5G“云网边端”一体化纵深安全防护体系研究及应用

张国新

（中国电信股份有限公司广东分公司，广东 广州 510081）

摘　要：创新地提出了一种 5G“云网边端”一体化纵深安全防护实现方案，探索了 5G 定制网的网络安全防护体系，介绍了体系的基本架构、特性、实现方案和应用效果。在实现方案中重点介绍了两个要点：通过部署 5G“云网边端”4 个方面的安全系统，形成多层次、多维度的安全防护能力；建立适配体系的运营流程，包含一键加固、安全防御、态势感知和一键应急 4 个部分。最后给出了 5G“云网边端”一体化纵深安全防护体系的实际应用效果。

关键词：5G；云网边端；一体化；可信终端；端到端

中图分类号：TN918.91

文献标志码：A

doi: 10.11959/j.issn.1000–0801.2022276

Research and application of 5G cloud-network-edge-end integrated in-depth security protection system

ZHANG Guoxin

Guangdong Branch of China Telecommunications Co., Ltd., Guangzhou 510081, China

Abstract: A 5G cloud-network-edge-end integrated in-depth security protection implementation scheme was innovatively proposed, the network security protection system of 5G customized network was explored, and the basic architecture, characteristics, implementation scheme and application effect of the system were introduced. In the implementation plan, two key points were emphasized. Firstly, by deploying the security system of the four aspects of the 5G cloud network, the edge and the end, the multi-level and multi-dimensional security protection capability was formed. Secondly, the operation process of the adaptation system, including one-key reinforcement, security defense, situational awareness and one-key emergency response was established. Finally, the practical application effect of the 5G cloud-network-edge-end integrated in-depth security protection system was given.

Key words: 5G, cloud-network-edge-end, integration, trusted terminal, end-to-end

0　引言

随着新基建战略的深入和 5G 网络的规模部署，5G 与经济社会各领域的融合应用不断深化，行业数字化转型升级进入新阶段。2020 年 11 月 7 日，中国电信全新发布“网定制、边智能、云协同、应用随选”的 5G 定制网解决方案，实现对连接、计算、智能等全部数字化能力的“融合定制”，为行业客户提供安全可信、自主可控的专用信息化基础设施，将成为企业数字化转型升级的基石和加速器[1]。

收稿日期：2022–04–20；修回日期：2022–10–14

5G 作为关键基础设施和数字化的重要基石，5G 的安全关系到应用领域的安全。随着中国电信 5G 定制网业务的不断落地，5G 核心网的用户面功能（user plane function，UPF）开始下沉，5G 核心网的重要网元直接暴露在客户侧，这将带来前所未有的安全风险。另一方面，5G 核心网采用了新的架构，也引入了新的风险点。5G 业务发展，安全先行，本文提出了 5G“云网边端”一体化纵深的安全防护体系思路，填补了 5G 网络安全防护体系的空白，并且在指导行业开展 5G 行业应用过程中，落实安全三同步（同步规划、建设、维护），确保 5G 业务安全可靠，提升 5G 行业应用安全能力[2]。

1　5G 网络安全风险分析

与 4G 相比，5G 核心网采用了颠覆性的设计，融入云原生思想，采用服务化架构，并引入网络切片、网络能力开放等技术，进一步实现控制面及用户面（controlplane & userplane，CU）分离，不仅对传统 4G 核心网网元网络功能虚拟化（network functions virtualization，NFV），还进一步将网络功能软件模块化，核心网网元共享计算、存储和网络资源，使安全边界模糊化、安全能力动态化、安全要求差异化多样化。5G 网络“云网边端”的安全风险如图 1 所示。

（1）云：5G 行业应用平台云化的安全风险

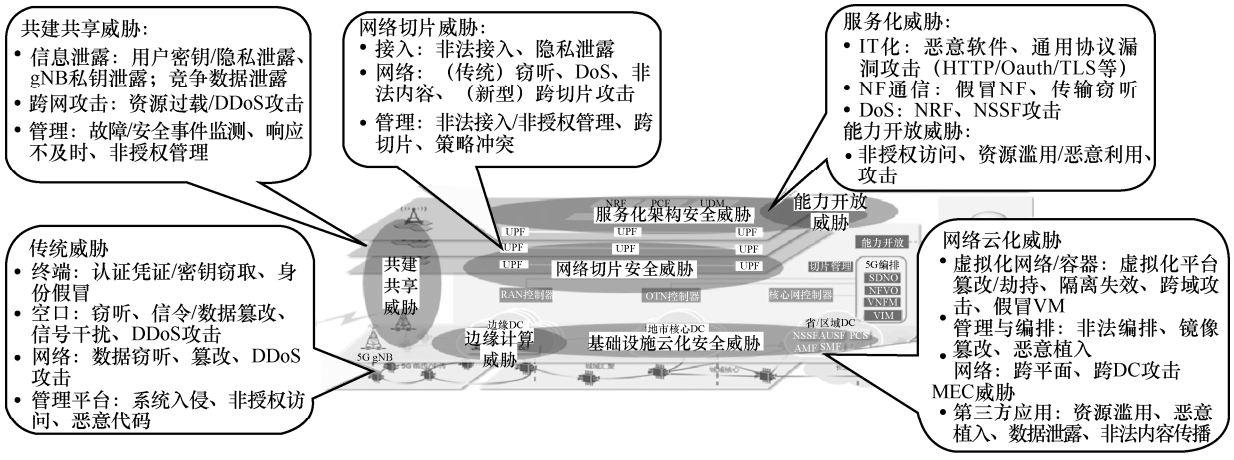
越来越多 5G 行业的应用平台开始云化，将传统封闭的生产应用和内部数据上云，促使 5G 行业的应用平台不断对互联网开放。5G 行业应用平台的流量会通过互联网进行传输，使得 5G 行业应用平台的生产实时应用和供应链管理等服务都面临着日益增多的安全威胁。

（2）网：新技术、新业务、新协议带来的各种风险

5G 核心网采用的服务化架构带来的恶意软件，通用协议漏洞攻击、假冒 NF、传输窃听等威胁，以及网络切片的非法接入、窃听、跨切片攻击等威胁，造成 5G 企业用户网络异常或信息泄露的风险。

（3）边：5G 共建共享及 5G 定制网扩大了安全风险

5G 共建共享带来信息泄露、跨网攻击等威胁；5G 实践应用中使用边缘计算能力，边缘节点 UPF 和 MEC 等会下沉到网络边缘或用户机房，边缘计算平台上部署第三方应用，应用的安全管理、设备



注：gNB（the next generation node B，下一代基站）
DDoS（distributed denial of service，分布式拒绝服务）
HTTP（hyper text transfer protocol，超文本传输协议）
TLS（transport layer security，传输层安全）
NRF（network repository function，网络存储功能）
NSSF（network slice selection function，网络切片选择功能）
VM（virtual machine，虚拟机）
DC（data center，数据中心）
NF（network function，网络功能）
MEC（multi-access edge computing，多接入边缘计算）

图 1　5G 网络“云网边端”的安全风险

的安全管理将会影响 5G 的安全[3]。

（4）端：5G 支持大连接，终端数量多易引发局部或全部规模攻击的风险

5G 网络支持终端连接密度为 $10^6/km^2$，大量终端由于应用原因、网络抖动或受黑客控制，突发性大规模接入或重连，可能引发信令风暴或 DDoS 攻击，海量终端同时发起流量攻击，更可能超越甚至击垮网络防御能力和体系，造成 5G 网络服务异常的风险[4]。

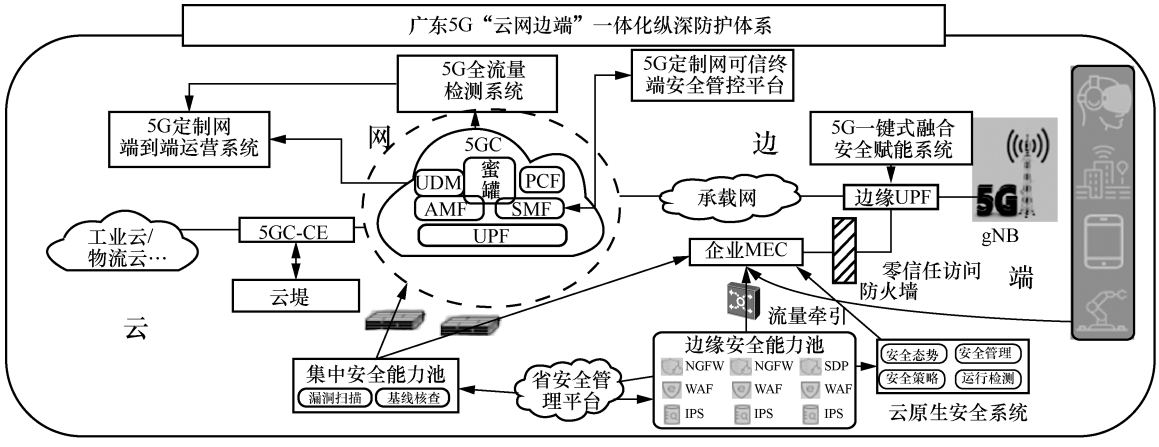
2　总体设计

本文提出了 5G“云网边端”一体化纵深安全防护体系，以端到端的安全运营为底座，以 5G 行业应用为防护核心目标，从云、网、边和端 4 个方面对 5G 定制网的网络安全进行一体化、内生化和智能化的防护，5G“云网边端”一体化纵深安全防护体系示意图如图 2 所示。图 2 的中间部分，从右到左，从 gNB 到工业云，是一个完整的 5G 定制网网络，外围是安全防护能力，共同组成“云网边端”一体化纵深防护体系。云是指企业的工业云/物流云，提供 5G 应用；网指的是 5G 核心网、承载网、基站及 5G 网络切片；边是指 UPF 和 MEC，用于实现 5G 终端的低时延访问；端是 5G 终端，通过自带 5G 模块或者 5G 客户前置设备（customer premise equipment，CPE）接入 5G 网络[5]。

2.1　体系架构

体系各部分的防护能力介绍如下。

- 云：云平台容易遇到 DDoS 流量攻击，为此加载了中国电信云堤系统的抗 DDoS 能力。中国电信云堤系统是国内唯一一个运营商级别的抗 DDoS 系统，可以防御已知所有 DDoS 流量。
- 网：引入 5G 全流量检测系统，建立 5G 信令面流量检测的专有模型；对接异常流量监测系统，实时监测工业企业的 5G 终端用户面流量，联合云堤系统进行清洗防护[6]。
- 边：提供了集中和边缘两种安全能力资源池，可以为电力、能源、医疗等客户按需提供各种服务。集中模式包含漏洞扫描、基线核查等，边缘模式包含 IPS、NGFW、防火墙



注：UDM（unified data management，统一数据库）
PCF（policy control function，策略决策功能）
AMF（access and mobility management function，接入和移动性管理网络功能）
SMF（session management function，会话管理网络功能）
5GC-CE（5G core network CE，5G核心网路由器）
NGFW（next generation firewall，下一代防火墙）
SDP（software defined perimeter，软件定义边界）
WAF（web application firewall，网站应用防火墙）
IPS（intrusion prevention system，入侵防御系统）

图 2　5G“云网边端”一体化纵深安全防护体系示意图

等虚拟化安全防护能力[7]。

- 端：部署了 5G 定制网可信终端安全管控平台，通过绑定设备信息和卡号信息，对终端和卡号进行严格鉴权，从而消除终端和卡号的盗用风险。

最后，还部署了 5G 定制网端到端运营系统，采集“云网边端业安”6 个维度的信息，实现多维度视图满足多层次需求，一屏展现 5G 定制网网络的运行全景。

2.1.1 云堤系统

云堤系统是中国电信首创的“运营商级”云网协同抗 DDoS 平台，也是国内唯一全球化部署的分布式近源防护抗 DDoS 平台，将 DDoS 的攻击流量遏制于“网络攻击源头”，真正实现了“互联网专线+抗 DDoS=一条永不拥塞的互联网通道”。

云堤系统在海外有 10 个防护节点，在国内有 26 个省会节点，清洗能力和带宽储备全国第一，具备 1 000 余台的核心路由器调度能力，拥有 36 组清洗节点的分布式近源防护能力，国内唯一实现了 1.3 万个中继接口、2.2 万个边界接口关联性流量监控分析的能力。

2.1.2 5G 全流量检测和新一代蜜罐

5G 全流量检测系统具备 5G 信令面和管理面的解析识别能力，应支持 5G 信令面和管理面的全量流量接入和分析，流量包括 5G 核心网的各个接口和专用协议流量、综合网管、采控平台等网管系统的管理流量、软件定义网络（software defined network，SDN）的管理流量、安全设备的管理流量、堡垒机等登录设备和操作的流量。

（1）5G 核心网业务威胁识别能力

- 信令风暴：对用户的接入 AMF 网元的日志进行分析，判断上下行流量是否对称、信令接入和释放频率是否正常，以此判断是否存在信令风暴异常。
- 网元间异常访问：将信令日志与流量日志结合，得到全部网元信息列表，形成网元间访问矩阵基线，当出现不在访问矩阵中的异常数据时，触发生成告警。
- 切片安全检测：通过监测网络切片的全生命周期，分析并识别切片运行异常行为，及时发现隔离失效、非法访问/越权管理等安全事件[8]。

（2）新一代蜜罐的 5G 核心网仿真能力

新一代蜜罐要求能提供良好的 5G 核心网仿真交互能力，以更好地欺骗攻击者，能对被诱捕过来的攻击行为进行隔离，通过隔离攻击对目标进行防护，从而实现 5G 网络纵深的安全防御。新一代蜜罐部署在和 5G 核心网相同的网络，对真实网元（UPF、AMF 等）进行虚拟，并进行信令层面的真实交互。新一代蜜罐包括但不限于 AMF/UPF/PCF/UDM，更加贴合 5G 核心网的真实环境。

2.1.3 5G 定制网可信终端安全管控平台

可信终端安全管控平台的认证授权计费（authentication authorization accounting，AAA）服务和 5G 核心网的 SMF/UPF 对接，通过 AAA 的鉴权能力完成企业 5G 终端的自主鉴权流程，实现 5G 定制网的终端“可信可控”，保障 5G 定制网终端的安全接入。

可信终端管控平台为客户提供自服务门户和 5G 定制网接入两大应用，具备四大核心功能，包括七码绑定（设备号/内网 IP/账号/密码等）、基站绑定、定向访问和用户流量行为分析。

2.1.4 5G 定制网端到端运营系统

5G 定制网端到端运营系统可以实现终端、无线网、承载网、核心网、MEC 和天翼云的端到端拓扑可视，切片质量管控等业务服务等级协定（service level agreement，SLA）监控管理信息，并开放能力接口，按需向企业转发 6 个维度的监控信息。

5G 定制网端到端运营系统面向运营商和客

户提供以下两类视图。

- 面向运营商视图从传统的多专业分散，转变为面向客户的云、网、端、边、终端和业务“五位一体”可视化运营，一屏管控，实现业务 SLA 实时差异化保障。
- 面向客户视图的能力统一对外开放，深度融合客户生产系统，满足客户自主运营的诉求。

2.1.5　5G 定制网一键式融合安全赋能系统

5G 定制网一键式融合安全赋能系统可以实现 5G 定制网 UPF 的快速安全加固和交付。系统参照国家等保 2.0 三级的标准[9]，特别是“安全通信网络”“安全区域边界”和“安全计算环境”的“可信验证”控制项和具体控制点，统一 5G 网络主机安全加固的标准，主要包括基线加固、访问控制和日志审计接入。系统各模块的功能包含系统基线检测、输出基线检测报告、基线安全加固、基线加固回退和人机交互模块。

系统有 4 个创新点：一是全面性，5G 加固实现了全面统一，涵盖了基线规范、访问控制列表（access control list，ACL）白名单、高危端口封堵和终端响应防护等一系列安全要求；二是便捷性，使用 shell 语言编程，实现用户一键式操作、融合多功能、运维可视化、加固前后的风险可对比，并自动备份，提供安全回退功能；三是轻量级，简易部署后以 SHELL 文件运行，主机资源占用很少；四是高解耦可扩展，适配主流开源 Linux 框架，同时兼容华为、中兴的定制版操作系统，测试驱动型开发，功能易扩展。

2.2　运营流程

运营流程以 5G 网络安全智能运营目标为导向，在 5G 网络自身安全基础上通过对人、流程、技术与数据的综合研判，把握安全风险管控和攻防对抗总纽带，建立一键加固、安全防御、态势感知和一键应急等手段，实现 5G 网络信令面、用户面及管理面的攻击流量检测、对入侵途径及攻击者的研判与溯源，以及 5G 业务异常的分析判断，并快速进行应急处置，采用数据驱动并具有高度自动化水平，有效提升 5G 网络安全的防护能力。5G“云网边端”一体化纵深安全防护体系的运营流程如图 3 所示。

各模块的功能点说明如下。

- 一键加固：通过 5G 定制网一键式融合安全赋能系统，实现 5G 核心网网元的基线、时钟及主机 ACL 的自动化一键加固，提高安全加固效率，加快 5G 定制网业务的交付。
- 安全防御：引入 5G 全流量检测、5G 可信终端安全管控、新一代蜜罐等安全系统和设备，通过流量采集、监测、分析和网络攻击检测，以及攻击流量诱捕，实现 5G 终端的精细化管控、5G 核心网出口的访问控制、内外网的纵深一体化安全检测、5G 信令面及管理面的威胁分析、5G 用户面异常攻击流量的监测，以及安全攻击的溯源取证。
- 态势感知：统一将 5G 相关安全系统或设备的告警日志输出到 5G 定制网端到端运营系统，并从资产、威胁手段、时间和攻击效果等多维度进行人工智能研判，判断威胁的真实性，确认攻击者的意图，对于不同网元发起的攻击行为，设置不同优先等级，特别是 5G 定制网 UPF 或 MEC 的异常日志，应生成优先级别较高的告警信息[10]。
- 一键应急：根据 5G 定制网端到端运营系统以及云堤广东节点判定的攻击信息，进行应急处置。由云堤清洗 DDoS 攻击流量，在 5G 核心网一键隔离异常网元，对失陷的资产进行一键业务屏蔽，对于设备不具备自动化联动的情况，应生成工单，利用工单管理工作流的能力，人工实现对威胁的离线处置。

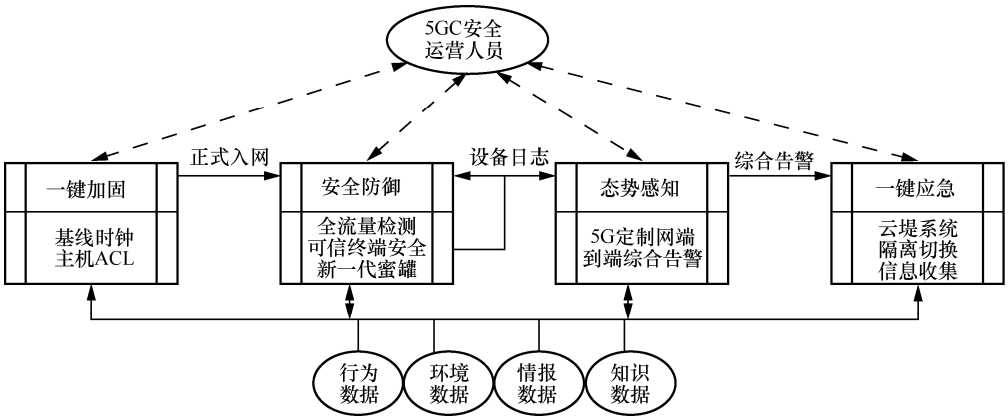


图 3　5G“云网边端”一体化纵深安全防护体系的运营流程

各种数据说明如下。

- 环境数据图，如 5G NFV、5G 切片编号、用户信息、云化管理架构信息等。
- 行为数据图，如 5G 全流量检测系统的告警日志、蜜罐日志、防火墙日志等。
- 情报数据图，5G 全流量检测系统的各类外部威胁情报。
- 知识数据图，各类常见的攻击模型知识库等。

3　应用效果

目前，已经在广东电信现网试运行 5G“云网边端”一体化纵深安全防护体系，取得了良好成果。综合来看，5G“云网边端”一体化纵深安全防护体系是可行的，可以有效提升包括智能化加固、一体化防御、全景化感知和闭环化处理的 5G 安全防护能力。

3.1　云堤和 5G 全流量检测系统等防护系统

5G 全流量检测系统每天实时采集超过 10 Gbit/s 流量，解析生成几十亿条日志，发现疑似信令风暴、异常网元访问和切片长时间未被访问的攻击行为，经核实原因是终端适配不成功、外省网元访问和切片配置失效。在 5G 信令面网络部署了新一代蜜罐设备，云堤广东节点已经开始对 5G 网络的异常大流量进行监控，运行至今，未发现访问蜜罐的恶意行为和异常大流量的攻击行为。省态势感知平台采集了 5G 安全设备的数据，综合研判后输出告警并派单处理，已完成多条告警信息的闭环处理。

3.2　5G 定制网可信终端安全管控平台

5G 定制网可信终端安全管控平台自上线以来，实现“七码一体”绑定、物理位置区域绑定、定向流量等诸多功能。平台已在深圳警务等项目试点，获得深圳公安部门的高度认可，满足政府部门对网络安全的高等级防护要求。未来将在更大范围推广，实现客户的 5G 终端可信安全接入。

3.3　5G 定制网端到端运营系统

5G 定制网端到端运营系统已有 200 多项功能上线，与七大系统 16 个接口对接，日数据量超过 10 亿级，覆盖广东等 22 个标杆项目，服务响应从小时级缩短至分钟级，为美的等 5G+智能制造多个龙头企业提供专属的定制网服务。客户可以快速获知当前业务状态、流量信息等信息，也可以对接企业态势感知平台进行闭环处理，互通关键信息实现安全共治。

3.4　5G 定制网一键式融合安全赋能系统

5G 定制网一键式融合安全赋能系统在广东省多个分公司进行了推广，提升了分公司安全加固的效率，受到分公司的好评。

广东省有多个分公司的 UPF 和虚拟机应用本项目，广东省分公司的应用推广率超过 80%，物理机使用率超过 80%。广东省积极参与项目转化及成

果升级，共上报 19 份详细的使用测试报告，提出 11 项改进建议，参与超过 6 项代码或功能模块开发，分公司的创新开发参与度高、推广效果显著，大大提升了分公司 5G 定制网安全交付的效率。

5G 定制网一键式融合安全赋能系统是中国电信进行安全核心能力技术攻关的有益尝试，显著提升定制网交付的工作效率，在全国范围内具备较好的推广应用价值。

3.5 运营效果

为确保 5G 安全防护体系运营流程的有效性，已开展多次 5G 网络安全防护的应急演练，检验了 5G“云网边端”一体化纵深安全防护体系的有效性，确保 5G 网络关键基础设施能够应对国内外的非法安全攻击。

2022 年开展的应急演练包括：模拟外网对 5G 网络发起了 DDoS 大流量攻击以及渗透攻击，对某个 5G 网络 UPF 节点的访问瞬间流量超过 10 bit/s，通过云堤广东节点实施一键应急清洗，UPF 节点网络流量恢复正常；对某个 MEC 和 UPF 进行渗透，尝试通过 UPF 接口非法越权访问切片用户的流量，通过全流量检测发现并实施一键隔离和溯源取证，恢复 MEC 和 UPF 运行正常。

4 结束语

5G 应用扬帆，安全先行，网络安全是 5G 业务发展的基石。本文在深入分析 5G 网络在“云网边端”4 个维度风险的基础上，创新提出了 5G“云网边端”一体化纵深的安全防护体系，部署了 5G 定制网可信终端安全管控平台等多个安全能力系统，并且和 5G 行业客户合作落地，助力 5G 行业客户加速数字化转型，获得行业客户的高度认可。

5G“云网边端”一体化纵深防护体系不仅提升了 5G 网络安全核心防护能力，符合国家安全监管的等保 2.0 三级标准，实现了 5G 网络安全运营要求，还满足了企业用户对 5G toB 切片安全等安全诉求，在全国范围内具备借鉴和推广的价值。

参考文献：

[1] 中国电信. 中国电信 5G 定制网产品手册（2020 发布版）[R]. 2020.
China Telecom. China Telecom 5G customized network product manual (Version 2020)[R]. 2020.

[2] 张滨. 5G 边缘计算安全研究与应用[J]. 电信工程技术与标准化, 2020, 33(12): 1-7.
ZHANG B. Research and application on the 5G edge computing[J]. Telecom Engineering Technics and Standardization, 2020, 33(12): 1-7.

[3] RAMEZAN A, ABDELNASSER B, LIU W. et al. EAP-ZKP: AZero-knowledge proof based authentication protocol to prevent DDoS attacks at the edge in beyond 5G[C]//Proceedings of 2021 IEEE 4th 5G World Forum (5GWF). Piscataway: IEEE Press, 2021: 259-264.

[4] IASHVILI G, IAVICH M, BOCU R, et al. Intrusion detection system for 5G with a focus on DOS/DDOS attacks[C]//Proceedings of 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Piscataway: IEEE Press, 2021: 861-864.

[5] YUAN J, ZHANG F, YU L, et al. Research of security of 5G-enabled industrial Internet and its application[C]//Proceedings of 2021 IEEE Conference on Telecommunications, Optics and Computer Science. Piscataway: IEEE Press, 2021: 428-435.

[6] YAN W F, SHU Q, GAO P. Security risk prevention and control deployment for 5G private industrial networks[J]. China Communications, 2021, 18(9): 167-174.

[7] ZHANG X J, FEI J X, JIANG H T, et al. Research on power 5G business security architecture and protection technologies[C]//Proceedings of 2021 6th International Conference on Power and Renewable Energy (ICPRE). Piscataway: IEEE Press, 2021: 913-917.

[8] MATHEW A. Network slicing in 5G and the security concerns[C]//Proceedings of 2020 4th International Conference on Computing Methodologies and Communication (ICCMC). Piscataway: IEEE Press, 2020: 75-78.

[9] 全国信息安全标准化技术委员会. 信息安全技术网络安全等级保护基本要求[R]. 2019.
National Information Security Standardization Technical Committee. Information security technology -- Basic requirements for classified protection of network security[R]. 2019.

[10] 韩洁, 钟逸铭, 陈明亮. 电力行业网络安全态势感知分析[J]. 软件, 2022, 43(5): 128-130.
HAN J, ZHONG Y M, CHEN M L. Analysis of network security situation awareness in power industry[J]. Software, 2022, 43(5): 128-130.

[作者简介]

张国新（1968– ），男，博士，中国电信股份有限公司广东分公司副总经理，中国电信集团有限公司科学技术委员会委员，长期从事通信网络、云计算、大数据、网络安全、企业数字化等专业规划建设及运营工作。