电力 5G 混合组网的安全风险分析

张小建[1,2]，费稼轩[1,2]，姜海涛[3]，姚启桂[1,2]
（1. 全球能源互联网研究院有限公司，江苏 南京 210003;
2. 信息网络安全国网重点实验室，江苏 南京 210003;
3. 国网江苏省电力有限公司电力科学研究院，江苏 南京 211103）

摘　要：5G 通信技术为电力物联网提供了有力支持，同时也在电力行业应用过程中引入了新的安全挑战。基于电力 5G 业务的需求，首先，提出了 5 种 5G 组网部署建设方案，并对其安全性与成本进行对比分析；其次，提出了 5G 与电力通信网混合组网架构，对 5G 网络切片架构按业务场景重新切分；最后，从终端接入、边缘计算、网络通道以及核心网 4 个部分，对 5G 技术引入的安全风险进行具体分析。

关键词：5G；网络切片；混合组网；安全风险；空间安全
中图分类号：TN915
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2022017

Security risk analysis of power 5G hybrid networking

ZHANG Xiaojian[1,2], FEI Jiaxuan[1,2], JIANG Haitao[3], YAO Qigui[1,2]
1. Energy Interconnection Research Institute Co., Ltd., Nanjing 210003, China
2. State Grid Key Laboratory of Information & Network Security, Nanjing 210003, China
3. State Grid Jiangsu Electric Power Co., Ltd., Research Institute, Nanjing 211103, China

Abstract: 5G communication technology provides strong support for the power internet of things, and it also introduces new security challenges in the application process of the power industry. Starting from the analysis of the needs of the power 5G business, five 5G networking deployment and construction plans were proposed, and a comparative analysis of them was conducted in security and cost. And then, a hybrid networking architecture of 5G and power communication networks was proposed, and the 5G network slicing architecture was re-segmented according to business scenarios. Finally, from the four parts of terminal access, edge computing, network channel and core network, the security risks introduced by 5G technology were analyzed in detail.

Key words: 5G, network slice, hybrid networking, security risk, cyber security

收稿日期：2021−9−18；**修回日期**：2022−01−10
通信作者：张小建，zhangxiaojian@geiri.sgcc.com.cn
基金项目：国家电网有限公司总部科技项目《5G 电力安全防护体系及关键技术验证研究》（No.5700-202058379A-0-0-00）
Foundation Item: The Science and Technology Project of State Grid Corporation of China “Research on 5G Electric Power Security Protection System and Key Technology Verification” (No.5700-202058379A-0-0-00)

0　引言

5G 技术是未来移动通信技术发展方向[1]。5G 的低时延、高可靠[2]特点使得电力监控系统等生产控制系统的“无线调控”成为可能。5G 网络切片[3]技术，可以为电力行业用户打造定制化的“业务专网”服务，更好地满足电网业务差异化安全需求。5G 的海量接入容量、高带宽特点和边缘计算能力，为电力物联网、视频类数据的采集传输和就地处理提供了有力支持[4-6]。

5G 在接入认证、通信加密等方面提出了更新、更安全的标准，但在电力行业应用过程中，仍有较多网络安全问题未能解决。5G 网络切片[7]、核心网下沉[8]、多接入边缘计算（multi-access edge computing，MEC）[9]等关键技术和全新的网络设计在更好地支撑多样化应用场景的同时，也对终端接入、边缘计算、网络通道等方面提出了新的挑战。

本文从电力 5G 业务需求分析出发，掌握了电力业务的总体特性和典型指标；提出了 5 种不同的 5G 组网部署建设方案，并对其进行安全性、时延、独立性、部署成本方面的对比分析；根据电力业务需求和企业组网模式分析，提出了 5G 与电力通信网混合组网架构；由于电网不同业务场景通信需求差异较大，对混合组网模式下的 5G 网络切片架构按业务场景进行重新切分；从终端接入、边缘计算、网络通道以及核心网 4 个部分，对 5G 技术引入的新风险、新挑战进行具体分析。

1　电力 5G 业务需求

从业务需求维度分析，5G 电力通信网主要涉及了电力生产控制类大区、信息管理类大区和互联网大区共 3 类业务。具体的细分业务主要包括配电差动保护、同步相量测量装置（phasor measurement unit，PMU）、配电自动化、用电负荷需求侧响应、智能巡检和设施运行状态监测等。

（1）总体特性

呈现超低时延、高安全隔离、高可靠性需求。电力业务应与其他行业业务隔离，电网内部业务应按照安全大区隔离；变电站等局域网应用环境的业务和数据不出园区；大区内的不同业务都需要有服务质量（quality of service，QoS）保障。

（2）典型指标

生产控制类和信息采集类业务之间要求严格隔离；生产 I/II 区的配电差动保护和配电自动化业务呈现确定性低时延需求，双向时延要求 2～5 ms，业务带宽大于 2 Mbit/s，可靠性需要达到 99.999%。管理信息 III 区的低压集抄业务端到端双向时延要求 1～3 s，业务带宽为 1～2 Mbit/s，可靠性需要达到 99.9%。

2　电力 5G 混合组网方案

2.1　5G 组网模式

5G 的应用需要建设和部署 5G 网络，5G 网络主要分为 3 个部分：无线电接入网（radio access network，RAN）、承载网和核心网[10-11]；部署方式大致可以分为企业自建、许可频谱、专网专用、公网专用、公网公用五大类[12-13]，为了满足通信网络需求并降低建设成本，根据实际情况提出不同的部署建设方案。以下对 5 种 5G 企业组网模式进行具体分析。

- 企业自建：独立申请专有频谱，建立完全私有的 5G 专网。
- 许可频谱：与企业自建类似，不同的是，运营商建设 5G 网络基础设施，将部分频谱许可给企业使用。
- 专网专用：采用专有用户面功能（user plane function，UPF）和 5G 核心网控制平面（5G core control plane，5GC CP），并与公共网络在物理上隔离。专有网络和公共网络之间仅共享公网的 5G 基站，采用专有频段或专用小区实现无线资源隔离。
- 公网专用：采用专有 UPF，除接入和移动

管理功能（access and mobility management function，AMF）、会话管理功能（session management function，SMF）等部分网元专享，其余核心网网元共享。使用公网的 5G 基站，但采用物理资源模块（physical resource block，PRB）预留方式进行空口传输隔离。

- 公网公用：共享公网的基础设施，采用网络切片实现业务隔离。

5G 组网模式对比见表 1，从安全性、时延、独立性和部署成本 4 个方面对上述 5 种方案进行具体的对比分析。方案 1 和 2 独立建设 5G 网络基础设施，部署成本较高；由于国家无线频谱资源分配政策，申请专用频谱比较困难。方案 3 和方案 4 采用专有频段或无线资源块预留方式，保障业务数据的安全隔离，满足电网生产控制类或管理信息类业务的应用需求。方案 5 共享公网 5G 基础设施，满足电网互联网大区业务的应用需求。

2.2 5G 与电力通信网混合组网架构

为安全承载电网 3 个安全大区的典型业务，设计了 5G 与电力通信网混合组网整体架构，如图 1 所示。5G 和电力通信网混合组网架构覆盖端、边、管、云 4 个层面。

感知层包括原 4G 网络架构中“端”和“边”的部分，部分终端通过改造直接支持 5G 通信，原边缘物联代理下的终端可通过在边缘物联代理中增加 5G 通信功能，使得边和端满足 5G 通信的接入功能需求。“端层”3 个大区的业务终端北向接入边缘物联代理设备，“边层”边缘物联代理通过

表 1 5G 组网模式对比

组网模式	安全性	是否低时延	独立性	部署成本
方案 1	与公网物理隔离，企业内部可自行管理	是	好	高
方案 2	5G 局域网完全私有	是	好	高
方案 3	所有数据在基站基带处理板共同处理，安全性稍差	是	较好	较高
方案 4	所有数据在基站基带处理板共同处理并混合传输，安全性较差	是	较差	中
方案 5	流量经过运营商的边缘云，安全性差	否	差	低

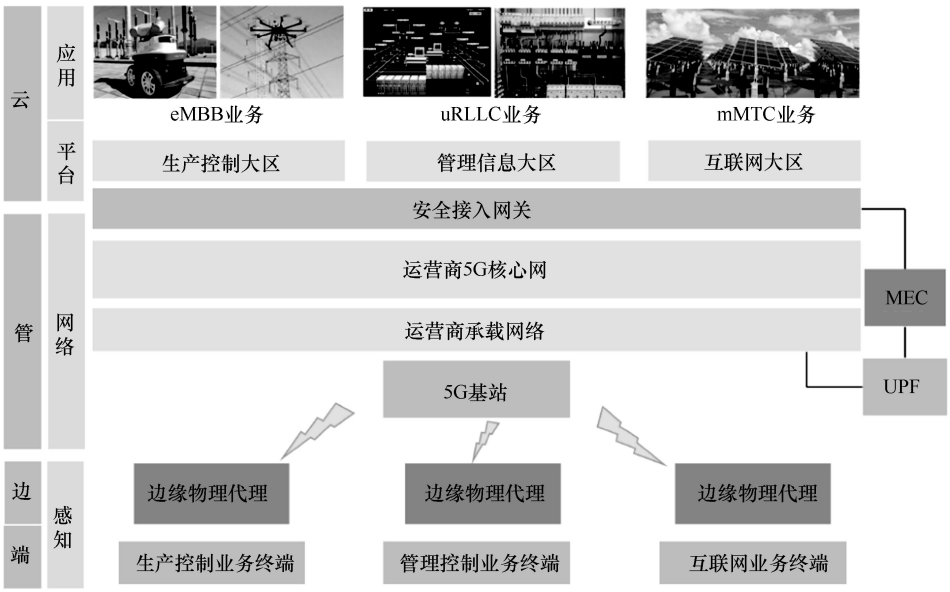

图 1 5G 与电力通信网混合组网整体架构

北向空口接入 5G 基站。

网络层形成网络架构中“管”的部分，包含了运营商的接入网、承载网、核心网、企业部署的 MEC 设备，以及生产控制大区的调度数据网和管理信息大区的数据通信网。“管层”中部分电力业务通过 5G 边缘侧 UPF 分流到 MEC 节点终结，或通过 MEC 预处理后通过地市的专线接入“云层”应用系统，其他业务通过 5G 承载网连接的电力通信网进入“云层”应用系统。

平台层和应用层共同组成网络架构中“云”的部分，包括电网的生产控制大区、管理信息大区和互联网大区。

2.3　电力 5G 业务部署架构

5G 端到端网络切片体系由业务驱动，5G 网络切片技术将基础的物理网络逻辑分割，通过云和虚拟化技术共享同一套物理基础设施，从而为不同性能要求的业务应用提供定制化的网络服务。鉴于电网不同业务场景通信需求差异较大，混合组网模式下的 5G 网络切片架构应按业务场景重新切分。

电力 5G 业务部署架构如图 2 所示，先对电力业务按照安全大区分类，然后在大区内分别形成增强型移动宽带（enhanced mobile broadband，eMBB）、低时延高可靠通信（ultra-reliable low latency communication，uRLLC）以及大连接物联网（massive machine type of communication，mMTC）切片。eMBB 切片主要为智能电网的视频采集类应用，包括变电站巡检机器人、输电线路无人机巡检、配电房视频综合监控、移动现场施工作业管控等；uRLLC 切片主要包括配电差动保护、智能分布式配电自动化、精准负荷控制等业务；mMTC 切片主要包括分布式能源调控及高级计量两大业务。根据业务切片分类，在三大场景切片基础上，同一切片场景下对具体业务提供的切片实例服务，通过与电网各类业务平台对接，实现电力终端至主站系统的端到端切片可靠承载。

3　电力 5G 混合组网安全风险分析

5G 面临的新安全风险和挑战主要包括终端接入安全风险、边缘计算安全风险、网络通道安全风险以及核心网安全风险，下面分别对以上 4 个部分

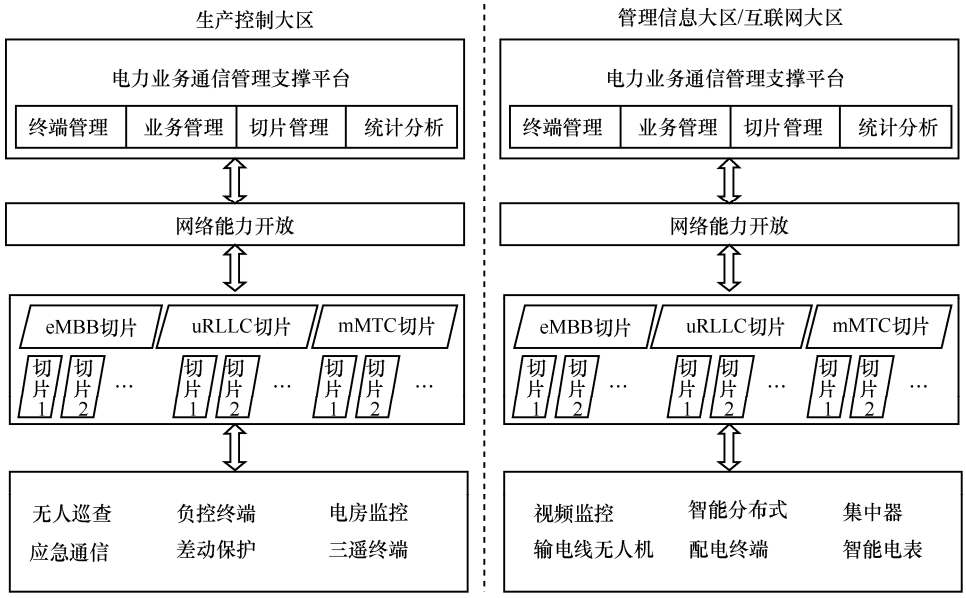

图 2　电力 5G 业务部署架构

引入的风险进行详细分析。

3.1 多业务场景带来的终端接入安全风险

智能终端的使用，不可避免地存在恶意程序、固件漏洞、窃听、篡改用户信息等威胁。除此之外，5G 高并发、大流量、低时延场景分别对接入认证协议提出了不同的要求，单纯使用通用的接入认证协议达不到三大应用场景的预期目标[14]。

（1）eMBB 场景的敏感信息泄露风险

eMBB 场景下传输速率高，涉及的用户隐私和敏感信息较多，相同应用场景下的不同业务也有不同的安全需求。eMBB 场景下的终端接入继承和扩展了 LTE 接入安全机制，接入时需要实现较高等级的认证和信息完整性保护，同时还需要保证高速率的加密能力。

（2）mMTC 场景的高并发接入风险

mMTC 场景下接入网络的终端数量巨大，但终端的安全能力较弱、功耗受限。如果终端仍然沿用传统接入方式，可能产生信令风暴造成网络拥塞；而且在接入失败的情况下，终端不断尝试重新接入网络发起认证将加速其电池消耗。攻击者可以通过恶意接入耗尽海量终端的频段资源和电池资源。因此该场景下的接入认证协议需要考虑采用轻量级、高效性和低成本方案，同时还需要保证空口传输的安全。

（3）uRLLC 场景的低防护能力风险

uRLLC 应用对通信可靠性、低时延有较高的要求，然而增强网络安全防护机制必然会以牺牲网络性能、降低网络效率为代价。uRLLC 场景下系统受攻击的后果一般较为严重，例如电力系统中低时延业务一旦受到影响甚至会威胁到生命安全；除了在接入认证时考虑高可靠低时延，超低时延的实现需要在端到端传输的各个环节进行一系列机制优化。

3.2 业务流量卸载带来的边缘计算安全风险

（1）UPF 流量卸载风险

业务流量一旦本地卸载到边缘节点后，就难以对其进行有效监测和治理；如果 UPF 配置不当，也可能会造成将 UPF 流量卸载到其他 MEC 平台的风险。

攻击者通过对某个特定 MEC 服务器卸载大量计算任务或者恶意卸载流量，造成 MEC 服务器资源过度供应，可能使其他用户服务超时，耗尽计算资源。

（2）MEC 数据卸载风险

业务流量经 MEC 应用处理后的业务数据存在因数据存储、数据传输的机密性不够造成的数据泄露风险。数据迁移和传输方面，由于在虚拟机迁移或平台间传输的过程中缺乏加密与完整性校验机制，引发数据被攻击者、非授权用户或虚拟机窃听甚至篡改的风险，且发生篡改时难以发现；数据共享方面，存在第三方非授权进行数据传播以及未采取分级分类、脱敏等手段而引发的敏感数据泄露风险。

3.3 网络切片带来的网络通道安全风险

（1）网络切片被攻击风险

在逻辑隔离的承载网切片中，一个切片超载可能引起同一物理管道中的其他虚拟切片工作异常。攻击者在访问一个切片时，可能消耗其他切片的资源导致资源不足，造成对其他切片 DDoS 攻击。

爱尔兰安全公司（Adaptive Mobile Security）报告了一种潜在的 DDoS 攻击，通过操纵基于 HTTP 的服务请求到运营商的网络存储功能（network repository function，NRF），欺骗它使其认为目标切片已经超载，不应与之联系，实现运营商网络内大量的拒绝服务攻击。

（2）网络切片接入风险

非法用户对切片进行违规操作或者合法用户以未授权的方式对切片进行操作，如仿冒攻击，都会造成对切片的非授权访问，从而影响切片的合法接入，用户无法正常进行通信，或者数据信息被拦截、窃听等。

爱尔兰安全公司报告发现，通过建立到 NRF 的安全传输层（transport layer security，TLS）协议连接请求访问同一网络里的其他切片时，NRF 不会检查请求是否为正确的切片而只检查共享网络功能，生成的令牌可能导致对切片的恶意访问。

（3）切片间的通信风险

不同网络切片之间、无线电接入网切片和核心网络切片之间都需要进行通信。在所有网间切片通信中，网络切片之间的接口可能受到攻击。另外，攻击用户面可以破坏或恶意转移用户数据，进而影响一个或多个用户设备（user equipment，UE）。

在 5G 通信信号质量较差时，5G 通信可能回落到 4G。对于只支持 5G 的基站，此时通信将直接断开；对于混合兼容 4G 的基站，当前通信状态将回落到 4G，相应地失去了 5G 条件下的切片通信功能，面临切片隔离失效的网络协议降级风险。

3.4　网络能力开放带来的核心网安全风险

5G 采用网络功能虚拟化（network function virtualization，NFV）实现了计算资源的按需部署和弹性扩缩容；采用软件定义网络（software defined network，SDN）技术实现了网络连接的虚拟化。虚拟化、服务化架构，使得核心网的物理安全边界模糊化和快速变化；同时核心网网络服务能力的开放，将进一步打破网络封闭状态，使得核心网更易遭受外部安全威胁风险，主要包括以下 3 个方面。

（1）API 拒绝服务攻击风险

网络能力开放将信息数据从运营商内部的封闭平台中开放出来，运营商对数据的管控能力减弱，可能会面临网络能力的非授权访问和使用、数据泄露等安全风险，同时攻击者还可以利用 5G 网络能力开放架构提供的 API 进行拒绝服务攻击。

（2）跨行业数据泄露风险

跨行业应用需要开放共享相应的数据信息，数据泄露的风险增大。开放网络能力给外部对手提供了更多的攻击面，使得基础设施配置易被篡改，并且也容易被内部攻击者恶意利用和篡改。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，增加了数据安全监管的难度。

（3）互联网接口协议风险

网络能力开放接口采用互联网通用协议，会进一步将互联网已有的安全风险引入 5G 网络。

3.5　电力 5G 混合组网风险整体评估

以下对每个风险进行评估计算，评价标准参照《GB/T 20984-2007 信息安全技术信息安全风险评估规范》，分为风险概率评价标准 P_n 和风险影响评价标准 E_n，安全风险整体评估根据两部分乘积的平方根得出，计算式为：

$$R=\sqrt{\sum_{n=1}^{3}a_nP_n\times\sum_{n=1}^{2}b_nE_n} \tag{1}$$

其中，R 为安全风险整体评估，风险概率由物理介入难度 P_1、实施难度 P_2 和时间消耗 P_3 加权决定，风险影响由业务数据影响 E_1 和业务设备影响 E_2 加权决定，a_n 和 b_n 分别为对应的权值，风险整体评估分级标准见表 2。对于每一个 P_n 和 E_n，由高到低可能的取值为 $\{10,6,3,1\}$。

表 2　风险整体评估分级标准

风险整体评估计算范围	风险整体评估分级结果
[7,10]	高
[5,7)	较高
[3,5)	中
[1,3)	低

电力系统和网络安全专家团队详细分析了每条风险因素，对每一条风险的各个因素进行赋值。电力 5G 混合组网风险整体评估见表 3，展示每条风险的具体内容以及它们对应的风险评价赋值、

表 3　电力 5G 混合组网风险整体评估

混合组网安全风险	具体风险内容	风险概率评价 P_n			风险影响评价 E_n		风险整体评估	风险分级
		物理介入难度 P_1	实施要求难度 P_2	时间消耗 P_3	数据影响 E_1	设备影响 E_2		
		30%	50%	20%	75%	25%		
终端接入安全风险	eMBB 场景的敏感信息泄露风险	6	3	3	6	1	4.30	中
	mMTC 场景的高并发接入风险	6	6	3	3	3	4.02	中
	uRLLC 场景的低防护能力风险	3	6	3	10	3	6.09	较高
边缘计算安全风险	UPF 流量卸载风险	1	3	1	3	3	2.45	低
	MEC 数据卸载风险	1	1	1	6	1	2.29	低
网络通道安全风险	网络切片被攻击风险	3	6	6	3	3	3.91	中
	网络切片接入风险	3	10	10	6	10	7.44	高
	切片间的通信风险	3	6	3	6	6	5.20	较高
核心网安全风险	API 拒绝服务攻击风险	3	6	6	6	3	5.17	较高
	跨行业数据泄露风险	6	6	3	6	3	5.32	较高
	互联网接口协议风险	3	6	3	6	3	4.86	中

评价计算和分级结果。

uRLLC 场景下的风险和切片接入风险需要引起关注。uRLLC 场景的安全防护，由于业务的超低时延要求，一旦受到攻击后果较为严重，依赖于高效可靠的接入认证协议，需要进一步研究轻量级认证算法和低时延多层级加密等技术。切片接入风险，由于电网业务在不同大区的安全等级差别较大，切片间的隔离受到破坏会对业务造成较大的影响，需要进一步研究网络切片安全隔离和资源分配技术。

4　结束语

首先，从电力 5G 业务的需求分析出发，提出了 5 种 5G 组网部署建设方案，并对其进行多方面的对比，分析适用于电网不同大区的建设模式；在此基础上提出了 5G 与电力通信混合组网的架构，考虑到电网不同业务场景下的通信需求差异较大，混合组网模式下的 5G 网络切片架构应按照业务场景重新切分；最后，从终端接入、边缘计算、网络通道以及核心网 4 个部分，对混合组网引入的新风险新挑战进行具体分析，在今后的研究中，还需要进一步研究轻量级认证算法、低时延多层级加密、网络切片安全隔离等关键技术，才能实现 5G 网络在行业的真正安全使用。

参考文献：

[1] SHAFI M, MOLISCH A F, SMITH P J, et al. 5G: a tutorial overview of standards, trials, challenges, deployment, and practice[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(6): 1201-1221.

[2] JABER M, IMRAN M A, TAFAZOLLI R, et al. 5G backhaul challenges and emerging research directions: a survey[J]. IEEE Access, 2016, 4: 1743-1766.

[3] ORDONEZ-LUCENA J, AMEIGEIRAS P, LOPEZ D, et al. Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges[J]. IEEE Communications Magazine, 2017, 55(5): 80-87.

[4] 王毅, 陈启鑫, 张宁, 等. 5G 通信与泛在电力物联网的融合: 应用分析与研究展望[J]. 电网技术, 2019, 43(5): 1575-1585. WANG Y, CHEN Q X, ZHANG N, et al. Fusion of the 5G communication and the ubiquitous electric Internet of Things: application analysis and research prospects[J]. Power System Technology, 2019, 43(5): 1575-1585.

[5] 王坤. 5G 时代物联网技术在电力系统中的应用[J]. 通信电源技术, 2018, 35(5): 187-188.

WANG K. The application of the internet of things in the 5G era in the power system[J]. Telecom Power Technology, 2018, 35(5): 187-188.

[6] 张亚健, 杨挺, 孟广雨. 泛在电力物联网在智能配电系统应用综述及展望[J]. 电力建设, 2019, 40(6): 1-12.
ZHANG Y J, YANG T, MENG G Y. Review and prospect of ubiquitous power internet of things in smart distribution system[J]. Electric Power Construction, 2019, 40(6): 1-12.

[7] 刘建伟, 韩祎然, 刘斌, 等. 5G 网络切片安全模型研究[J]. 信息网络安全, 2020, 20(4): 1-11.
LIU J W, HAN Y R, LIU B, et al. Research on 5G network slicing security model[J]. Netinfo Security, 2020, 20(4): 1-11.

[8] ARFAOUI G, BISSON P, BLOM R, et al. A security architecture for 5G networks[J]. IEEE Access, 2018(6): 22466-22479.

[9] 项弘禹,肖扬文, 张贤, 等. 5G 边缘计算和网络切片技术[J]. 电信科学, 2017, 33(6): 54-63.
XIANG H Y, XIAO Y W, ZHANG X, et al. Edge computing and network slicing technology in 5G[J]. Telecommunications Science, 2017, 33(6): 54-63.

[10] 王庆扬, 谢沛荣, 熊尚坤, 等. 5G 关键技术与标准综述[J]. 电信科学, 2017, 33(11): 112-122.
WANG Q Y, XIE P R, XIONG S K, et al. Key technology and standardization progress for 5G[J]. Telecommunications Science, 2017, 33(11): 112-122.

[11] 朱浩, 项菲. 5G 网络架构设计与标准化进展[J]. 电信科学, 2016, 32(4): 126-132.
ZHU H, XIANG F. Architecture design and standardization progress of 5G network[J]. Telecommunications Science, 2016, 32(4): 126-132.

[12] 李立平, 李振东, 方琰崴. 5G 专网技术解决方案和建设策略[J]. 移动通信, 2020, 44(3): 8-13.
LI L P, LI Z D, FANG Y W. The technical solutions and construction strategies for 5G private networks[J]. Mobile Communications, 2020, 44(3): 8-13.

[13] 李良, 谢梦楠, 杜忠岩. 运营商 5G 智能专网建设策略研究[J]. 邮电设计技术, 2020(2): 45-50.
LI L, XIE M N, DU Z Y. Research on construction strategy of operators' 5G intelligent private network[J]. Designing Techniques of Posts and Telecommunications, 2020(2): 45-50.

[14] 闫新成, 毛玉欣, 赵红勋. 5G 典型应用场景安全需求及安全防护对策[J]. 中兴通讯技术, 2019, 25(4): 6-13.
YAN X C, MAO Y X, ZHAO H X. Security requirements and protection countermeasuresy for typical 5G application scenarios[J]. ZTE Technology Journal, 2019, 25(4): 6-13.

[作者简介]

张小建（1969− ），男，现就职于全球能源互联网研究院有限公司，主要研究方向为电网信息、通信网络安全技术。

费稼轩（1984− ），男，现就职于全球能源互联网研究院有限公司，主要研究方向为电力工控安全。

姜海涛（1985− ），男，博士，国网江苏省电力有限公司电力科学研究院高级工程师，主要研究方向为电力系统网络与信息安全。

姚启桂（1983− ），男，全球能源互联网研究院有限公司高级工程师，主要研究方向为电力工控系统网络安全。