全技术的本质,即利用无线信道特性的内生安全机制为实现 C. E. SHANNON 安全模型一次一密提供了一种可行思路。针对 5G 高速率数据传输加密、5G 鉴权认证、eMBB 场景信令、业务数据完整性保护和 5G 物联网场景轻量级加密等方面存在的问题,提出了无线物理层安全解决方案。文章中,我们进一步设计了可行的物理层安全 5G 工程实现框架,将物理层安全作为一种

可选服务模块,以插件形式嵌入基站/终端,为物理层安全技术 在 5G 中的应用落地提供指导。

参考文献

- [1] SHANNON C E. A Mathematical Theory of Communication[J]. Bell System Technical Journal, 1948, 27(3): 379–423. DOI:10.1002/j.1538-7305.1948.tb00917.x
- [2] SHANNON C E. Communication Theory of Secrecy Systems[J]. Bell System Technical Journal, 1949, 28(4): 656–715. DOI:10.1002/j.1538-7305.1949.tb00928.x
- [3] SCHNEIER B. Applied Cryptography: Protocols, Algorithms, and Source Code in C [M]. USA: John Wiley & Sons, 2007
- [4] SINSON D R. Cryptography: Theory and Practice[M]. British: Chapman and Hall/CRC, 2005
- [5] DUNKELMAN O, KELLER N and SHAMIR A. A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony [J]. Journal of Cryptology, 2013, 27(4): 824–849. DOI:10.1007/978-3-642-14623-7_21
- [6] GUERON S. Intel® Advanced Encryption Standard (AES) New Instructions Set [EB/OL]. (2012-08-02) [2019-05-25]. <https://software.intel.com/en-us/node/165683>
- [7] DUNKELMAN O, KELLER N, SHAMIR A. Improved Single-Key Attacks on 8-Round AES-192 and AES-256[J]. Journal of Cryptology, 2010, 28(3): 158–176. DOI: 10.1007/500145-013-9159-4
- [8] WANG X, YU H. How to Break MD5 and Other Hash Functions[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Germany: Springer, 2005: 19–35. DOI: 10.1007/11426639_2
- [9] EKERT A K. Quantum Cryptography based on Bell's Theorem[J]. Physical Review Letters, 1991, 67(6): 661. DOI: 10.1103/PhysRevLett.67.661
- [10] KOLLMITZER C, PIVK M. Applied Quantum Cryptography[M]. Germany: Springer, 2010
- [11] CLARK A P. Equalizers for Digital Modems [M]. British: Pentech, 1985
- [12] LITVA J, LO T K. Digital Beamforming in Wireless Communications[M]. USA: Artech House, 1996
- [13] BLOCH M, BARROS J. Physical-Layer Security: From Information Theory to Security Engineering[M]. British: Cambridge University Press, 2011
- [14] 楼洋明, 金梁, 钟州, 等. 基于 MIMO 接收信号空间的密钥生成方案[J]. 中国科学: 信息科学, 2017(3): 92–103. DOI: CNKI:SUN: PZKX.0.2017-03-007

- [15] XIAO L, GREENSTEIN L, MANDAYAM N. Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication[C]//IEEE International Conference on Communications. USA: IEEE, 2007: 4646–4651. DOI: 10.1109/ICC.2007.767
- [16] 无线接入子系统前端传输接口演进的技术研究[R/OL]. [2019-06-20]. <http://www.doc88.com/p-1595045775755.html>

作者简介



黄开枝, 中国人民解放军战略支援部队信息工程大学教授、博士生导师, “网络通信与交换技术”国家科技进步奖创新团队核心成员, 河南省“无线移动通信创新型科技团队”主要带头人; 主要研究方向为无线移动通信网络和信息安全; 主持或参与国家“863”计划、国家科技重大专项、国家自然科学基金等各类课题 10 余项; 获国家科技进步二等奖 1 项, 省部级科技进步一等奖、二等奖各 1 项; 发表学术论文 150 余篇, 申请专利 30 余项, 出版译著 5 本。



金梁, 中国人民解放军战略支援部队信息工程大学教授、博士生导师, 百万人才工程国家级人选, 享受政府特殊津贴; 主要研究方向为移动通信网络和信息安全; 主持国家“863”计划、国家科技重大专项、国家重点研发计划、国家自然科学基金等课题多项; 获国家科技进步一等奖 1 项、国家教学成果一等奖 1 项、国家科技进步奖创新团队奖 1 项, 并曾获中国青年科技奖、中国科协“求是奖”; 发表学术论文 150 余篇, 申请发明专利 30 余项。



钟州, 中国人民解放军战略支援部队信息工程大学讲师; 主要研究方向为移动通信网络和信息安全; 已发表学术论文 10 余篇。

基于 5G 的垂直行业安全 新特征与对策

New Characteristics and Countermeasures for Vertical Industries Security in 5G

汤凯/TANG Kai

(中兴通讯股份有限公司, 广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)



摘要: 分析了 5G 的新技术给网络安全性带来的新挑战。针对传统安全产品和技术,提出了优化与增强的要求。同时还从环境、业务、资产和运营 4 个角度,总结了垂直行业应用的各种新特征,并分析了这些特征给安全性带来的挑战与影响,同时提出了一些针对性的缓解措施。

关键词: 5G; 垂直行业; 安全; 物联网; 网络切片; 移动边缘计算; 运营技术

Abstract: The new challenges brought by the new technologies of 5G on network security are analyzed, and the optimization and enhancement requirements for traditional security products and technologies are proposed in this paper. Various new application characteristics of vertical industry applications are extracted from four perspectives of environment, service, assets and operations. The challenges and effects of these characteristics on security are analyzed, and some targeted mitigation measures are put forward.

Key words: 5G; vertical industries; security; internet of things; network slice; mobile edge computing; operation technology

DOI: 10.12142/ZTETJ.201904009

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1603.004.html>

网络出版日期: 2019-07-09

收稿日期: 2019-05-28

1 安全是产业互联网的基石

如果说在消费互联网时代,“控制住了网络就控制住了世界”只是一句口号的话,那么在 5G 时代,这句话即将变成现实。随着越来越多的设备、基础设施、行业应用与数字化资产承载于 5G 网络之上,网络安全逐步上升为事关国家和社会稳定发展的重大命题。

根据越来越频繁的安全事件可以看出,针对物联网、电网、交通基础设施等非传统价值目标的攻击比

例越来越高,攻击的门槛越来越低,手段也越来越丰富。随着 5G 网络大规模部署,无论是从黑色产业链角度,还是出于其他政治、军事、经济、社会等目的,5G 所连接的重要基础设施,对攻击者的吸引力都会与日俱增。未来 20 年,通过网络对各类基础设施进行破坏、劫持、勒索的网络恐怖主义将会成为各国政府、各行业监管机构、基础设施提供者、企业运营者以及广大公众需要经常直面的问题。全社会需要从政策、法规、组织、技术等各个层面提

前做出应对,设立多条安全防线,构建完善的网络空间安全治理框架,为未来产业互联网的可持续发展提供稳定的基石。

2 传统威胁叠加新挑战

在 5G 阶段,大量现有的方法论、信息技术(IT)将会继续在垂直行业中使用,传统上用于攻击的漏洞、工具与手段都能够直接作用于垂直行业应用并产生威胁。由于被攻击的目标往往还会连接物理世界的人、资产和关键基础设施,会使得

风险后果更为严重,处置起来也更为复杂。由于垂直行业应用往往会具有多种不同的特征,相互之间关联交织,从而导致威胁与攻击显得更加隐蔽和复杂。5G 面向网络架构的定制化,引入了软件定义网络(SDN)/网络功能虚拟化(NFV)等,这种基础设施层面的灵活性与动态性也进一步加剧了安全挑战。因此,总体上基于 5G 的垂直行业应用安全呈现出攻击面扩大化、攻击方式泛在化、安全边界模糊等趋势。

传统的安全机制与防御产品、服务与技术,例如认证/加密算法、密钥管理系统、防火墙、入侵检测系统(IDS)/入侵防御系统(IPS)、各种面向主机以及云基础设施的漏洞管理以及安全加固手段,需要针对性地进行优化、增强,以适应 5G 时代垂直行业应用的新特征。必要时,还需要引进一些特殊的安全技术,来填补传统安全盲点。

3 新特征下的安全对策

区别于传统的消费互联网的商业模式与业务架构的单一性,产业互联网由于面向场景的多元化,具备了很多独特的新特征。我们对这些新特征进行了如下的更细维度的系统化归纳与分类。每一类新特征,都可能会对垂直行业应用安全带来消极影响。

- 加:增加新的威胁与风险
 - 减:降低安全架构可选择性
 - 乘:叠加、放大传统的威胁与风险
 - 除:影响安全架构实施效果
- 另外,还有一些新特征会对垂

直行行业应用安全带来积极影响。通过降低成本与复杂性,提升可定制性,这些特征可以从相反的方向对消极特征带来的影响起到一定的抵消作用。以上各种影响都需要在制定垂直行业安全解决方案时,基于威胁模型进行统筹分析,以被保护的垂直行业资产为中心,依据威胁的重要性以及风险后果进行技术方案权衡与定制。

按照对应的能力层次,本文中,我们将各种垂直行业应用新特征划分为 4 种类型:环境型特征、业务型特征、资产型特征以及运营型特征。

3.1 环境型特征

(1) 低功耗:大规模物联网(IoT)的要求。

很多负责传感、环境监测控制的设备,需要运行在无法进行持续外部供电的环境当中。由于体积或成本等因素的限制,这些设备自身很难储备太大的电能,需要设法降低功耗,以获得更长的工作时间。目前,产业界对于此类设备连续工作时间的初步共识是 10 Y 左右。设备的功耗来自于各个方面,优化也需要针对不同的组件分别展开,例如使用更高集成度的处理硬件、轻量级的操作系统与协议,采用窄带物联网(NB-IoT)、远距离无线(LoRa)等低功耗广域网(LPWAN)技术。从安全角度看,在此类终端中加载复杂的安全逻辑是比较困难的,因此需要考虑使用其他的辅助手段来提供增强型保护,例如在汇聚/网关设备上加载安全逻辑,对来往终端的行为与流量进行监测控

制、分析与过滤;使用具有高度网络隔离性的接入措施等。通过对认证协议进行优化,尽量减少网络交互的次数。对于必须使用加密的场景,需要在安全性与功耗之间进行适当的权衡,选用合适的加密算法,并根据业务特点对其进行轻量化改造,例如减少密钥长度、降低加密计算轮次、减少密钥更新次数等。

低功耗的微控制单元(MCU)中很少配置硬件随机数发生器,这会极大地影响加密算法的安全性,因此需要研究软硬件结合的方法来提供足够的随机性。

(2) 无人化:缺乏可视度。

诸如 IoT 设备、网关之类的边缘基础设施经常部署在远离人群与管理中心的环境中,存在大量管理盲点,难以对其进行现场维护与管理。这类设备无论是被攻击还是被劫持作为攻击发起者,往往很难立即发觉并进行快速处置。需要考虑通过 5G 网络对各种基础设施与设备进行资产发现与管理,以提高对于设备的可视度,并对软件无线更新(OTA)/固件无线更新(FOTA)提供安全通道。在资源允许的情况下,可以在设备版本中内置相应的安全代理软件,对设备运行的安全状态进行充分。

(3) 开放性:信任边界退行至硬件内部。

大量物联网设备将会暴露在公开的环境中,这使得安全威胁从原先多发生在网络边界开始向不设防的硬件层次转移,攻击者也更容易针对设备发起拒绝服务攻击(DoS)攻击、侧信道攻击等。

从终端整体看,要考虑防拆型设计。该设计将使任何物理性的侵入都会破坏掉设备的关键部件,从而减少硬件上的侵入对设备的机密性与完整性带来的威胁。防拆型设计适用于用户对于设备本身的物理价值不太敏感的场景。

从硬件接口或电路的角度考虑,要注意防调试设计。该设计能够使得入侵者获得设备硬件的控制权后,无法从软件上对设备的操作系统、服务、应用编程接口(API)和业务软件进行窃听、调试与修改,或难以获取设备硬件或者软件的最高权限。

从操作系统的角度考虑,除了基本的安全加固手段之外,还可以参考可信计算工作组(TCG),并基于可信平台模块(TPM)芯片提供根信任并构建完整的信任链,来保护设备上系统的机密性与完整性,防护恶意代码注入。还可以对代码进行混淆或加壳处理,防止攻击者进行反向工程,对软件知识产权产生威胁。对于终端能力受限的场景,可以只引入部分加固能力,例如 Secure Boot、镜像签名等。

大多数一般性场景往往只需要保护关键信息,例如安全密钥、重要配置参数等。此时可以引入 TEE 可信执行环境,以较低成本方式实现对于关键信息与能力的保护。

(4)异构性:系统之系统。

面对多样化的环境,物联网系统会根据自身需要综合采用射频标识(RFID)、Zigbee、蓝牙、WiFi、5G 等多样化的设备类型与接入方式,增加了攻击向量。同样的防御手

段,必须要在不同的硬件、操作系统、协议栈上部署,加大了安全成本与防御难度。此时,点防御的概念已难以奏效,面防御以及立体化防御成为首选,各种无代理安全技术将在其中发挥更大的作用。通过对设备、流量等扫描分析,能够从设备外部及时发现与处置各种威胁。

边缘计算(MEC)^[1]由于更为靠近用户的资产,可以为物联网提供第一道安全屏障。通过在其上部署相应的物联网网关或平台,在对业务流量进行收敛与处理的同时,对物联网终端及其连接的资产进行隔离保护,以降低资产的暴露性,减少网络攻击面。

(5)灵活性:动态基础设施。

网络切片技术是 5G 网络中一种在共享基础设施上提供私网服务能力的技术。关于连接、服务和数据在网络切片中被隔离保护的效果,需要有不低于传统企业专网的可靠性与安全性,用户才敢于将企业专网迁移到 5G 基础设施之中。

5G 网络切片引入的 NFV/SDN 技术,在带来灵活性的同时,也带来租户间的东西向威胁以及安全边界的不确定性。随着 NFV 的自动编排与虚拟机位置的动态变化,基础设施的架构也需要通过 SDN 进行相应的动态调整。因此,一方面,基础设施内部需要通过微分段等零信任网络技术,构建更加立体化、细粒度的安全防御体系;另一方面,安全能力需要跟随计算能力进行动态编排、定制与调整,以减少基础设施的灵活性与弹性带来的威胁。

(6)区域性:降低了移动性的复

杂度。

由于需要连接到实际的物理资产,很多行业应用一般会具有较强的固定性与区域性,这也给安全解决方案带来了很多的便利性,例如无需考虑复杂的漫游性场景与环境的多变性与复杂性。

3.2 业务型特征

(1)大连接:海量设备以及海量数据。

在智慧城市环境监测控制、资源计量等场景,为了追求高精度的管理,连接密度往往会非常高。大连接已经成为 5G 的典型特征之一,这直接导致了安全威胁从攻击源与攻击目标 2 个方向上的规模快速变大,并在空间上呈现广域化与分散化的特征。

一些特殊的问题需要进行一些针对性的设计来解决,例如信令风暴、海量设备密钥管理等。可以考虑引入聚合认证、层次化标识与密钥生成技术等。

传统的防御手段主要面向移动互联网,相应的产品设计参数也是参照人的行为模式以及业务模型而配置。物联网带来的大连接、小数据包会给基础设施层面带来全新的流量模型,相应的产品设计、参数配置也需要进行调整。例如,防火墙类的设备的连接数以及小报文处理能力,需要进行优化调整。防御设备上对于过滤策略的配置,也需要针对海量设备的特点,进行更加精准的匹配,例如通过设备身份信息。

(2)低时延:实时性体验。

车联网、互动娱乐、远程医疗、

工业互联网等应用,对于通信的低时延、实时性、抗抖动性有着非常高的要求。如不满足这些要求则会导致很多问题,有时会很严重,例如涉及车内/车外的人身安危的自动驾驶业务;有时则不严重,可能仅会在商业上降低用户的满意度,例如第一人称射击(FPS)类游戏等。

从安全角度考虑,除了提高设备处理能力,5G网络还通过减少层次之间、端到端之间的安全冗余的方式在安全性与低时延之间进行优化,甚至可以完全基于业务层面实现安全性,而不依赖于5G网络。

有些业务场景对接入时延比较敏感,可以简化、优化认证框架,以减少网络交互次数以及处理流程。对于加密的场景,需要对加密算法进行优化,以减少加密、解密带来的时延,减少密钥更新频率。对于基于MEC的业务,可以将认证能力下沉到边缘进行。

有些场景对接入时延并不敏感,仅对用户面或业务执行过程中的时延敏感;因此可以将时延敏感业务下沉到MEC执行,以减少到远程数据中心的数据及逻辑依赖。

(3)高可用:保证业务连续性。

高可用性一般是成本问题。对于5G网络而言,一般会分配专门的网络切片进行隔离保护。垂直行业可以根据各自业务的可靠性等级要求,订购相应等级的网络切片,获得相应安全等级的隔离保护能力。

对于工业互联网等场景,可以在企业网络与工业网络之间建立相应隔离区(DMZ)。

对于连接的可用性,在有些特

殊场景下,可以考虑引入低轨卫星等备份连接通道,保持节点网络连接的高可用性^[2]。

(4)机械性:行为基线稳定。

相比于传统消费互联网中人的行为的复杂性与不确定性,机器的行为模式相对简单,流量模型可预测。同时,由于网络切片的使用,隔离了各种不同业务特征的网络流量;因此,通过快速的学习和训练,人工智能(AI)技术可以更加准确地对垂直行业的流量与行为的异常进行检测、回溯与根因分析,为垂直行业用户提供实用化的安全分析与告警,抵御各类高级持续性威胁(APT)攻击。

另外,垂直行业关键业务的网络拓扑与业务关系相对固定。该特性结合5G的融合身份认证能力,有助于构建零信任的垂直行业网络。

3.3 资产型特征

(1)长寿命:一个不连续的生命周期。

某些物联网设备(例如低功耗类)将会长期服役,其设备生命周期超过设备制造厂家的自身存续时间。这在未来将会是较大概率事件,会给系统的长期可用性与安全性带来挑战。

由于技术的不断演进,市场会优先选择具有更低成本、更高效能的新型设备。这会导致传统型号设备的市场窗口不断缩小,其可维护性(备件供应、硬件升级、固件/软件补丁支持等)也会随着时间推进而不断降低。

对于很多行业系统而言,设备、

系统的定期维护与升级是业务健康与持续发展的必要保证。为了保证业务的连续性,降低对运营层面的冲击,垂直行业应用在设计系统方案时需要考虑以下问题:

- 物理资产与设备解耦(通过标准接口连接);
- 多设备供应商策略,以提升设备可替代性;
- 硬件标准化,优先采用通用性强的硬件设计;
- 软件开发与硬件独立(尽量采用开源平台与技术);
- 系统可平滑升级能力(支持新、旧设备的共存与过渡);
- 不依赖于制造厂商的补丁更新与漏洞维护;
- 不依赖于制造厂商的安全密钥与证书管理;
- 设备终身问责机制。

另外,大量的、未经过较好的安全设计的传统物联网终端仍将长期运行,并有平滑迁移到5G基础设施中的需求。安全方案需要对这一类终端建立隔离区,并设计专门的保护措施,避免降级攻击。

(2)关键性:攻击性价比提升。

针对垂直行业的攻击,更多的将会有针对性地选择高价值的目标进行。传统的黑色产业主要利用一些通用的技术漏洞,而5G时代将会面向特定的目标进行针对性地漏洞挖掘与渗透,从而进行精准式攻击。从性价比的角度考虑,越是重要的基础设施和价值目标,越是能吸引APT攻击。

安全架构师需要像罪犯而非黑客与工程师一样来思考,他们不但

要理解业务,还需要理解业务的价值、关键处理逻辑、重要数据位置。另外,垂直行业的安全不再仅仅是 IT 系统的职责,更需要 IT 与运营技术(OT)在组织架构层面、业务流程层面结合,协同完成维护职责。

5G 网络切片提供了一种多等级的网络隔离机制,因此我们可以基于各种专用资源构建关键业务网络切片。例如,垂直行业可以与运营商共建 5G 基站并提供排他性的网络接入,基于 MEC 直接提供边缘接入与认证功能,同时将流量本地转发至垂直行业自有的基础设施,而不经外部的公共网络。基础设施可以更多地采用安全专网、内联网等特殊定制的基础设施架构,来对安全性进行加固;使用类似网闸这样的设备来将关键目标与外界网络进行高度隔离,并通过封闭性与内部的隐蔽性、动态性,来增强内生防御能力。

高价值对象的保护需要保证底层基础设施的安全与可信。路由器、交换机等容易被忽略的基础设施,很容易成为一个安全漏洞,需要提升安全性要求。可以基于 5G 网络切片以及固定移动融合的接入能力,构建安全专网,提供一揽子的全程设备安全能力,并且支持回溯与行为轨迹跟踪,通过审计与问责降低内部攻击风险。

对于高价值目标的保护,还需要建立人机协同防御机制,以避免对机器的过度依赖与盲目信任。区块链技术对于类似工业互联网这样的高安全场景,同样具有优势,管理者在实施重要的控制之前,通过多

方主体的共识认可后才予以执行。

(3)隐私性:设备即身份。

5G 把网络的触角延伸到了各行各业之中,包括健康、智能家居、公共服务等场景,会产生大量更为精确、更为敏感的个人数据。而这些数据一旦泄露,对于用户的影响将非常严重。另外,由于设备的暴露性,以及各种边缘能力的使用,非法获取用户隐私可从任何地点发起,例如个人可穿戴设备,以及驾驶数据等。

由于设备与个人存在的对应关系,对于设备的标识以及其他相关的隐私性数据,也需要参考隐私保护相关的法规进行保护。为了防止对设备身份的识别与关联,必要时应当采用临时设备标识的方式对设备的永久标识进行替代。例如,介质访问控制(MAC)地址、IPv6 地址等等。

3.4 运营型特征

(1)权属性:管理关系明确。

不同于安全边界的模糊化,大多数行业应用的解决方案涉及到的设备、资产、基础设施以及软件服务等,都是处于同一个产权边界中,因此,安全需求可以在同一个产权边界之内进行端到端一体化设计和实施。对于 5G 网络及基础设施而言,具有明确产权边界的行业应用系统,对于定制一揽子增强的端到端的安全服务能力非常有利。

(2)低信任:万物互联互通的空中楼阁。

开放与安全永远是一对矛盾。互联网业务通过人的自治与认知能

力建立起通信对象之间的信任关系,并由业务提供者进行背书。5G 生态带来了更多的参与者与商业模式,各种创新型的业务需要跨越多商业主体的产权边界与系统边界进行协同。然而,除了传统的法律手段,各商业主体之间的信任关系难以找到可信第三方进行背书。这导致大量的物联网能力实际上处于封闭状态,数据本身的价值流转仍然缺乏行之有效的手段与平台,所谓的万物互联仍然是空中楼阁。基于用户身份识别卡(SIM)/嵌入式用户身份识别卡(eSIM)的实名制、端端可信连接能力以及产业链中的位置,运营商成为 5G 生态中商业化信任网络的核心。通过运营商特有的各种安全认证通道、强大的基础设施地位,可以采用去中心化标识(DID)技术^[4]通过区块链聚合商业生态中多方权威与信任主体,建立跨越多监管主体、多运营商网络、多垂直行业平台之间的可信数字身份体系,消除 5G 信任鸿沟,支持跨垂直行业的商业模式的创新。

在诸如车联网(V2V)等设备到设备(D2D)的通信场景下,随机、动态的设备之间天然缺乏信任,并且也没有建立长期信任关系的需求。在这种场景下,如何对身份进行验证并建立安全的通道是 5G 车联网需要重点考虑的一个安全问题。诸如基于标识的加密(IBE)、匿名认证等技术将在此发挥更大的作用。

(3)文化差异:IT 与 OT 的碰撞。

由于文化与经验各不相同,IT 安全专家与 OT 专家之间在组织、方法、流程与策略等方面存在很大的

差异性。IT 安全专家缺乏 OT 方面的专业知识,优先考虑的是安全性、合规性和审计性等要求;而 OT 专家缺乏安全专业知识,优先考虑的是设备或者资产的可用性。

垂直行业应用的安全需要兼顾 IT 与 OT 2 个领域、2 种文化,其中领导者的支持尤为重要,需要将 IT 与 OT 的融合安全,作为企业的重要风险进行评估与跟踪。

4 结束语

为了使垂直行业用户对 5G 网络有足够的信心,相信 5G 网络能够提供与传统企业专网同样甚至更高等级的可靠性与安全性,并愿意将关键业务迁移到 5G 网络之上,运营

商还需要做更多的工作:一方面需要提供专业化的 5G 安全专网的定制能力;另一方面,还需从法律层面为用户的服务质量与安全性做出承诺与保证,并能够根据相应的服务等级协议(SLA)对 5G 安全专网进行全生命周期端到端的安全治理。

随着国家信息安全技术网络安全等级保护基本要求 2019 版(等保 2.0)的推出,国家对于关键信息基础设施的保护已经有了法律依据与实施准则,尤其面向物联网、云计算、大数据等新的技术环境,提出了针对性的等级保护与评测要求^[5]。垂直行业需要主动对齐相应的保护等级要求,在保护自身资产的同时,承担应尽的社会责任。

参考文献

- [1] ETSI. MEC Technical Requirements: ETSI GS MEC-002[S].
- [2] 5G-ENSURE_D2.5 Trust Model (final) v2.2 inc History[EB/OL].[2019-05-20] <http://5gensure.eu/files/5g-ensure25-trust-model-final-v22-inc-history.pdf>
- [3] CHALLENGER D, YODER K, CATHERMAN R. A Practical Guide to Trusted Computing[M].USA: IBM Press.2008
- [4] Data Model and Syntaxes for Decentralized Identifiers (DIDs)[EB/OL].[2019-05-20] <https://w3c-ccg.github.io/did-spec/>
- [5] 信息安全技术网络安全等级保护基本要求:GB/T 22293-2019[S]. 2019

作者简介



汤凯,中兴通讯股份有限公司资深系统架构师;先后从事 3G 核心网系统与 IMS 系统的研究、架构设计与研发管理工作,以及物联网标识体系、区块链及安全、可信数字身份体系等方面的研究与项目孵化工作,目前主要从事 5G、物联网与垂直行业等领域的解决方案与新技术研究等工作;曾参与多项国家标准的制定工作;提出 10 余项发明专利。

←上接第 24 页

相关的信息,做散列或者加密处理,保护数据安全。

根据通用数据保护条例(GDPR),涉及的个人数据包括:国际移动用户识别码(IMS)、国际移动设备识别码(IMEI)、UE IP、网管用户电话号码和 Email。我们采取的策略为内安全、外脱敏:欧盟内系统间数据,通过数据加密、传输通道加密、权限控制、系统加固等措施,保证个人数据的安全;欧盟外的数据转移,则使用强制脱敏的方法,要求数据使用非可逆算法脱敏处理。

(5) 日志审计。

基站对于系统运行过程中的安全事件和关键信息予以记录并保存。如果发生安全入侵,可以根据日志或记录对事件进行回溯,确

定事件原因,提供有效证据防止人员或实体否认执行过的活动。

3 结束语

中兴通讯 5G 网络设备实现了 3GPP 协议要求的安全功能,同时在基础设施的硬件和软件资产、操作维护的接入认证、访问控制进行了安全控制增强,在敏感数据保护、防 DoS 攻击方面采取了强化措施,确保 5G 网络设备的运营安全。

参考文献

- [1] 3GPP. System Architecture for the 5G System; Stage 2(Relase 15): 3GPP TS 23.501 [S]. 2019
- [2] 3GPP. Security Architecture and Procedures for 5G System(Relase 15):3GPP TS 33.501 [S]. 2019
- [3] 3GPP. Network Domain Security (NDS); Authentication Framework (AF)(Release 15) 3GPP TS 33.310[S]. 2018
- [4] RFC. Internet Key Exchange Protocol Version 2 (IKEv2): RFC 5996[S]. 2015
- [5] RFC. IP Encapsulating Security Payload (ESP): RFC 4303[S]. 2005

作者简介



陆海涛,中兴通讯股份有限公司高级工程师、资深系统架构师;负责 5G 移动通信超密集组网关键技术研究,从事 SDR 软件平台、大规模信道仿真验证平台、FDD-Massive MIMO 产品和 5G 产品的系统方案设计工作;获广东省科学技术二等奖以及深圳市科技创新一等奖;发表论文 2 篇,申请发明专利 20 项。



李刚,中兴通讯股份有限公司高级工程师、研发总工;从事 TD-LTE、FDD-LTE、Pre5G、5G 等产品的技术方案设计、架构和研发项目管理工作;发表 2 篇论文,申请发明专利 15 项。



高旭昇,中兴通讯股份有限公司高级工程师、5G 产品研发总工;负责 CDMA、WiMAX、LTE、5G 等产品的系统方案设计、技术改进和研发管理工作;发表 2 篇论文,申请发明专利 10 项。



网络安全——5G 的基石

Keystone for 5G: Network Security

苏洲/SU Zhou

(西安交通大学, 陕西 西安 710049)
(Xi'an Jiaotong University, Xi'an 710049, China)

DOI: 10.12142/ZTETJ.201904010

网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1915.002.html>

网络出版日期: 2019-07-09

收稿日期: 2019-06-10

摘要: 随着移动通信和智能设备的迅速发展, 5G 通信网络以其高速率、广连接、低时延引发了新一代的信息网络变革。如何建立可信、可靠、可管的 5G 通信网络面临一系列网络安全挑战。网络空间安全已成为 5G 通信网络发展的基石所在。在回顾网络安全技术发展的基础上, 探讨了 5G 通信网络面临的新型安全问题, 并结合用户隐私保护、信任管理和数据存储 3 个方面研讨了相应的网络安全保护策略。

关键词: 5G 通信网络; 网络安全; 用户隐私保护; 信任管理; 数据存储

Abstract: With the rapid development of mobile communication and intelligent devices, the 5G network has emerged as a new revolution for information networks, which can provide high speed, wide connection and low delay to improve the quality of service for mobile users. How to establish the credible, reliable and manageable 5G communication network faces a series of network security challenges, which are keystones for 5G communication. In this paper, the security problems in the 5G communication network are discussed, and the corresponding network security solutions including privacy protection, trust management and data storage are studied.

Key words: 5G communication network; network security; user privacy protection; trust management; data storage

1 移动网络安全发展

从古代的飞鸽传书到今日的第 5 代通信技术(5G), 通信与人类历史的发展紧密相关。尤其是近几十年来, 随着无线通信技术的快速发展和不断变革, 移动网络从基于模拟信号的第 1 代通信技术(1G)逐渐发展到基于数字信息的 5G, 业务类型也从单一的语音通话转变到语音、数据、多媒体等综合业务并行发展。与此同时, 通信网络安全问题也逐渐地引起了人们的广泛关注和讨论。

1G 作为第 1 代的移动通信技术, 其网络安全也处于起步阶段。1G 移动通信系统的语音业务基于模拟信号, 每一个语音通话都会在

无线电发射塔中回放, 使得语音通话有可能受到第三方的窃听、劫持或篡改^[1]。第 2 代通信技术(2G)主要是基于全球移动通信系统(GSM)的语音业务, 其网络安全主要面向语音通话应用^[2]。2G 通信网络利用 GSM 数字信息进行信息交换和数据传输。GSM 可实现基于共享密钥的用户认证、基于 A5/1 和 A5/2 流秘密无线通信加密、基于用户身份识别卡(SIM)安全模块的用户身份保密等网络初步安全^[1]。

第 3 代通信技术(3G)除了提供语音业务外, 还支持多媒体业务、数据业务等多种信息业务, 从而提供了支持语音和数据并重的业务环境。该业务环境给通信网络系统提出了新的安全特性需求。3G 通信

网络安全措施主要有用户身份认证、消息认证和机密、无线借口存取控制等^[2]。第 4 代通信技术(4G)网络与 2G、3G 网络相比, 在传输速率、通信质量及稳定效果等多个关键点都获得了突破性进展。与传统网络相比, 4G 出现了多项新技术来提升网络服务的安全性: 在无线接入网方面, 4G 网络通过安全传输、安全接入、身份认证、安全信息数据过滤、访问控制等方式提升了接入网安全性能; 在移动智能终端方面, 4G 网络利用物理硬件防护、强化操作系统等方式在保护网络设备安全上取得了一定进展^[3]。

2 5G 通信网络安全挑战

5G 网络的服务多样性使其不

再局限于个人用户,它不仅能为智能终端提供更快的通信速率或更丰富的功能,还将服务于移动物联网等垂直行业,并衍生出多种新服务和新应用。由于不同垂直行业的业务目标不同,5G网络服务之间的安全需求也有较大差异。例如,移动物联网设备要求轻量级网络安全,而高速移动服务要求高效移动安全,因此,基于网络的逐跳安全的保护方法无法为多样化的服务构建差异化的端到端通信安全。随着物联网的蓬勃发展,越来越多的人能够远程操作联网设备或与联网设备“交谈”。例如,指示智能家居的启动和关闭。因此,在5G网络中,需要更严格的网络安全维护方法来有效应对诸如物联网设备未经授权的访问等带来的网络安全课题^[4]。

虚拟与现实是5G的另一热点。以网络功能虚拟化(NFV)/软件定义网络(SDN)为代表的相关技术被广泛应用于5G网络中来提供更灵活、更高效、更低成本的相关网络服务。虽然NFV与SDN提高了5G网络的效率和性能,但新的安全问题也随之产生。传统网络中,网络节点的安全性很大程度上取决于它们物理实体间的隔离程度。然而,在5G网络中,NFV技术使得部分网络节点以虚拟网络节点的形式部署在基于云处理器的基础设施上。因此,为了保证5G业务在VNF环境中的安全运行,需要开发出更可靠的隔离方法和技术。SDN技术的应用可以提高5G网络数据传输速率,优化资源配置。但在5G环境中,也需要考虑SDN控制虚拟网络

节点和转发节点的安全隔离策略和可信管理方案,并保证SDN流表的可靠性和执行的准确性。

异构性是5G网络的另一主要技术特征。异构性不仅体现在诸如WiFi和长期演进(LTE)等接入技术的不同,还体现在接入网络架构的差异化和多样化;因此,5G网络需要构建综合安全机制,在多样化的接入技术和接入网络架构上建立安全的服务网络。物联网设备在5G网络接入方式上有多种选择,如设备直接连接网络,通过接入点汇聚后连接到网络,或通过设备到设备(D2D)、中继等方式连接到网络;因此,5G物联网设备和网络之间需建立准确的信任关系,需要高效、轻量级的安全管理方式。

5G网络还具有深度推广性,包括远程医疗、智能家居、智能交通在内的越来越多的垂直产业将采用5G网络。作为开放的平台,5G网络引起了人们对隐私泄露的密切关注。移动通信网络作为网络访问的主要方式,承载着大量的个人隐私信息(如身份、位置和隐私内容)的数据和信令。为了提供差异化的服务质量,网络可能需要感知用户使用服务类型,而服务类型往往涉及用户隐私,有产生用户隐私泄露风险。因此,为了保护用户隐私,5G网络需要提供更加严密和广泛的保护技术。

3 5G 通信网络安全举措

3.1 隐私保护机制

以5G通信网络内容分发为例,

例如在微信好友间的图片、视频的分享和传递过程中,移动用户在本地产生成内容,然后将内容上传到内容分享服务器,最后内容请求用户可以从内容分享服务器中获取所需的内容。然而,由于用户产生的内容往往包含用户位置隐私信息,内容分享后易造成隐私泄露。若恶意用户或者不可信服务器泄露这些位置隐私信息,会造成用户人身和财产的损失和危害。因此,在5G网络中需要建立合理的隐私保护机制来避免用户隐私信息的泄露。

假名变换策略和匿名算法有助于保护5G通信网络中的用户隐私。在5G网络中,移动用户通过不定期变换通信使用的假名,隐藏自己的位置信息与真实身份之间的映射关系,从而防止位置隐私的泄露。在匿名算法中,针对一般用户对不可信内容分享服务商的位置隐私泄露问题,通过将移动用户的真实位置泛化为 k 个在概率上不可区分的位置,使得攻击者获得用户真实位置的概率最高为 $1/k$,从而确保移动用户位置的隐私性。

3.2 信任管理机制

5G通信网络中,移动用户可以作为感知节点来感知环境信息。例如,在群智感知中,感知服务请求者向感知服务平台发布感知任务,感知服务平台根据感知任务请求移动用户完成感知任务,移动用户将感知结果返回给感知服务平台,最后感知服务平台将感知结果发送给感知服务请求者。然而,移动用户为了节省资源,获取利益,有可能向感

知服务平台注入虚假或者恶意的感知数据,造成感知结果不准确甚至破坏网络的正常运行。因此,在信息感知服务过程中,需要对参与感知任务的移动用户进行信任分析,选取可信用户的感知数据。

面向 5G 通信网络,对用户进行信任评估的方法可大致分为以下的 2 类:

(1)集中式信任管理机制。该机制利用集中式处理器获取信任信息,并实时管理和实现全局的用户信任评估。集中式处理器可以通过统计感知用户任务完成情况来实现信任评估,也可以根据感知服务平台对感知用户的评价来评估用户的信任值。

(2)分布式信任管理机制。该通过模拟现实社会的用户社交关系来建立和维护用户信任信息,将移动用户信任的评估分散到多个不同的实体,并通过实体之间的通信和信任推荐来实现各个实体自主地对移动用户的信任评估。

3.3 灾备缓存机制

无线终端的迅速普及和无线通信技术的快速发展也带来了不容忽

视的带宽压力和服务延迟。5G 网络通过将内容存放在离用户较近的边缘缓存设备上,降低服务延迟,缓解骨干网络带宽压力。然而,由于网络组网模式异构性和缓存设备可靠性的不一致性,较低可靠性的节点易遭到攻击,缓存内容易遭到篡改和丢失。因此,在 5G 网络中需要合理的内容缓存机制来确保缓存内容的安全性和缓存服务的可靠性。

基于云服务器的内容灾备机制利用多个云服务器作为边缘缓存设备的灾备服务器,为缓存内容提供协作灾备服务,从而防止缓存内容在边缘缓存服务器上丢失、损坏和篡改。在基于边缘缓存服务器协作的内容灾备机制中,由于边缘缓存服务器的异构性和差异性,多个边缘缓存服务器具有不同的安全性和缓存性能;因此,多个边缘缓存服务器能够相互协作灾备缓存内容,从而提高单个边缘缓存服务器缓存服务的可靠性,提高缓存内容的安全性。

4 结束语

5G 通信网络在新一代通信网络的布局 and 规划中起着战略性的关

键作用。网络安全是保障 5G 进一步推进、普及和应用的关键所在,用户隐私、信任管理、灾备存储等方面已成为 5G 网络安全的关键课题和挑战,其核心技术势必会促使相关产业的变革和发展,为人们带来安全、迅速、绿色的 5G 通信网络体验。

参考文献

- [1] PAVIA J, LOPES D, CRISTOVAO P, et al. The Evolution and Future Perspective of Security in Mobile Communications Networks [C]// International Congress on Ultra Modern Telecommunications and Control Systems. Germany: ICUMT. 2017:267-276.DOI:20.1109/ICUMT.2017.8255180
- [2] 曹鹏, 文灏, 黄载祿. 第三代移动通信系统安全[J]. 移动通信, 2001, 1(1): 20. DOI:10.3969/j.issn.1006-1010.2001.01.004
- [3] 李炜键, 孙飞. 基于 4G 通信技术的无线网络安全通信分析[J]. 电力信息与通信技术, 2014, 12(1): 127. DOI:10.3969/j.issn.1672-4844.2014.01.028
- [4] IMT-2020(5G)推进组. 5G 网络安全需求与架构白皮书[R]. 2017

作者简介



苏洲,西安交通大学网络空间安全学院教授、博导、院长;主要研究方向为物联网信息安全、隐私保护、大数据存储与人工智能关键技术等;主持国家自然科学基金重点项目、重大研究计划培育项目等科研项目;获得 IEEE ComSoc GCCTC2018、IEEE CyberSciTech2017、WiCon2016 等国际会议最佳论文奖。



5G 网络设计与规划优化探讨

Optimization of 5G Network Design and Planning

韩玮/HAN Wei
江海/JIANG Hai
李晓彤/LI Xiaotong

(中兴通讯股份有限公司, 广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTETJ.201904011
网络出版地址: <http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1517.002.html>

网络出版日期: 2019-07-09
收稿日期: 2019-05-23

摘要: 基于 4G 时代丰富的组网经验, 中兴通讯研究适用于 5G 高性能组网的技术方案, 包括覆盖容量关键指标分析、多场景下波束配置优化、精细化网络规划、智能化网络优化等, 同时依托全球数十张规模试验网络, 使得这些技术方案不断演化生长, 进一步促进 5G 的商用发展。

关键词: 大规模多输入多输出(MIMO); 网络规划; 智能网络

Abstract: Based on the rich networking experience of the 4G era, ZTE researches the technical solutions applicable to 5G high-performance networking, including analysis of key capacity indicators, beam configuration optimization in multiple scenarios, refined network planning, and intelligent network optimization. Relying on dozens of scale test networks at home and abroad, these technical solutions have been continuously evolved to further promote the commercial development of 5G.

Key words: massive multiple-input multiple-output (MIMO); network planning; intelligent network

1 5G 网络设计面临的挑战

1.1 丰富的应用场景

4G 改变生活, 5G 改变社会。5G 具有鲜明的场景应用特征, 它围绕人们居住、工作、休闲、交通以及垂直行业的需求展开商用部署。这些场景需求分别具有超高速率、超高质量、超高可靠低时延、超高密度、超高连接数、超高移动性等一系列特点^[1-2]。

(1) 增强移动宽带(eMBB)场景。该场景指面向移动通信的基本覆盖环境, 可为用户随时随地提供 100 Mbit/s 以上的体验速率。在室内外、局部热点区域的覆盖环境, 甚至可提供 1 Gbit/s 的用户体验速率

和 10 Gbit/s 以上的网络峰值速率, 满足 10 Tbit/(s·km²) 以上的流量密度需求。

(2) 高可靠低时延通信(uRLLC)场景。该场景能够面向车联网、工业控制等物联网的特殊应用需求, 为用户提供毫秒级的端到端时延和接近 100% 的业务可靠性保证。

(3) 海量机器类通信(mMTC)场景。该应用场景具有小数据包、低功耗、低成本、海量连接等特点, 并要求支持 10⁶/km² 以上的连接数密度。

其中, eMBB 场景是当前商业模式最清晰的业务场景, 也是运营商重点投入的领域。uRLLC、

mMTC 类业务与垂直行业紧密相关, 随着 5G 生态的演进完善, 必然将产生大量应用, 并能改变社会生活方方面面。本文中, 我们将以 eMBB 场景为核心, 论述中兴通讯在组网性能、网络规划和优化等方面的研究成果与技术观点。

1.2 鲜明的技术特点

5G 的技术特点的关键词是“灵活”和“复杂”。为了匹配未来社会的多变场景, 新空口(NR)技术从协议设计之初就考虑灵活配置, 不可避免地带来架构和实现细节上的复杂性。大规模多输入多输出(MIMO)、丰富参考信号、灵活多波束、独立组网(SA)/非独立组网

(NSA)架构等构成了NR最鲜明的技术特征。这些核心技术对NR组网提出了最大的挑战。

(1)大规模MIMO技术。

大规模MIMO在4G长期演进(LTE)后期即出现在商用部署中,中兴通讯是该技术的领导者。在单链路香农限和噪声限被高度逼近的情况下,空分复用是唯一成倍提升频谱效率的方法。大规模MIMO就是用更多的空分复用增强空口流量,这一技术在NR中继续被发扬光大。

大规模MIMO设计复杂精密,其实质是基于探测参考信号(SRS)的波束赋形技术,利用上下行互易性降低资源开销,很好地实现MIMO的赋形和更高的空分倍数,还使得单用户MIMO、多用户MIMO的性能显著改善。同时,考虑到部分终端不支持SRS轮发功能而无法通过基于SRS的赋形实现单用户MIMO的情况,需要补充基于预编码矩阵指标(PMI)反馈方式赋形。2种波束赋形相结合的方式极具创新性,既能有效提高小区吞吐量,又能提升单用户体验。

(2)丰富的参考信号设计。

NR的参考信号在LTE基础上做了大量扩展和改进,以适应于大规模MIMO的应用。小区参考信号(CRS)是LTE中最重要的参考信号,LTE的测量、数据解调均依赖于此,同时它也是LTE组网的重要参考指标,广泛用于网络规划和优化中。但CRS占用固定时频资源,并且随着天线端口增加而带来更大的系统开销,同时也会对邻区产生更

强的固定干扰等不利因素。需要在NR系统中删去CSR的设计,代之以更先进、更丰富的参考信号设计。LTE与NR参考信号的作用对比见表1。

NR在信道状态信息参考信号(CSI-RS)、解调参考信号(DMRS)、SRS等方面做了增强设计,包括灵活周期配置,减少系统开销等。NR的DMRS等可根据用户的移动速度灵活发送:在低速场景下以固定位置发送;在高速场景下可随着移动速度灵活地插入1~3个DMRS,以增强解调能力。SRS也可配置为更短周期,以适用无线信道的快速变化。NR协议对CSI-RS的设计发扬光大,可支持配置多种天线端口数目,并且还可配置为用户级CSI-RS,实现更精准的下行信道估计。此外,NR协议还设计了一系列测量参考信号,如跟踪参考信号(TRS)、相位跟踪参考信号(PTRS)等,为高质量的通信链路保驾护航。

第3代合作伙伴计划(3GPP)协议设计了如此纷繁复杂的参考信

号,但并未规定在实际建网中应该如何组合和使用。这显然对NR网络建设提出巨大挑战,需要在网络规划和优化中不断研究摸索。

(3)灵活多波束设计。

NR基于大规模MIMO技术,采用多波束进行赋型、扫描、跟踪,提升了网络覆盖,减少干扰。相比LTE技术,NR在业务和控制信道、在水平和垂直维度均能提供动态窄波束,并且数目更多,配置更灵活。例如,同步/广播块(SSB)承载了同步和广播功能,是NR最重要的公共信道之一,也是网络性能设计的重要参考指标。SSB可实现时频域灵活配置,在空域还可采用时分波束扫描。由于增加了扫描维度,可选广播权数量增多,如何选优NR广播权成为影响NR网络建设首要解决的问题。

1.3 网络性能挑战

5G不仅仅是一张传统通信网络的升级演进,它带来的是信息生态的改变。从传统的人与人的链

▼表1 LTE与NR参考信号作用对比

参考信号		NR	LTE
CRS	N/A		RSRP/SINR 测量 CQI/PMI/RI 测量(TM2/3/7/8) 数据解调(TM2/3)
CSI-RS	RRM 测量 无线链路状态监测 CQI/PMI/RI 测量		CQI/PMI/RI 测量(TM9)
TRS	更精确的时域跟踪		N/A
PTRS	用于高频相噪补偿		N/A
DMRS(上下行)	公共/控制/业务解调,支持自包含帧		数据解调(TM7/8/9)
SRS(上行)	更高精度信道测量,用于预编码设计、上行波束管理;可具备轮发功能		为调度和链路适配进行信道测量

CQI: 信道质量指示

CRS: 小区参考信号

CSI-RS: 信道状态信息参考信号

DMRS: 解调参考信号

LTE: 长期演进

NR: 新空口

PMI: 预编码矩阵指示

PTRS: 相位跟踪参考信号

RI: 秩指示

RRM: 无线资源管理

RSRP: 参考信号接收功率

SINR: 信干噪比

SRS: 探测参考信号

TM: 传输模式

TRS: 跟踪参考信号

接,发展为人与物、物与物的链接。迄今为止,对于5G应用场景,还无法完全确定未来的真实需求到底会是什么?会对无线网络形态带来哪些革命性冲击?

另外一方面,3GPP用极具灵活的协议设计应对未来组网的不确定。无论是大规模MIMO技术多种传输机制,灵活配置的参考信号和波束、帧结构,或SA/NSA的架构设计等,都使得NR网络灵活、复杂而难于驾驭。

中兴通讯依托于LTE时代Pre5G的成熟商用经验,在NR项目之初就组建了专注网络解决方案的专家团队,在NR组网技术研究、精细化网络规划、智能化网优等方面做了充足准备,形成整套方法论,并辅之以算法分析和外场验证、配套支撑工具等不断改进和优化。

2 5G 组网技术

自从3G时代引入高速共享下行包接入技术(HSDPA),采用共享信道资源来提升业务信道能力之后,覆盖、容量、性能就成为网络设计中相互制约和转换的铁三角^[3]。

在5G NR中,波束选择方案、参考信号选择方案、终端能力等也是影响网络性能的关键因素,在组网设计中都需要重点被分析。

2.1 覆盖能力

覆盖能力是组网首先要解决的课题,包含3个关键点:首先找出NR上下行信道受限逻辑关系,确定网络建设的依据;其次,分析哪些技术对覆盖能力产生影响,以被列为组网调优储备手段;最后,确定关键信道配置和指标,实施具体网络规划设计。

2.1.1 覆盖受限逻辑

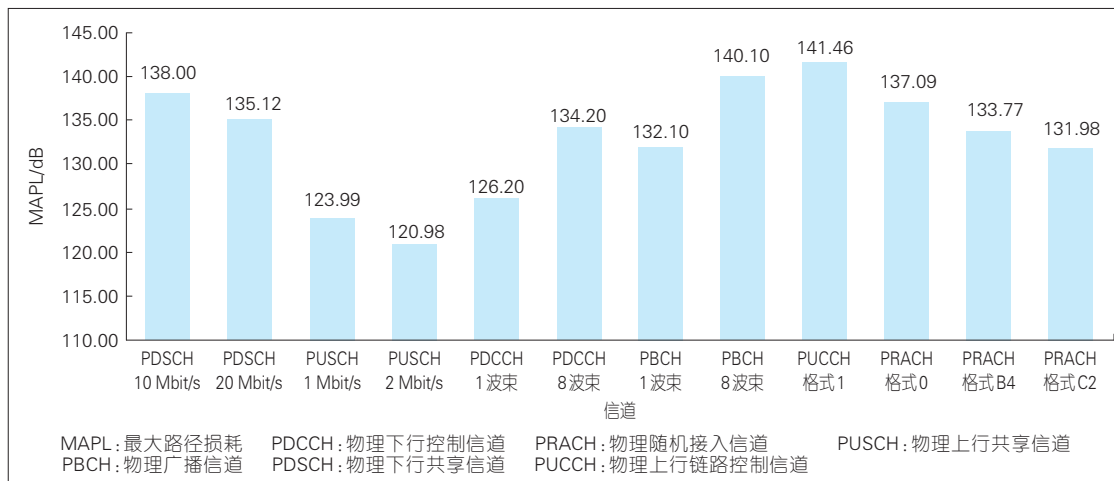
我们将NR的上下行所有链路放在一张链路预算图中,如图1所示。从图中的对比关系可知,当边缘用户目标为2 Mbit/s时,物理上行共享信道(PUSCH)的覆盖最短;其次是采用单波束的公共物理下行控制信道(PDCCH)和广播信道(BCH)存在覆盖受限风险。因此,NR的覆盖短板是上行方向的PUSCH业务信道,该信道应成为组网设计的首要目标对象。

PUSCH成为首要受限目标的原因是:NR的上行承载业务需求高,通常是边缘1 Mbit/s或2 Mbit/s,但NR终端的发送功率有限,无法在大带宽上保持高功率谱密度。在NSA链路预算时还需考虑增加终端能力,因NSA终端的发送功率削减、预编码增益损失等因素都会对上行覆盖能力产生更大压力。其次,NR在下行可采用多波束方式,增强公共信道覆盖,缓解下行覆盖能力的压力,这使得下行信道不易成为覆盖受限瓶颈。以图1为例,如果下行从单波束改为4波束或者8波束,理论上又可增加5~8 dB的覆盖能力。因此,在通常配置情况下,NR网络是一个上行业务信道覆盖受限系统,应进行网络覆盖规划与站点规模估算;但依然要做完备性分析,例如通过分析基站下行发送功率、多波束等系统配置,判断是否会改变NR上行受限的逻辑。

2.1.2 SSB波束选择

在NR系统中,SSB是由主同步信号(PSS)+辅同步信号(SSS)+系统信息块(SIB)3部分组成。用户

图1 新空口技术上下行信道链路预算对比关系



(UE)基于SSB的测量和解调,完成网络同步和读取广播,SSB因而成为NR系统中最基本覆盖质量参考。同步信道参考信号接收功率(SS-RSRP)、同步信道信干噪比(SS-SINR)是对SSS的测量值,该指标在衡量网络建设覆盖质量时具有重要意义,常被用于网络规划和优化的关键指标。

LTE采用CRS信号的RSRP/SINR作为网络评估参考指标,CRS采用宽波束时频错开的方式发送;而NR系统中SSB采用多波束技术,实现时、频、空域的精细化组网覆盖,具备更精细化的组网能力。

以NR系统5ms帧结构为例,系统可配置1~8个SSB波束。波束个数越多,单个波束越窄,覆盖能力越强。通过广播权值设计,这1~8个波束可分别覆盖小区内不同的方向,包括垂直维度,形成真正的3D网络波束扫描,有效地提升了在密集城区楼宇场景中的广播覆盖质量。

SSB在时频域对齐的配置下,对SS-SINR等同于网络在100%负荷下的干扰测量,可通过SS-SINR发现越区或重叠覆盖导致的同频干扰,适合在工程建设阶段发现干扰隐患。但是,SSB单波束会导致边缘某些位置点的SINR偏低,从而引起同步失败等问题。因此,需要结合广播权设计,根据不同场景设计SSB波束以及配置方案。

通过中兴通讯大量的外场实践,我们发现增加波束数目能明显提高弱场的RSRP以及SINR值,进而提升整个网络的覆盖率,如图2

所示;因此,在商用阶段需要尽量配置更多SSB波束,以实现广播信道的精细化覆盖。此外,通过广播权设计,可发挥SSB多波束垂直覆盖能力,尤其对于密集城区的高层建筑场景,需要增强UE接入和驻留能力。这些SSB相关的研究结论,对后续网络规划和优化工作方向至关重要。

2.2 容量能力

2.2.1 参考信号配置

相比于LTE网络,NR网络能获得更多的测量,并需要对广播信道和业务信道分别测量。SSB适合做广播公共信道覆盖的预测,而对用户容量的预测则需要另外一种重要参考信号——CSI-RS。CSI-RS主要用于信道质量指示(CQI)、PMI、秩指示(RI)等的测量。相比SSB,CSI-RS与用户容量性能有更大的相关度。在NSA系统中,由于部分终端不支持上行SRS轮发,因此CSI-RS承担着PMI测量值的重任,更是直接影响用户速率体验。

CSI-RS有2个关键配置:端口与预置波束。端口相当于等效天线,把多个物理天线映射为一个等效天线端口;预置波束则是通过每

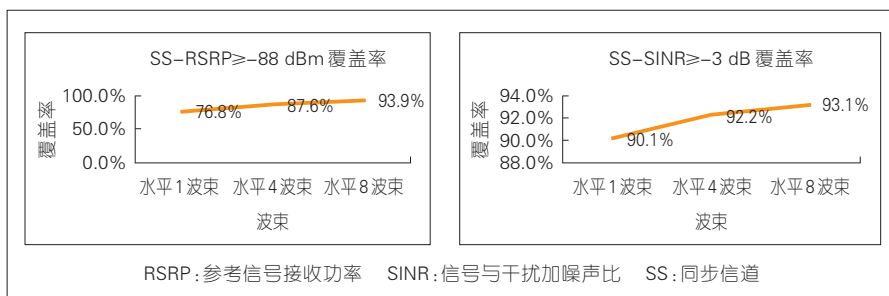
个等效天线端口实现轮扫波束,用于对信道进行探测。CSI-RS通过这2个设置,实现了对空间信道测量的量化,通过反馈方式获取信道信息,为实现以PMI方式的MIMO传输奠定基础。

理论上,CSI-RS端口越多,信道的量化精度越高,预编码增益越大,赋形性能越好;但随着CSI-RS端口数增加,需要的下行CSI-RS资源将更多,对UE测量能力的要求更高,上行反馈的开销更大。在确定的CSI-RS端口数下,预置波束越多,信道的量化精度通常越高,波束扫描增益越大,赋形性能越好;但随着波束数增加,需要的下行CSI-RS资源更多且波束扫描周期更长。另外,波束数增加还意味着波束变窄。由于窄波束内的多径数量变少,将会导致信道表现为缺秩,从而不利于多流传输。

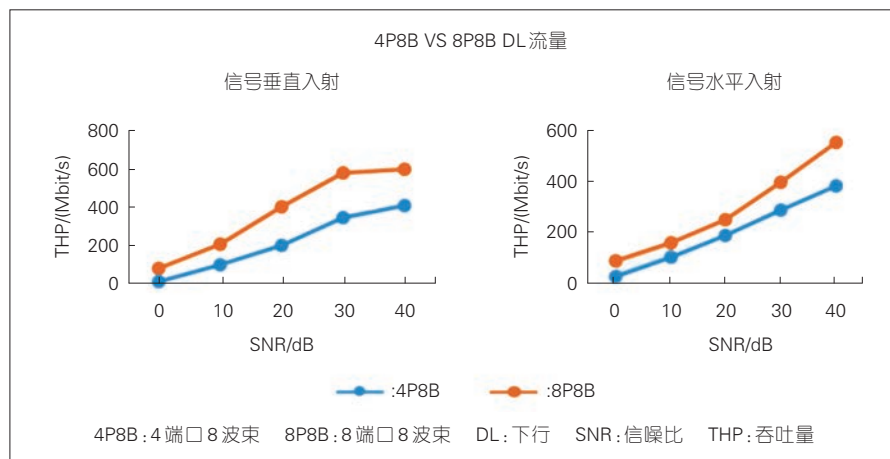
如图3所示,可以看出对于相同预置波束数目,8端口明显优于4端口。

如图4所示,可以看出对于相同端口数目,2波束相对1波束提升约10%。

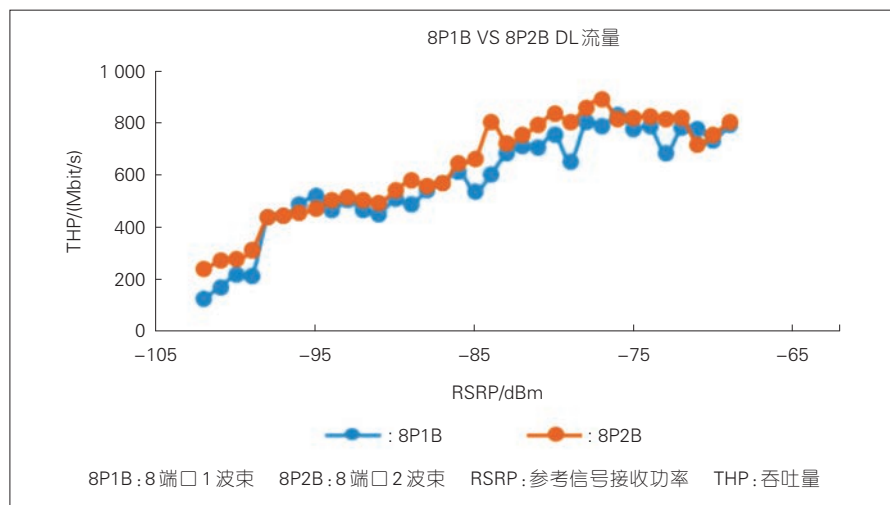
通过研究表明,CSI-RS与系统容量具备高相关性,适合在网络运维和优化阶段作为预测容量性能的



▲图2 不同波束下的广播覆盖质量



▲图3 4端口与8端口信道状态信息参考信号性能对比



▲图4 1波束与2波束信道状态信息参考信号性能对比

参考信号。此外, SRS、DMRS等参考信号也会不同程度上影响容量能力。在网络设计和后续优化中,需详细分析、优化配置系统侧与终端侧各类参数,提升网络容量能力。

2.2.2 设备能力

同LTE等通信系统一样, NR也会推出系列化设备,以适应不同场景和建网成本、体积、功耗等需求。在高层楼宇覆盖需求的密集城区,推荐采用64收发通道(TR)规格设备,在郊区或农村推荐采用低配置

规格设备。

在密集城区,复杂的无线环境导致干扰恶化,高楼林立导致垂直覆盖要求高、用户容量需求大。64 TR设备能提供更优的大规模MIMO的波束赋形,实现高流量的多用户MIMO传输,同时可显著提高垂直维度的覆盖。在郊区和农村, MU-MIMO配对成功率降低, 64 TR设备不能充分发挥其容量优势,因此可采用低配置规格设备。

除了宏站产品之外,室内分布系统、微基站等不同产品规格对应

不同的覆盖和容量能力,每种产品规格也都有各自适用的建网场景。在NR网络建设时需要进行综合考虑,选择对客户最优的配置和组网方案。

3 精细化网络规划

相比LTE网络规划, NR网络规划有3个方面的特点:首先其网络指标设定到较高性能水准,需要精密细致建模的网络规划工具;其次是能洞察LTE现网数据,有的放矢地进行NR网络精细化设计;最后是场景化组网解决方案。对于NR技术特征与组网特性,无一例外地需要在网络规划和优化中被研究和分析,并最终体现为网络性能指标。

3.1 NR网络规划工具

NR网络建设标准是LTE的数倍,并通过采用更复杂的空分传输、多波束、参考信号配置等技术来确保实现网络高性能。这对网络规划工具提出前所未有的高要求。

在通常情况下, NR网络规划边缘速率城区以上行(UL)2 Mbit/s、下行(DL)50 Mbit/s为基准,高热区域则以UL 5 Mbit/s、DL 100 Mbit/s为主要目标,郊区以UL 1 Mbit/s、DL 20 Mbit/s为基准。以上标准是基于对5G关键业务预测而推算得到,例如未来大视频业务会比4G更普遍,在城区场景下,上行2 Mbit/s可以支持720 P直播;下行50 Mbit/s可以支持2 K/4 K高清视频。为了确保对网络性能的准确规划,网络规划工具在无线环境、用户业务以及无线技术等方面的仿真建模的复杂度

都会非常高。

NR 的大规模 MIMO 在垂直维度最大有 4 层波束实现对建筑物等做垂直覆盖,能够大幅地提升通过室外宏站对高层楼宇的室内覆盖性能。这就需要网络规划工具能引入高精度 3D 电子地图,并具备射线追踪仿真能力。NR 的核心之一——多天线技术的性能表现极度依赖于无线环境,只有基于准确的无线环境建模,才能最大限度模拟 NR 的网络性能,实现准确的网络规划设计。

除了 3D 电子地图、射线追踪建模之外,多天线技术建模是 NR 网络规划的核心发动机。各设备厂家的多天线算法不同,需抽象为指标列表与网络规划工具相接口,才能在把贴近真实的性能体现在规划结果中。这些重要的抽象指标有多天线的天线模型、最优权值、链路解调性能等。例如,对于 SSB 多波束轮扫,CSI-RS、DMRS、SRS 等参考信号配置等需在工具中预计抽象建模,这些重要配置是影响网络规划结果的重要因素。另外,由于 NR 系统过于庞大复杂,即使对核心算法指标做了抽象,其参数规划工作量依然巨大,需要诸如自动选站、射频参数自动寻优、弱覆盖区自动识别与加站等工作。并行计算、远程仿真等信息技术(IT)也被大量引入到 NR 网络规划工具中,以提升网络规划运行效率。

中兴通讯在网络规划工具方面已有数年准备,在其全球共享网络仿真中心已实现 NR 网络规划工具的规模部署,并在核心算法、复杂建

模、云仿真等方面走在业界前列。

3.2 网络规划方法论

“基于 4G live data 的 5G 网络规划”是中兴通讯的 NR 规划方法论。LTE 与 NR 在技术体系、应用场景、业务行为等有很多相似之处,用现网 LTE 数据分析来指导 NR 网络设计是最直接有效的方式。NR 独有的技术特点,如多天线、多波束、灵活参考信号配置等也会融合考虑到规划过程中,影响最终分析结论。

LTE 数据可直接帮助识别和锁定 NR 时代的价值区域,包括话务预测、热点评估、重点场景识别。采用人工智能(AI)技术,对现网的用户数、流量等多维数据进行自动价值聚类,快速抓住 NR 网络的规划重点,可以更有针对性地做精细化设计。源源不断的 LTE 海量活跃数据,是无线大数据分析的天然养料,能够帮助 NR 运营者在网络规划、性能优化到日常运维的各阶段都能站在用户视角进行预测和决策。

基于 LTE 网络洞察的 NR 网络精细化规划分为 2 个阶段:预规划阶段、工程执行阶段。

在预规划阶段,需要基于 LTE 网络的覆盖/容量/价值/站点拓扑等多维综合分析,确定 NR 网络建设的区域以及站点预规划方案,并进行初步仿真验证,输出初始规划结果及广播权值配置建议。在此阶段,LTE 与 NR 的系统差异,如功率、频段、路损模型等都会融入进基于 LTE 现网数据分析过程中,进而获得准确的 NR 性能指标预测结果。

在工程执行阶段,需要输出工

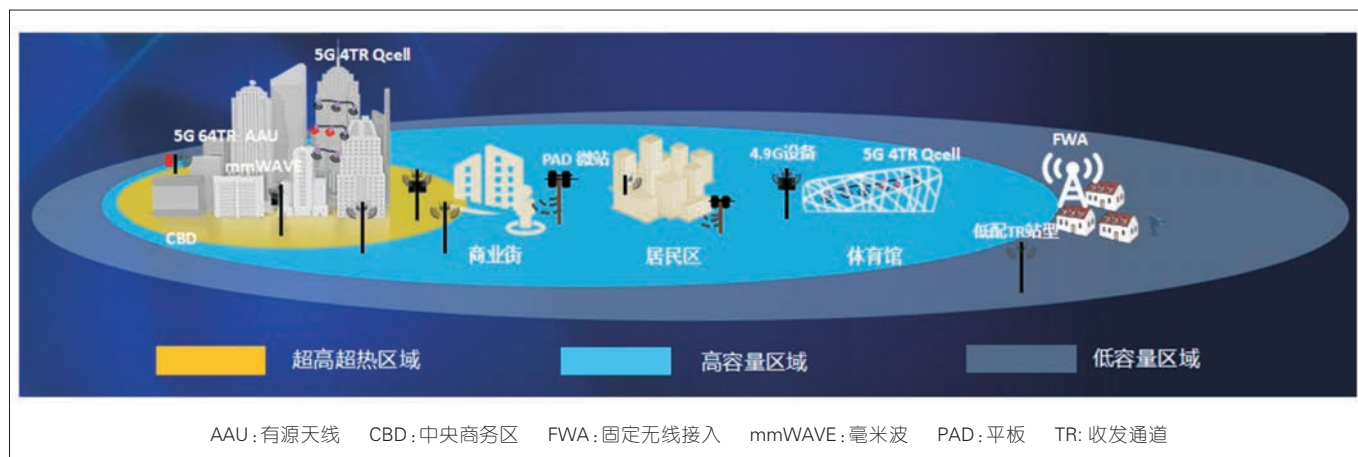
勘确定站点规划落地方案,提供天面整合方案,并进行精细化仿真,以确定多天线广播权值规划、射频(RF)参数规划等无线参数规划。

特别需要指出的是:在 NR 网络预规划以及后续优化阶段,AI 算法引入到传统规划流程之后,大幅提升了工作效率和规划效果。例如,热点站聚类算法实现对价值区域的甄别选取,机器学习方法提取相同环境指标预测覆盖效果,利用大数据平台工具对广播权进行优化等。AI 算法必将与无线通信算法一样,在网络性能规划与优化中持续占据重要地位。

3.3 场景化解决方案

中兴通讯在系列化宏站、室内分布系统、微站等方面进行组合,形成场景化解决方案(如图 5 所示),解决不同场景下的 NR 组网难题。宏站是最重要的产品形态,64 TR 产品解决 4G/5G 阶段持续高容量需求,用低配置规格产品解决 4G/5G 低流量区域、低成本建网需求。针对 NR 的大带宽使用策略以及 4G/5G 网络共享需求,宏站设备支持混模配置功能,能够支持在运营商在当期和未来的经营抉择。室内分布系统产品有 2 TR 和 4 TR 设备,利用现网无源室分系统或者新建等方式,解决高价值、高流量的室内场景。此外,微站也是必不可少的产品形态,4 TR 平板(PAD)射频单元(RRU)产品广泛应用于居民区、步行街等补忙补热场景。

随着市场需求和技术的不断发展,更多新设备会走向小型化、低功



▲图5 场景化新空口站点解决方案

耗、高性能,共同组成按需而动的NR网络。

4 智能网络优化

NR时代,大规模MIMO等革命性技术不仅带来了网络性能的提升,同时使得网络优化的难度有所提升。另外uRLLC、mMTC的特性也与传统通信业务大相径庭,这些都使得NR网络优化的难度大幅增加。中兴通讯提出了网优“三化”思路以应对NR时代新课题,即网优工具的远程化、自动化、智能化,其中远程化、自动化是基础,智能化是核心。

云技术的广泛应用,使得网优工具远程化成为可能,无论是海量测量数据的收集筛选,还是网络性能仿真预测,都可在云端进行。同时,各种路测和分析软件日臻完善,可实时收集、上报分析数据,减轻了网优工程师日常工作量,实现自动化问题定位与解决实施,提升工作效率与质量。5G时代的参数组合高达上万种,如要匹配到最优参数组合,传统的网优专家系统分析已

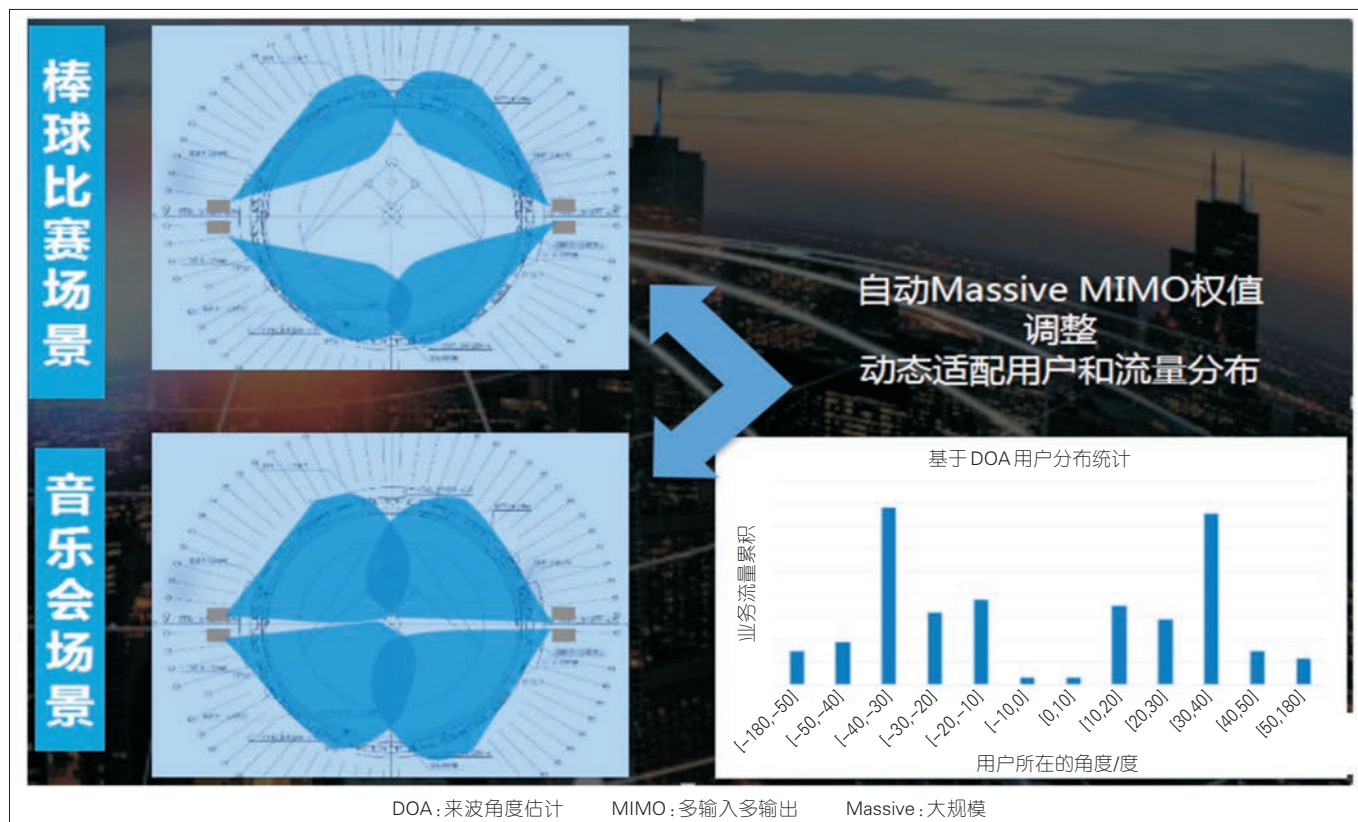
经无能为力。NR迫切要实现更高层次智能化,AI必然在网优系统中扮演重要角色。

在网络层中,处于上层的网元更容易集中化,跨领域分析能力更强,适合对全局性的策略集中进行训练及推理,例如跨域调度、端到端编排等。通常对计算能力要求很高,需要跨领域的海量数据支撑,对实时性要求一般敏感度较低。越下层的网元,越接近端侧,专项分析能力越强,对实时性往往有较高要求,比如NR新空口的移动性策略移动边缘计算(MEC)的实时控制等^[4]。基于这些分层智能化理念,中兴通讯设计推出了5G网优工具集,如价值专家分析系统(VMAX)、集中式自由化网络(C-SON)等工具,形成自环、小环、大环组合,引入AI算法,能够全方位对NR网络进行高效运维和性能优化。不同类型的AI算法被部署到不同的“环”中,以解决不同层面的优化难题^[5]。

基于上述理论和工具,中兴通讯已在NR预商用外场成功验证了AI对天线权值的优化能力。利用

大规模MIMO波束调整原理,部署在各“环”中的AI算法组合协同工作,可针对高楼的垂直面、场馆、具备潮汐效应的区域等场景,分析用户的分布规律,灵活调整广播和控制信道的波束分布,达到覆盖和容量的最优,减少干扰。如图6所示的案例,针对固定场馆类的场景,由于人员分布在长时间内相对固定,可根据这一特点设计广播权值自适应来达到最优覆盖。基于网管、测量报告等数据,结合相关AI算法,进行场景识别,可判断是体育赛事场景还是演唱会场景,并计算出基于此场景和当前用户分布下的最优权值,以提升场馆区域内的CQI、SINR等指标。将权值组合与关键性能指标、用户分布等信息建立关联数据库,便于后期同类场景快速匹配获取优化权值,指导前瞻性运维策略。

每个网元在机器学习、推理自治路上不断进化,实现网络性能的智预测、智能优化、智能决策,其基础是强大的AI算法研究和应用能力。AI算法与通信算法是2个截然



▲图6 人工智能权值自适应的大规模MIMO网络

不同的技术概念,前者推崇逻辑相关,让数据说话;后者则较为注重理论推导,要自证严谨。这两者在5G网络优化中是必不可少,相辅相成,共同守护着一张高性能的无线通信网络。

5 结束语

5G带来的是通信系统建设的全方位改变,无论是对3GPP协议的细节理解,还是组网技术的架构设计以及网规、网优的指标体系和工具平台,处处体现出灵活与变革。同时5G也是包容性很强的技术体系,融入IT云化、AI等技术,构建高效系统。5G也在不断加速发展,“无处不在,随需而动”的高性能无线通信网必然会给人们带来惊喜

体验。

致谢

在文章的撰写过程中,中兴通讯5G产品专家李玉洁、原均和、束裕、张文娟对提出很多卓有见地的修正建议,蒋新建、吴明皓等产品总工为提出大量而翔实的论证数据,在此对他们的专业精神和无私分享谨致谢意!

参考文献

- [1] 3GPP. System Architecture for the 5G System: 3GPP TS 23.501[S]. 2018
- [2] 尤肖虎,潘志文,高西奇,等. 5G移动通信发展趋势与若干关键技术[J]. 中国科学:信息科学, 2014,44(5):551-563.DOI:10.1360/N112014-00032
- [3] 徐志宇,蒲迎春. HSDPA技术原理与网络规划实践[M]. 北京:人民邮电出版社, 2007
- [4] 3GPP. Study of Enablers for Network Automation for 5G: 3GPP TR 23.791[S]. 2010
- [5] 张嗣宏,左罗. 基于人工智能的网络智能化发展探讨[J]. 中兴通讯技术, 2019,25(2): 45-48. DOI: 10.12142/ZTETJ.201902009

作者简介



韩玮,中兴通讯股份有限公司5G系统架构师;主要研究方向为5G产品算法仿真、性能设计与规划。



江海,中兴通讯股份有限公司5G产品无线总工;主要研究方向为5G产品外场性能分析、先进算法架构设计等。



李晓彬,中兴通讯股份有限公司TDD产品团队规划部部长;主要研究方向为TDD/5G产品软硬件以及新技术规划。

《中兴通讯技术》杂志(双月刊)投稿须知

一、杂志定位

《中兴通讯技术》杂志为通信技术类学术期刊。通过介绍、探讨通信热点技术,以展现通信技术最新发展动态,并促进产学研合作,发掘和培养优秀人才,为振兴民族通信产业做贡献。

二、稿件基本要求

1. 投稿约定

- (1)作者需登录《中兴通讯技术》投稿平台:tech.zte.com.cn/submission,并上传稿件。第一次投稿需完成新用户注册。
- (2)编辑部将按照审稿流程聘请专家审稿,并根据审稿意见,公平、公正地录用稿件。审稿过程需要1个月左右。

2. 内容和格式要求

- (1)稿件须具有创新性、学术性、规范性和可读性。
- (2)稿件需采用WORD文档格式。
- (3)稿件篇幅一般不超过6000字(包括文、图),内容包括:中、英文题名,作者姓名及汉语拼音,作者中、英文单位,中文摘要、关键词(3~8个),英文摘要、关键词,正文,参考文献,作者简介。
- (4)中文题名一般不超过20个汉字,中、英文题名含义应一致。
- (5)摘要尽量写成报道性摘要,包括研究的目的、方法、结果/结论,以150~200字为宜。摘要应具有独立性和自明性。中英文摘要应一致。
- (6)文稿中的量和单位应符合国家标准。外文字母的正斜体、大小写等须写清楚,上下角的字母、数据和符号的位置皆应明显区别。
- (7)图、表力求少而精(以8幅为上限),应随文出现,切忌与文字重复。图、表应保持自明性,图中缩略词和英文均要在图中加中文解释。表应采用三线表,表中缩略词和英文均要在表内加中文解释。
- (8)所有文献必须在正文中引用,文献序号按其在文中出现的先后次序编排。常用参考文献的书写格式为:
 - 期刊[序号]作者.题名[J].刊名,出版年,卷号(期号):引文页码.数字对象唯一标识符
 - 书籍[序号]作者.书名[M].出版地:出版者,出版年:引文页码.数字对象唯一标识符
 - 论文集中析出文献[序号]作者.题名[C]/论文集编者.论文集名(会议名).出版地:出版者,出版年(开会年):引文页码.数字对象唯一标识符
 - 学位论文[序号]作者.题名[D].学位授予单位所在城市名:学位授予单位,授予年份.数字对象唯一标识符
 - 专利[序号]专利所有者.专利题名:专利号[P].出版日期.数字对象唯一标识符
 - 国际、国家标准[序号]标准名称:标准编号[S].出版地:出版者,出版年.数字对象唯一标识符
- (9)作者超过3人时,可以感谢形式在文中提及。作者简介包括:姓名、工作单位、职务或职称、学历、毕业于何校、现从事的工作、专业特长、科研成果、已发表的论文数量等。
- (10)提供正面、免冠、彩色标准照片一张,最好采用JPG格式(文件大小超过100kB)。
- (11)应标注出研究课题的资助基金或资助项目名称及编号。
- (12)提供联系方式,如:通讯地址、电话(含手机)、Email等。

3. 其他事项

- (1)请勿一稿两投。凡在2个月(自来稿之日算起)以内未接到录用通知者,可致电编辑部询问。
- (2)为了促进信息传播,加强学术交流,在论文发表后,本刊享有文章的转摘权(包括英文版、电子版、网络版)。作者获得的稿费包括转摘酬金。如作者不同意转摘,请在投稿时说明。

编辑部地址:安徽省合肥市金寨路329号凯旋大厦1201室,邮政编码:230061

联系电话:0551-65533356,联系邮箱:magazine@zte.com.cn

本刊只接受在线投稿,欢迎访问本刊投稿平台:tech.zte.com.cn/submission

办刊宗旨:

以人为本,荟萃通信技术领域精英
迎接挑战,把握世界通信技术动态
立即行动,求解通信发展疑难课题
励精图治,促进民族信息产业崛起

双月刊 1995年创刊 总第147期
2019年8月 第25卷 第4期

主管:安徽出版集团有限责任公司
主办:时代出版传媒股份有限公司
深圳航天广宇工业有限公司
出版:安徽科学技术出版社
编辑、发行:中兴通讯技术杂志社

总编:王喜瑜
主编:蒋贤骏
常务副主编:黄新明
责任编辑:徐烨
编辑:卢丹、朱莉
排版制作:余刚
发行:王萍萍
编务:王坤

《中兴通讯技术》编辑部
地址:合肥市金寨路329号凯旋大厦1201室
邮编:230061
网址:tech.zte.com.cn
投稿平台:tech.zte.com.cn/submission
电子信箱:magazine@zte.com.cn
电话:(0551)65533356

传真:(0551)65850139
发行范围:公开发行
印刷:合肥添彩包装有限公司
出版日期:2019年8月10日
中国标准连续出版物号:ISSN 1009-6868
CN 34-1228/TN
定价:每册 20.00 元