

# 5G MEC 安全评估体系与方法研究

卢秋呈[1,2]，唐金辉[2]，鲍聪颖[3,4]，吴昊[4]，伏玉笋[2]

（1. 上海交通大学宁波人工智能研究院，浙江 宁波 315000;
2. 上海交通大学电子信息与电气工程学院，上海 200240;
3. 宁波市永耀电力投资集团有限公司，浙江 宁波 315099;
4. 国网浙江省电力有限公司宁波供电公司，浙江 宁波 315016）

**摘　要：**多接入边缘计算（multi-access edge computing，MEC）部署在网络边缘，在实现移动网络中高效、快速的数据处理的同时，还承担着重要的安全功能，这使得 MEC 成为攻击者的主要目标。因此，MEC 节点将面临巨大的安全风险，如何准确地评估、量化 MEC 安全能力是迫切需要解决的课题。为了准确地评估、量化 MEC 安全能力，结合 MEC 安全风险提出了 MEC 安全评估体系，该评估体系选取的评估指标较为全面地反映了 MEC 的基本特性，体现了其完整的安全能力。基于此评估体系，利用层次分析法（analytic hierarchy process，AHP）和模糊评价设计了 MEC 安全评估方法，创新性地提出了 MEC 漏洞评分系统，并参考该系统的结果给出指标评价，最终计算出 MEC 安全能力量化值。实例结果证明了方法的有效性。

**关键词：**5G MEC；安全评估体系；漏洞评分系统；层次分析法；模糊评价

**中图分类号：**TP309

**文献标志码：**A

**doi:** 10.11959/j.issn.1000−0801.2023152

# Research on 5G MEC security assessment system and method

LU Qiucheng[1,2], TANG Jinhui[2], BAO Congying[3,4], WU Hao[4], FU Yusun[2]

1. Ningbo Artificial Intelligence Institute of Shanghai Jiao Tong University, Ningbo 315000, China
2. School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
3. Ningbo Yongyao Power Investment Group Co., Ltd., Ningbo 315099, China
4. State Grid Zhejiang Electric Power Co., Ltd. Ningbo Power Supply Company, Ningbo 315016, China

**Abstract:** Multi-access edge computing (MEC) is deployed at the edge of the network, enabling efficient and fast data processing in mobile networks, while also undertaking important security functions, making MEC a prime target for attackers. Therefore, MEC nodes will face huge security risks. How to accurately evaluate and quantify MEC security capabilities is an urgent issue to be solved. For accurately evaluating and quantifying MEC security capabilities,

**收稿日期：**2023−05−29；**修回日期：**2023−08−05

**通信作者：**伏玉笋，fu_yusun@sina.com

**基金项目：**国家重点研发计划项目（No.2019YFB1705703）；宁波市重大科技任务攻关资助项目（No.2021Z022）；宁波市永耀电力投资集团有限公司资助项目（No.NBGC21P05A-0926-41）

**Foundation Items:** The National Key Research and Development Program of China (No.2019YFB1705703), The Major Scientific and Technological Research Program of Ningbo (No.2021Z022), The Research Program of Ningbo Yongyao Power Investment Group Co., Ltd. (No.NBGC21P05A-0926-41)

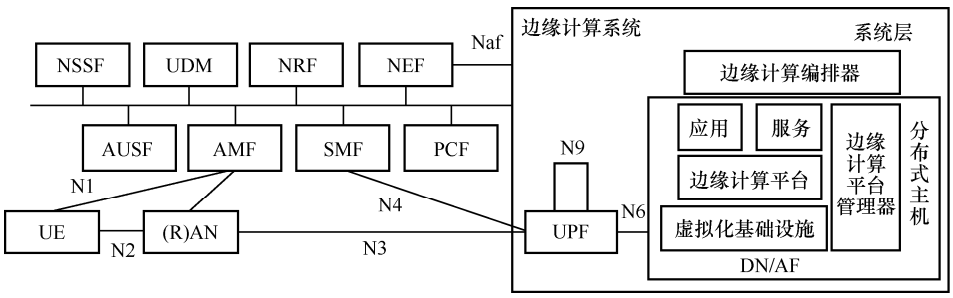
the MEC safety assessment system was proposed in combination with MEC safety risks. The assessment indicators selected in the assessment system comprehensively reflect the basic characteristics of MEC and its complete safety capability. Based on this evaluation system, the MEC security evaluation method was designed by using the analytic hierarchy process (AHP) and fuzzy evaluation, the MEC vulnerability scoring system was creatively proposed, and the evaluation indicators were provided based on the results of MEC vulnerability scoring system, the MEC security capability quantification value was finally calculated. The experimental result proves the effectiveness of the method.

**Key words:** 5G MEC, security assessment system, vulnerability scoring system, AHP, fuzzy evaluation

## 0 引言

伴随着云计算、软件定义网络（software defined network，SDN）和网络功能虚拟化（network functions virtualization，NFV）等技术的发展，5G网络使用新的技术框架，以超可靠、低时延的特性满足宽带接入、用户和设备移动性及海量设备的连接性需求[1]。多接入边缘计算（multi-access edge computing，MEC）是5G网络转型的关键技术，MEC在设备边缘与数据中心之间架起了桥梁，将云计算的相关能力，包括数据计算、存储、网络能力扩展到移动网络的边缘，通过5G切片技术使不同用户的边缘数据与MEC能够进行隔离通信[2]，实现移动网络中高效、快速的数据处理，以满足超高清视频流、虚拟现实/增强现实、工业物联网[3]、车联网[4]、机器类通信[5]业务发展的需要。

5G MEC网络架构如图1所示[6-7]，SDN将网络控制面和用户面分离，并将网络控制集中到基于软件的控制平台，简化了网络控制、管理和操作[8]。其中，边缘计算系统包含用户面功能（user plane function，UPF）、分布式主机和边缘计算编排器。分布式主机搭建在虚拟化基础设施上，虚拟化基础设施承载着边缘计算平台、应用和服务，边缘计算平台实现数据网络（data network，DN）功能和应用功能（application function，AF）；边缘计算平台管理器负责边缘计算平台的资源配置、数据监控等工作；边缘计算编排器负责UPF、边缘计算平台管理器的编排管理。在控制面中，5G核心网网元接入和移动性管理功能（access and mobile management function，AMF）主要负责注册管理、连接管理、接入性管理、移动性管理，以及安全和访问管理和授权等功能；会话管理功能（session management function，SMF）负责




NSSF：（network slice selection function，网络切片选择功能）
UDM：（unified data management，统一数据管理）
NRF：（NF repository function，网络存储功能）
NEF：（network exposure function，网络开放功能）
AUSF：（authentication server function，认证服务器功能）
PCF：（policy control function，策略控制功能）
UE：（user equipment，用户设备）
(R)AN：（(radio) access network，（无线电）接入网）

图1 5G MEC网络架构

IP 地址分配和管理、策略实施等。UPF 衔接起 5G 核心网、MEC 和终端设备，实现流量控制、数据路由及边缘设备的移动性管理。

5G MEC 部署在无线电接入网边缘侧，为垂直行业应用场景修建了一条“快车道”，通过边缘节点就近为用户提供计算和网络资源，实现信息技术和云计算能力，用户数据在边缘侧就能得到及时处理，使其具备超低时延、超大带宽等特性。同时，MEC 提供了一个开放的边缘平台，以较高的灵活性允许授权的第三方按需接入，使用其存储和处理能力[9]，MEC 已展示出广泛的应用前景。但同时，MEC 也面临着巨大的安全挑战，是攻击者的目标。除了传统云平台面临的数据、虚拟化安全问题[10]，MEC 还因其部署特性面临特有的安全挑战，涉及自身的安全挑战包括 MEC 硬件、MEC 平台、MEC 应用安全风险，涉及 5G 网络的安全挑战包括用户面、控制面、能力开放及编排管理安全风险。准确地量化 MEC 安全能力成为迫切需求。MEC 安全研究成为热点，从 MEC 安全风险分析到 MEC 安全能力部署方案探讨[11]，再到边缘服务器的可信度量研究[12]，鲜有关于 MEC 安全评估的研究，缺乏应用于 5G MEC 的安全评估体系与方法。传统云平台安全评估体系[13]的评估指标未能涵盖 5G MEC 特有的威胁向量，不能准确量化 MEC 安全能力，无法直接应用于 MEC 安全评估。因此，一套为 5G MEC 量身定做的安全评估体系成为迫切需求，MEC 安全评估体系需要考虑 5G 网络的特征，包括接入网、控制面与用户面的安全需求。为了体现其真实安全能力值，评估指标要具备全面性和完备性，能够体现 MEC 的基本特征，且囊括 MEC 存在的安全风险；同时，评估指标若选取过多，会导致其权重计算量过大，在牺牲计算资源的同时还会给评估结果带来偏差。

因此，如何准确地评估、量化 MEC 的安全能力是当前最具挑战性的课题之一。在此背景下，本文提出了一套 5G MEC 安全评估体系，基于该评估体系设计了一种 5G MEC 安全评估方法，该方法利用层次分析法（analytic hierarchy process，AHP）计算评估体系中各项指标的权重，再结合模糊论对 MEC 节点进行评价，使用安全评估结果量化了 MEC 安全能力。

模糊评价主观性较强，为了能够更客观、准确地评估各项指标，需要有一定的参考。漏洞评分是一种思路，专家们在评价时可以参考具体漏洞的评分对相应指标进行评估。为了更加契合 5G MEC 特定的安全需求，需要为其量身打造一套漏洞评分系统。目前信息安全领域中对漏洞的评估方法以通用漏洞评分系统（common vulnerability scoring system，CVSS）为主，CVSS 采用基础、生命周期和环境 3 组指标描述软件漏洞的不同方面的严重性程度，3 组指标分别刻画了漏洞的基本分数、暂时分数和环境分数[14]。其中，基础指标描述软件漏洞的固有特征，反映漏洞本身的严重性，是 CVSS 评分里最重要的一个指标，CVSS v3.1 使用攻击途径、机密性、可用性、攻击复杂性等 8 组基础指标对漏洞进行风险评估。但是，CVSS 标准中的量化评估标准更加侧重信息安全，且未能基于不同安全需求对漏洞进行评估，例如，对于超高可靠低时延通信业务，某个漏洞对于它的机密性和可用性来说非常关键，但对于攻击复杂性却不然。

面对 CVSS 存在的问题，产业界根据不同的应用场景，提出了不同的新型漏洞评估体系。陶耀东等[15]考虑工业背景，综合工业场景下特定安全需求和 CVSS 基础指标，提出了一种工控漏洞评分系统（industrial vulnerability scoring system，IVSS）。IVSS 在 CVSS 的基础上加入了更能体现工控安全特性的指标：可见性和可控性。

李舟等[16]基于软件即服务（software as a service，SaaS）云平台，为了量化云服务安全性，考虑云服务中业务场景的服务间相关性，用特定

业务的安全需求综合评估漏洞的危害程度，设计了面向云平台的安全漏洞评分系统 VScorer。VScorer 在实际服务场景进程中的漏洞评分比 CVSS 更加出色。

5G MEC 基础设施承载在容器、虚拟机之上，MEC 平台涉及域名系统（domain name system，DNS）解析处理，MEC 将其能力对外开放，将业务能力和网络能力通过开放应用程序接口（application program interface，API）的方式给用户使用，MEC 应用涉及包括 DNS、文件传送协议（file transfer protocol，FTP）、超文本传送协议（hypertext transfer protocol，HTTP）、简单邮件传输协议（simple mail transfer protocol，SMTP）在内的各类协议。从中国国家信息安全漏洞库收集涉及容器/虚拟机、DNS 服务器、FTP、HTTP、SMTP 的漏洞信息，该漏洞库包含漏洞编号、危害等级、漏洞类型等具体指标。基于漏洞数据库的收集和创建，本文创新性地提出了 MEC 的漏洞评分系统（MEC vulnerability scoring system，MVSS），该系统包含针对 5G MEC 的漏洞基础指标量化表及漏洞评分规则。其中，MVSS 基础指标除了沿用了 CVSS 中的漏洞利用、范围和影响三大指标，还制定了更加贴合 5G MEC 特定业务场景的安全、时延需求指标；MVSS 的漏洞评分规则能够更加灵敏、准确地感知安全、时延需求的不同带来的漏洞危害程度的变化。该评分系统的评分结果可作为指标评价的重要参考。

## 1 基于 5G MEC 安全风险的安全评估体系建立

本节结合 MEC 网络架构分析 5G MEC 存在的安全风险，并由此指定评估指标，最终完善为一套全面、完备的 5G MEC 安全评估体系。根据 5G MEC 网络架构，其主要面临 MEC 硬件、控制面、用户面、虚拟化、MEC 平台、应用和管理面 7 个方面的安全风险[17-18]，这 7 个方面较为全面地体现出 MEC 的基本特征，七大风险也囊括了传统安全需求和 5G MEC 特定安全需求，具有一定的完备性。下面将基于对 5G MEC 安全风险的分析，设计相应的安全评估指标。

（1）硬件安全风险

MEC 部署在网络边缘，这样的中心数据机房靠近用户，往往无人值守，且处于相对开放的环境中，安全性较差，易遭受攻击者物理破坏。硬件安全评估指标如下。

- 物理环境安全性：主要考察 MEC 基础设施所处的物理环境在机房位置、电力供应、温/湿度控制情况，以及防盗窃、防火、防水、防静电、防电磁等方面的安全防护情况。
- 基础设施访问安全性：主要分为两个方面，首先是 MEC 机房出入口需要控制、鉴别和记录进出人员，并记录、审计机柜的开关；其次，应考虑 MEC 设备是否为可信设备，防止非法人员窃取敏感数据。

（2）控制面安全风险

控制面网元 SMF 与边缘 UPF 的 N4 接口可能会成为攻击者的目标，造成信令伪造、敏感信息泄露等威胁[19]。控制面安全评估指标如下。

控制面安全防护能力：控制面接口是否遵循 3GPP 标准使用互联网络层安全协议（Internet protocol security，IPSec）隧道保护接口的完整性和机密性。

（3）用户面安全风险

用户面功能衔接 5G 核心网、MEC 节点和用户终端，根据不同业务的需求实现数据分流，实现边缘场景下的移动性管理、合法监听、计费、服务质量保障等功能。MEC 平台如果被攻击者非法入侵，将会导致 UPF 数据泄露。用户面安全评估指标如下。

- 用户面攻击防护能力：对用户面进行数据拦截、恶意数据伪造、畸形报文攻击，验证 MEC 节点对用户面非法访问、攻击的防

御能力。

- 用户面访问安全性：UPF 与应用资源是否共用，MEC 平台资源是否进行隔离操作，是否创建防火墙防止对 UPF 进行非法访问。

（4）虚拟化安全风险

MEC 基于虚拟化基础设施，安全边界模糊，资源越权访问风险较大；MEC 应用多数基于微服务架构[20]，存在资源共用的现象，因此，容器与宿主机、容器与容器之间要严格隔离。如果隔离不当，可能存在内核资源被恶意占用、虚拟机逃逸、宿主机被攻击等安全风险。虚拟化安全评估指标如下。

- 容器与宿主机安全隔离性：获取并解析虚拟机中当前执行的二进制文件，将其访问路径信息与预置逃逸访问路径信息匹配，以验证是否存在虚拟机逃逸漏洞。
- 容器与容器安全隔离性：检查 Docker 隔离机制的完整性，验证该 MEC 平台上容器之间的资源隔离及资源限制情况。

（5）MEC 平台安全风险

MEC 平台安全风险主要包括 MEC 平台和应用的通信数据可能被篡改、拦截、重放；攻击者可利用第三方应用对平台发起非授权访问，从而发起拒绝服务攻击或窃取敏感数据；平台的系统配置如果被恶意更改，会导致应用的越权访问，进而影响其他应用和 MEC 主机的运行；还可能导致用户数据被转发给非授权的第三方应用，带来用户数据泄露的安全风险；还包括 MEC 平台对日常运维、安全事件的监测能力。MEC 平台安全评估指标如下。

- 内外部攻击防护能力：从外部向 MEC 节点发起数据拦截、非授权访问、拒绝服务、恶意入侵等攻击，验证 MEC 节点防御外部威胁的能力；从内部窃取 MEC 节点和 UPF 之间的通信数据，验证 MEC 节点防御内部威胁的能力。
- 日常运维监测能力：通过管理员权限登录 MEC 管理平台，审查审计日志以验证 MEC 对日常运维、管理操作的监测情况。
- 安全事件监测能力：使用各种测试用例，如非授权访问、拒绝服务、数据重放等，验证 MEC 节点对恶意攻击事件、异常事件的监测能力。

（6）应用安全风险

不同应用运行于同一 MEC 节点上，不同应用之间隔离不当将对其他应用产生安全威胁；不同应用共享 MEC 平台提供的虚拟化资源，如果资源分配与应用需求不匹配，则会影响应用的正常运行。应用安全评估指标如下。

应用安全监测能力：对应用生命周期进行监测并记录，验证 MEC 节点对应用的监测能力。

（7）管理面安全风险

MEC 编排管理与 MEC 节点之间的通信数据可能会被窃取、篡改、拦截和重放；攻击者可通过入侵 MEC 平台管理系统非法获得 MEC 编排管理权限，窃取 MEC 管理信息，并通过仿冒合法编排管理系统控制 MEC 节点资源。管理面安全评估指标如下。

编排管理安全响应能力：对 MEC 节点发起非法访问控制，验证 MEC 节点对 MEC 编排管理安全响应的能力。

针对 MEC 安全风险的分析，建立了 5G MEC 安全评估体系目标−准则−指标（target-criterion-index，T-C-I）3 层架构，如图 2 所示，T 层为目标层，MEC 安全评估为最终目标；C 层为准则层，共 7 项，分类标准为 MEC 面临的七大安全风险，在完整包含 MEC 安全风险的同时考虑了 5G 网络的特征，体现出准则层具有一定的完备性；I 层为指标层，包含 12 项涉及七大准则的具体评价指标。

基于上述 3 层安全评估架构，设计了 5G MEC 安全评估方法。该方法首先基于层次分析法求取

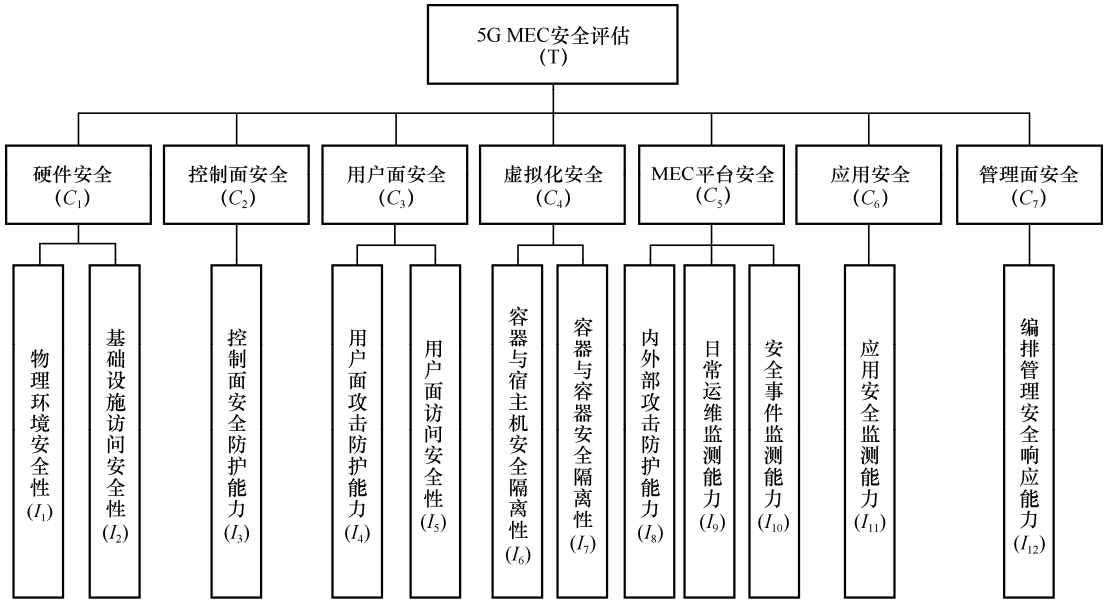



图 2　5G MEC 安全评估体系

指标层 12 项指标对于总目标的权重，然后将 MEC 漏洞评估系统评分结果作为评价参考，基于模糊论对各项指标进行评价，最后得到 MEC 安全评估结果。5G MEC 安全评估流程如图 3 所示。

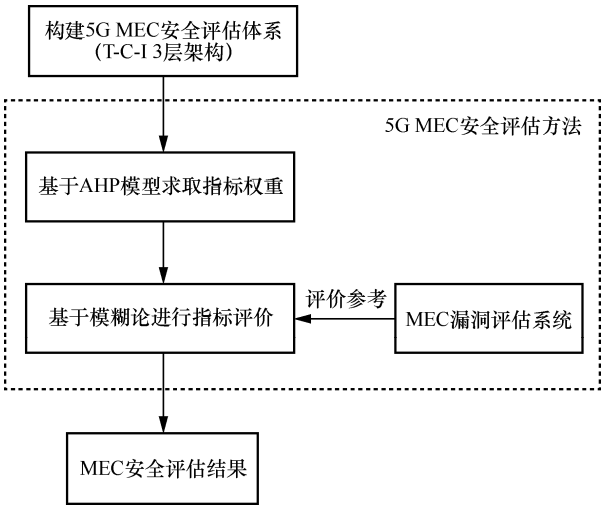



图 3　5G MEC 安全评估流程

## 2　基于 AHP 和模糊论的 5G MEC 安全评估方法设计

对于安全评估，常见的方法有层次分析法、图模型、支持向量机及神经网络。层次分析法将问题分解处理，层层递进，可以量化 MEC 安全能力，并且在 T-C-I 3 层架构下能充分发挥自身优点；图模型通过有向图分析网络潜在威胁，待评估问题具有节点、路径等特征；支持向量机的学习能力、泛化能力较强，适用于二分类评估问题，MEC 安全评估不涉及有向图且不是二分类问题，因此图模型和支持向量机不适合作为评估方法；神经网络因其需要大量 MEC 安全数据，在带来巨大计算开销的同时增加了数据暴露的风险，同样不适用。通过上述分析选取层次分析法作为评估方法。

### 2.1　基于 AHP 求取指标权重

AHP 将待决策问题层层分解，再对同一层次元素进行重要性比较和一致性分析，最后做出决策。其基本步骤如下。

（1）构造递阶层次的结构模型

图 2 所示的 5G MEC 安全评估体系即所需模型。

（2）构造各层次的判断矩阵

对同一层级的各项指标两两相比，用比例标度量化判断结果，得出判断矩阵：

$$\boldsymbol{A}_{n\times n}=\begin{bmatrix}1 & a_{12} & \cdots & a_{1n}\\ a_{21} & 1 & \cdots & a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n1} & a_{n2} & \cdots & 1\end{bmatrix} \tag{1}$$

其中，$a_{ij}$ 表示第 $i$ 项指标对第 $j$ 项指标的重要性。判断矩阵对权重的求取具有决定性的影响，传统的 9 级标度法[21]对指标之间的重要性判断划分得不够详细，导致判断过程中出现误差，从而影响权重结果。鉴于此，本文使用改进的指数标度构造判断矩阵，在第 3 节的实例验证中比较了两种标度法对判断矩阵一致性的影响。指数标度见表 1。

**表 1　指数标度**

| 标度 | 含义 |
|---|---|
| $9^0$ | 两因素相比，同等重要 |
| $9^{1/9}$(1.277) | 两因素相比，前者比后者稍重要 |
| $9^{3/9}$(2.080) | 两因素相比，前者比后者明显重要 |
| $9^{6/9}$(4.327) | 两因素相比，前者比后者强烈重要 |
| $9^1$ | 两因素相比，前者比后者极端重要 |
| $9^{1/18}$、$9^{2/9}$、$9^{1/2}$、$9^{5/6}$ | 上述判断的中间值 |
| 倒数 | 以上标度对应的相反概念 |

（3）同层次一致性检验和权重计算

计算判断矩阵的最大特征值 $\lambda_{\max}$ 及其对应的最大特征向量 $\boldsymbol{W}$，由最大特征值检验判断矩阵的一致性。对判断矩阵一致性检验如下，首先求取一致性检验指标 CI：

$$\mathrm{CI}=\frac{\lambda_{\max}-n}{n-1} \tag{2}$$

其中，$n$ 为判断矩阵的阶数。再求取随机一致性比率 CR，RI 取值见表 2。

$$\mathrm{CR}=\frac{\mathrm{CI}}{\mathrm{RI}} \tag{3}$$

**表 2　RI 取值**

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| RI | 0 | 0 | 0.52 | 0.89 | 1.12 | 1.26 | 1.36 | 1.41 | 1.46 |

当且仅当 CR<0.1[18]时，一致性检验通过，此时归一化的最大特征向量即指标权重；若检验不通过，则需重新构造判断矩阵。特别地，当 $n$=1 或 $n$=2 时，判断矩阵总满足一致性。

（4）总层次一致性检验和权重计算

为了避免各层的非一致性的累积导致最终一致性不满足要求，需要进行组合一致性检验，并计算指标层对目标层的权重：

$$\mathrm{CR}=\frac{\sum_{i=1}^{m}W_{C_i\text{-T}}\mathrm{CI}_i}{\sum_{i=1}^{m}W_{C_i\text{-T}}\mathrm{RI}_i} \tag{4}$$

其中，$m$ 为 C 层准则数，CR 指 I 层对 T 层的随机一致性比率，$W_{C_i\text{-T}}$ 表示 C 层第 $i$ 项占 T 层的权重，$\mathrm{CI}_i$、$\mathrm{RI}_i$ 表示 C 层第 $i$ 项对应 I 层对其的一致性指标。当且仅当 CR<0.1 时，总层次一致性检验通过，此时，I 层对 T 层的权重通过 I 层对 C 层的权重与 C 层与 T 层的权重相乘求得；若一致性检验不通过，则需要考虑重新构造一致性指标较大的判断矩阵。

## 2.2　基于模糊论的指标评价

第 1 节基于对 5G MEC 安全风险的分析建立了 T-C-I 3 层 MEC 安全评估体系，利用 AHP 给出了 I 层 12 项指标对于总目标的权重，基于此，本节利用基于模糊论的评价方法完成各项指标评价[22]。模糊评价通常采取专家直接评价的方式，评价过程中过多地依赖专家的经验判断，主观性较强。为了让指标评价更客观，同时又更契合 5G MEC 的安全需求，本文创新性地提出了一种适用于 5G MEC 的漏洞评分系统 MVSS，其在结合通用漏洞评分系统的基础上，充分考虑了 MEC 特定业务的实际需求，该评分系统的评分结果可作为指标评价的重要参考。漏洞可认为是已知的威胁，对于没有先验知识的未知威胁，为了安全性考虑，开展安全评估时对相应评价指标做最低评价[23]。模糊评价的基本步骤如下。

（1）构造评价指标集

根据本文提出的 T-C-I 3 层 MEC 安全评估体系，得到评价指标集：

$$U=\{C_1,C_2,C_3,C_4,C_5,C_6,C_7\} \tag{5}$$

其中，

$$\begin{cases} C_1=\{I_1,I_2\} \\ C_2=\{I_3\} \\ C_3=\{I_4,I_5\} \\ C_4=\{I_6,I_7\} \\ C_5=\{I_8,I_9,I_{10}\} \\ C_6=\{I_{11}\} \\ C_7=\{I_{12}\} \end{cases} \tag{6}$$

（2）确定评价等级

构造评价指标集 $U$ 对 MEC 安全评估的评判集：

$$\begin{aligned} &\boldsymbol{V}=\{V_1,V_2,V_3,V_4,V_5\}= \\ &\{\text{差},\text{较差},\text{中等},\text{较好},\text{好}\}= \\ &\{[0,3),[3,6),[6,7),[7,9),[9,10]\} \end{aligned} \tag{7}$$

每一个等级集合相当于一个模糊子集，一般取各区间的中值作为评价等级的分值。

（3）指标评价

由专家作为决策者对指标进行评判，若某一指标存在相关漏洞，且该漏洞被 MVSS 评定为“极危”，则专家在对该指标评价时应给出“差”；相反，若不存在漏洞或者漏洞评定等级为“低危”，则相应上调指标评价。MVSS 设计和评分过程将在后文给出。建立模糊映射，单因素评判 $f:U\to F(\boldsymbol{V}),c_i\mapsto f(c_i)=(r_{i1},r_{i2},\cdots,r_{i5})$，$r_{i1},r_{i2},\cdots,r_{i5}$ 表示对指标 $c_i$ 做出的评价，归一化得出准则层 $C_i$ 的评价矩阵：

$$\boldsymbol{R}_i=\begin{bmatrix} r_{11} & \cdots & r_{15} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{n5} \end{bmatrix} \tag{8}$$

其中，$n$ 为 $C_i$ 层对应的指标数。

（4）计算评价结果

利用指标层对准则层 $C_i$ 的权重 $\boldsymbol{W_i}$ 计算 $C_i$ 的单指标模糊评价：

$$\boldsymbol{M}_i=\boldsymbol{W}_i\cdot\boldsymbol{R}_i \tag{9}$$

计算 $C_1$ 到 $C_7$ 的单指标模糊评价，得到隶属度矩阵：

$$\boldsymbol{M}=(\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3,\boldsymbol{M}_4,\boldsymbol{M}_5,\boldsymbol{M}_6,\boldsymbol{M}_7)^{\mathrm{T}} \tag{10}$$

结合准则层 $C$ 对目标层 T 的权重 $\boldsymbol{W}$，得到准则层对目标层的综合模糊评价结果：

$$\boldsymbol{R}=\boldsymbol{W}\cdot\boldsymbol{M} \tag{11}$$

其中，$\boldsymbol{R}$ 为评价指标集的隶属度向量，最终评价结果为：

$$S=\boldsymbol{R}\cdot\boldsymbol{V}^{\mathrm{T}} \tag{12}$$

此结果为 5G MEC 安全评估结果。

2.2.1　5G MEC 漏洞评分系统设计

相比于 CVSS 和 IVSS 主要关注通用场景和工控场景下的漏洞风险，5G MEC 风险评估需求有所不同，5G 通过切片技术划分了三大应用场景[24]，不同应用场景对应着不同的安全需求，即同一个漏洞在不同场景下其风险指数可能会不同；且不同于 VScorer 涉及的云服务场景，在 5G MEC 中一个业务往往只涉及一个 MEC 服务器，VScorer 中的多服务器协同的场景并不适用于 5G MEC。因此，本文基于 CVSS 的基础指标，针对 5G MEC 安全防护特点，设计了 MVSS。CVSS 关注通用场景下的信息安全，IVSS 更侧重工控安全，VScorer 则注重云服务环境下的云平台安全，与它们三者不同，MVSS 基础指标在设计上更侧重于 MEC 业务安全，它包含 4 类指标，其中沿用了 CVSS 体系中的漏洞利用指标、影响范围指标、漏洞影响指标[25]，特别地，还针对 5G MEC 不同应用场景下的特定业务对安全、时延的不同需求制定了业务需求指标。

漏洞利用指标包含攻击向量、攻击复杂度、所需权限、用户交互，反映了目标的脆弱性。影响范围反映了漏洞是否会影响目标以外的主体。影响范围指标本身没有评分，但根据漏洞影响范围的不同，所需权限指标评分会受到影响。漏洞影响指标包含机密性、完整性、可用性，反映了漏洞利用对目标产生的安全性影响。

特别地，MVSS 根据 5G MEC 业务的特殊性，使漏洞评分根据特定业务具体化，制定了业务需求

指标，其中包含业务安全需求和时延需求。安全需求指特定业务对安全性的需求，例如，在 5G MEC 垂直行业场景中，内容分发网络（content delivery network，CDN）直播、云游戏、虚拟现实/增强现实等业务对安全性需求较低[26]，无人机、自动驾驶、智慧医疗等业务对安全性需求极高。因此，对于不同的 MEC 业务，安全需求指标的评分应根据实际业务的安全性需求评分。同样地，时延需求指特定业务时延的需求，云游戏、虚拟现实/增强现实等业务对时延要求较高，智慧零售、智慧家庭等业务对时延要求较低。因此，时延需求指标评分也应根据实际业务需求进行调整。

MVSS 基础指标量化见表 3。参照表 3，根据特定业务需求，将漏洞各项分值代入式（13）～式（19）。其中，$S_u$ 表示漏洞利用指标得分，$\mathrm{BS}_i$ 表示漏洞影响指标基础得分，$S_i$ 表示漏洞影响指标得分，sr 表示安全需求系数，dr 表示时延需求系数，BS 表示 MVSS 的基础指标最终得分。式（13）～式（17）沿用 CVSS 的评分规则，在通用条件下给出漏洞的基础指标得分。式（18）和式（19）则根据不同的安全和时延需求，给出 5G MEC 特定业务场景下的漏洞得分。

$$\mathrm{BS}_i = 1-((1-C)\times(1-I)\times(1-A)) \tag{13}$$

若影响范围不变，则：

$$S_i = 6.42\times \mathrm{BS}_i \tag{14}$$

若影响范围改变，则：

$$S_i = 7.52\times(\mathrm{BS}_i - 0.029) - 3.25\times(\mathrm{BS}_i - 0.02)^{15} \tag{15}$$

$$S_u = 8.22\times \mathrm{AV}\times \mathrm{AC}\times \mathrm{PR}\times \mathrm{UI} \tag{16}$$

若 $S_i < 0$，则：

$$\mathrm{BS} = 0 \tag{17}$$

若影响范围不变，则：

$$\mathrm{BS} = \mathrm{Roundup}(\mathrm{Min}((\mathrm{sr}+\mathrm{dr})\times(S_i + S_u),10)) \tag{18}$$

若影响范围改变，则：

$$\mathrm{BS} = \mathrm{Roundup}(\mathrm{Min}((\mathrm{sr}+\mathrm{dr})\times 1.08\times(S_i + S_u),10)) \tag{19}$$

其中，Roundup 函数指保留一位小数，并向上取整；Min 函数指取最小值。至此，得出 MEC 漏洞的 MVSS 基础评分。

### 2.2.2　MVSS 评分结果分析

本节通过对具体的漏洞进行评分，展示 MVSS 的评分过程，并将具体漏洞的 MVSS 评分结果与 CVSS 评分结果比较，验证 MVSS 在 5G MEC 漏洞风险评估中的有效性。以国家信息安全漏洞共享平台（China national vulnerability database，CNVD）提供的编号为 CNVD-2019-42040 的虚拟机漏洞（后文简称为“该漏洞”）为例，CVSS 对该漏洞评分为 7.9，根据 CVSS 漏洞风险划分依据（0.1～3.9 为低危，4.0～6.9 为中危，7.0～8.9 为高危，9.0～10.0 为极危），该漏洞的危害级别为高危。MVSS 漏洞风险划分同 CVSS，不另做修改。下面通过分析该漏洞在 MVSS 中的相关指标情况，对其进行评分。

该漏洞涉及 QEMU-KVM 虚拟机到宿主机内核逃逸漏洞，主要影响 Linux kernel，即 Linux 操作系统内核。Linux 是 ARM 架构计算芯片广泛使用的操作系统，该漏洞会影响 MEC 虚拟化基础设施的安全性，攻击者可利用该漏洞导致虚拟机逃逸，并获得在宿主机内核中任意执行代码的权限。

分析该漏洞的 MVSS 基础指标，在漏洞利用和影响范围指标方面，该漏洞在 CNVD 中显示的威胁类型为本地，即漏洞利用需要在本地进行，攻击向量指标分值为 0.55；该漏洞源于在内存上执行操作时，未正确验证数据边界，导致在关联的其他内存位置上执行了错误的读写操作，因此攻击复杂度低，分值为 0.77；攻击者仅需要普通用户权限即可利用该漏洞对目标虚拟机进行攻击，且发生攻击时可能导致虚拟机逃逸，因此影响范围发生改变，所以所需权限指标分值为 0.68；

表 3　MVSS 基础指标量化

| 指标分类 | 指标名称 | 指标值 | 指标描述 | 数值 |
|---|---|---|---|---|
| 漏洞利用指标 | 攻击向量（attack vector，AV） | 网络 | 远程利用 | 0.85 |
| | | 局域 | 共享网络或本地网络 | 0.62 |
| | | 本地 | 在本地利用漏洞 | 0.55 |
| | | 物理 | 攻击需要物理接触 | 0.2 |
| | 攻击复杂度（attack complexity，AC） | 低 | 攻击复杂度低 | 0.77 |
| | | 高 | 攻击复杂度高 | 0.44 |
| | 所需权限（privileges required，PR） | 无 | 无特权即可实施攻击 | 0.85 |
| | | 低 | 需要普通用户权限 | 0.62（0.68，若范围指标 S 的指标值为改变） |
| | | 高 | 需要管理员权限 | 0.27（0.50，若范围指标 S 的指标值为改变） |
| | 用户交互（user interaction，UI） | 无 | 不需要用户交互 | 0.85 |
| | | 需要 | 需要用户交互 | 0.68 |
| 影响范围指标 | 范围（scope，S） | 不变 | 存在漏洞主体与受攻击主体一致 | — |
| | | 改变 | 存在漏洞主体与受攻击主体不一致 | — |
| 漏洞影响指标 | 机密性（confidentiality，C） | 无 | 机密性没有丧失 | 0 |
| | | 低 | 机密性部分丧失 | 0.22 |
| | | 高 | 机密性完全丧失 | 0.56 |
| | 完整性（integrity，I） | 无 | 完整性没有丧失 | 0 |
| | | 低 | 完整性部分丧失 | 0.22 |
| | | 高 | 完整性完全丧失 | 0.56 |
| | 可用性（availability，A） | 无 | 可用性没有丧失 | 0 |
| | | 低 | 可用性部分丧失 | 0.22 |
| | | 高 | 可用性完全丧失 | 0.56 |
| 业务需求指标 | 安全需求（safety requirement，SR） | 低 | 业务安全需求低 | 0.6 |
| | | 中 | 业务安全需求中 | 0.8 |
| | | 高 | 业务安全需求高 | 1.0 |
| | 时延需求（delay requirement，DR） | 低 | 业务时延需求低 | 0.6 |
| | | 中 | 业务时延需求中 | 0.8 |
| | | 高 | 业务时延需求高 | 1.0 |

该漏洞利用需要用户在内存上执行操作，因此用户交互指标分值为 0.68。

在漏洞影响指标方面，漏洞利用会对被攻击虚拟机的机密性、完整性、可用性造成一定的影响，但虚拟机本身的机密性、完整性、可用性不会完全丧失，因此 3 项漏洞影响指标分值均为 0.22。

在业务需求指标方面，该漏洞涉及 MEC 底层的虚拟化基础设施安全，各类安全、时延需求不同的业务都可能会涉及此漏洞，因此对各种情况进行讨论。

将上述分值代入式（13）～式（19），得到 $BS_i$=0.525（保留 3 位小数，下同），$S_i$=3.730，$S_u$=1.610，若在业务 A 场景下的 sr=dr=0.6，则得到 BS=6.9，由 CVSS 漏洞评分等级表可知，该漏洞为中危漏洞；在业务 B 场景下 sr=0.6、dr=0.8，

得到 BS=8.1，则该漏洞为高危漏洞；在业务 C 场景下 sr=dr=1.0，得到 BS=10，则该漏洞为极危漏洞。由此可见，MVSS 可根据不同的业务需求灵活地调整同一漏洞的危害级别，而 CVSS 对该漏洞的评估结果在特定的业务下并不适用。由上述结果可知，CVSS 未能考虑漏洞在 5G MEC 垂直领域业务场景下对安全、时延需求的影响[27]，相比之下，本文提出的 MVSS 对 MEC 漏洞的危害程度评估更加准确。

## 3　实验验证与分析

本节基于提出的评估体系与评估方法，给出特定业务下的 5G MEC 安全量化值计算过程。该过程包括：基于 AHP 确定指标层对总目标的权重，针对不同的 MEC 业务场景，准则层涉及的七大安全风险的影响程度会产生差异，从而导致指标层的权重发生变化；基于模糊论给出各项指标安全评分，此评分参考 MVSS 对漏洞数据库中的漏洞评分结果，针对不同业务背景将更具针对性，评分结果更准确；此外，还对该方法做了灵敏度分析，验证该方法能较为灵敏地感知影响程度高的指标；在实际 5G MEC 应用场景下，将本文提出的方法与传统云平台安全评估方法进行比较分析。

### 3.1　基于 AHP 确定指标权重

分析准则层七大安全风险对 MEC 安全性的影响程度，构造准则层判断矩阵，为了完整地展示评估过程，本节使用指数标度法构造判断矩阵，见表 4，准则间的重要性程度判断参考文献[11]中关于 5G MEC 安全能力部署需求等级的论述。判断矩阵可根据不同业务需求下各大安全风险对安全性的不同影响程度做出相应调整。为了验证指数标度法比 9 级标度法有更好的精度，将计算相同重要性程度下的 9 级标度法判断矩阵对应的一致性检验。表 4 中 $C_1$ 到 $C_7$ 对应 3 层架构中的准则层。

计算两种不同标度法下的判断矩阵的最大特征值 $\lambda_{max}$，并由式（2）和式（3）求出 CR 进行一致性检验。$\lambda_{max}$ 对应的最大特征向量归一化即准则层各项权重，两种标度法的计算结果比较见表 5。

由结果可知，两种标度法下的 CR 均小于 0.1，满足一致性检验，但指数标度法的 CI 更小，即该标度法下的判断矩阵一致性更强。因此，本文后续判断矩阵的构造均参照指数标度法。取 $\boldsymbol{W}=(0.115, 0.101, 0.181, 0.203, 0.147, 0.163, 0.090)^{\mathrm{T}}$。

同样地，计算出指标层对准则层的随机一致性比率和权重向量，指标层计算结果见表 6。

表 4　使用指数标度法构造的判断矩阵

| 对比项 | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ |
|---|---|---|---|---|---|---|---|
| $C_1$ | 1 | 1.129 | 0.614 | 0.481 | 0.886 | 0.783 | 1.277 |
| $C_2$ | 0.886 | 1 | 0.481 | 0.614 | 0.783 | 0.481 | 1.129 |
| $C_3$ | 1.629 | 2.080 | 1 | 0.886 | 1.277 | 1.129 | 1.629 |
| $C_4$ | 2.080 | 1.629 | 1.129 | 1 | 1.129 | 1.129 | 3 |
| $C_5$ | 1.129 | 1.277 | 0.783 | 0.886 | 1 | 1 | 1.629 |
| $C_6$ | 1.277 | 2.080 | 0.886 | 0.886 | 1 | 1 | 1.629 |
| $C_7$ | 0.783 | 0.886 | 0.614 | 0.333 | 0.614 | 0.614 | 1 |

表 5　两种标度法的计算结果比较

| 标度法 | $\lambda_{max}$ | CI | CR | $\boldsymbol{W}$ |
|---|---|---|---|---|
| 9 级标度法 | 7.28 | 0.047 | 0.035 | $(0.072, 0.049, 0.248, 0.297, 0.133, 0.162, 0.037)^{\mathrm{T}}$ |
| 指数标度法 | 7.06 | 0.01 | 0.007 | $(0.115, 0.101, 0.181, 0.203, 0.147, 0.163, 0.090)^{\mathrm{T}}$ |

表 6　指标层计算结果

| 对比项 | $W_i$ | CI | RI | CR |
|---|---|---|---|---|
| $C_1(I_1, I_2)$ | $W_1$=(0.64,0.36) | 0 | 0 | — |
| $C_2(I_3)$ | $W_2$=(1) | 0 | 0 | — |
| $C_3(I_4, I_5)$ | $W_3$=(0.71,0.29) | 0 | 0 | — |
| $C_4(I_6, I_7)$ | $W_4$=(0.50,0.50) | 0 | 0 | — |
| $C_5(I_8, I_9, I_{10})$ | $W_5$=(0.55,0.21,0.24) | 0.021 | 0.52 | 0.04 |
| $C_6(I_{11})$ | $W_6$=(1) | 0 | 0 | — |
| $C_7(I_{12})$ | $W_7$=(1) | 0 | 0 | — |

从表 6 可知，各项一致性检验均满足要求。根据：

$$\boldsymbol{W}_{\mathrm{I-T}}=\boldsymbol{W}^{\mathrm{T}}\cdot\begin{bmatrix}\boldsymbol{W}_1 & 0 & 0 & 0\\ 0 & \boldsymbol{W}_2 & 0 & 0\\ 0 & 0 & \ddots & 0\\ 0 & 0 & 0 & \boldsymbol{W}_7\end{bmatrix} \tag{20}$$

求得指标层 I 对目标层 T 的总权重向量 $\boldsymbol{W}_{\mathrm{I\text{-}T}}$=(0.074, 0.041, 0.101, 0.129, 0.052, 0.101, 0.102, 0.081, 0.031, 0.035, 0.163, 0.090)。

最后进行组合一致性检验，将准则层权重 $\boldsymbol{W}$=(0.115, 0.101, 0.181, 0.203, 0.147, 0.163, 0.090)$^{\mathrm{T}}$，$\mathrm{CI}_5$=0.021、$\mathrm{RI}_5$=0.52 代入式（4），得 CR=0.04<0.1，通过一致性检验。至此，在各层一致性检验和总一致性检验均满足要求的条件下，求出了指标层各项对总目标的权重。

### 3.2　基于模糊评价计算安全指数

构建评语集，并选取中值作为评语代表的分数：

$$\boldsymbol{V}=\{\text{差},\text{较差},\text{中等},\text{较好},\text{好}\}=\{1.5,4.5,6.5,8,9.5\}$$

对于给定的业务背景，参考 MVSS 评分结果（如果存在未知威胁，如漏洞库中不存在的未知漏洞，为了安全性考虑将对应指标评价为“差”），对评价指标集中 7 个子集的 12 项指标进行评价（此评价结果仅为了完整展现评估流程，实际评估中的评价结果应根据实际情况调整），模糊评价结果见表 7。

表 7　模糊评价结果

| 对比项 | 差 | 较差 | 中等 | 较好 | 好 |
|---|---|---|---|---|---|
| $I_1$ | 1 | 2 | 2 | 4 | 1 |
| $I_2$ | 0 | 1 | 5 | 4 | 0 |
| … | … | … | … | … | … |
| $I_{11}$ | 2 | 1 | 5 | 2 | 0 |
| $I_{12}$ | 0 | 2 | 2 | 4 | 2 |

将评价结果归一化，得到准则层 $C_1$ 的评价矩阵 $\boldsymbol{R}_1$：

$$\boldsymbol{R}_1=\begin{bmatrix}0.1 & 0.2 & 0.2 & 0.4 & 0.1\\ 0 & 0.1 & 0.5 & 0.4 & 0\end{bmatrix}$$

$C_1$ 的单因素评价：

$$\boldsymbol{M}_1=\boldsymbol{W}_1\cdot\boldsymbol{R}_1=(0.064,0.164,0.308,0.4,0.064)$$

同样地，计算 $C_2$ 到 $C_7$ 的单因素评价，得到隶属度矩阵：

$$\boldsymbol{M}=(\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3,\boldsymbol{M}_4,\boldsymbol{M}_5,\boldsymbol{M}_6,\boldsymbol{M}_7)^{\mathrm{T}}=\begin{bmatrix}0.064 & 0.164 & 0.308 & 0.4 & 0.064\\ 0 & 0.1 & 0.3 & 0.4 & 0.2\\ 0 & 0.271 & 0.329 & 0.329 & 0.071\\ 0 & 0.1 & 0.3 & 0.55 & 0.05\\ 0.021 & 0.266 & 0.562 & 0.151 & 0\\ 0 & 0.1 & 0.2 & 0.5 & 0.2\\ 0 & 0.1 & 0.1 & 0.7 & 0.1\end{bmatrix}$$

准则层对目标层的综合评价结果为：

$$\boldsymbol{R}=\boldsymbol{W}\cdot\boldsymbol{M}=(0.007\,4,0.168\,9,0.318\,4,0.420\,3,0.083\,0)$$

最终得到的 5G MEC 安全评估结果为：

$$S=\boldsymbol{R}\cdot\boldsymbol{V}^{\mathrm{T}}=6.99$$

结果在分数区间[6,7)内，评估结果为“中等”，说明该 MEC 节点安全性一般。

### 3.3　灵敏度分析

基于前文中的 MEC 节点安全评估实例，下面探讨该评估方法的灵敏度。5G MEC 搭载于虚拟化基础设施之上，通过容器、虚拟机技术实现各类服务，因此，虚拟化安全关乎整个 MEC 平台的安全，准则层 $C_4$ 的权重占比也最高。由前文可知准则层 $C_4$ 的评价矩阵为：

$$\boldsymbol{R}_4=\begin{bmatrix}0 & 0.1 & 0.2 & 0.7 & 0\\ 0 & 0.1 & 0.4 & 0.4 & 0.1\end{bmatrix}$$

将其改为：

$$\boldsymbol{R}_4'=\begin{bmatrix}0 & 0 & 0.2 & 0.5 & 0.3\\ 0 & 0 & 0.3 & 0.3 & 0.4\end{bmatrix}$$

计算最终评估结果为 $S'=7.25$，结果为“较好”。

若将其改为：

$$\boldsymbol{R}_4''=\begin{bmatrix}0.4 & 0.4 & 0.2 & 0 & 0\\ 0.4 & 0.4 & 0.2 & 0 & 0\end{bmatrix}$$

计算最终评估结果为 $S''=5.93$，结果为“较差”。

通过计算可以看出，评估结果对准则层 $C_4$ 的评价结果敏感程度较高，能较灵敏地感知其变化，说明该 MEC 安全评估方法有效。

### 3.4　比较分析

通过对特定应用场景、不同漏洞情况的 MEC 节点进行评分，将本文提出的评估方法与传统云平台评估方法进行比较，以证明本文方法在量化 5G MEC 安全能力中的优势。以工业互联网边缘计算智慧工厂这一典型应用场景（如图 4 所示）为例，该场景下主要的安全问题和需求包括工厂车间生产线多，设备类型、数量众多，设备间通信通常使用不安全的协议，不同生产线之间没有网络隔离措施，缺少访问控制手段；现场层和 MEC 层之间的通信未隔离，会导致一方受到攻击后波及另一方；部分车间主机操作系统老旧、补丁更新不及时、病毒查杀不全面；对车间网络流量缺少监测审计和安全管理，缺少对网络系统的实时安全监控。通过对该场景安全需求的分析，可以发现本文提出的安全评估体系能较为完整、全面地覆盖其安全问题，与真实系统的安全指标贴合度较高。

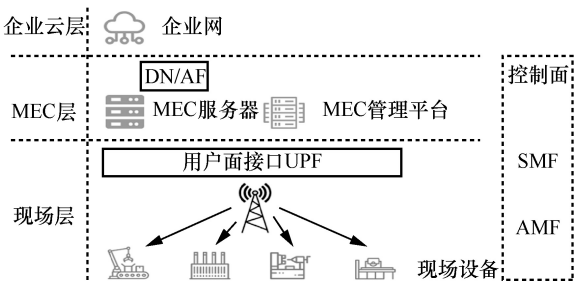



图 4　智慧工厂 MEC 应用场景

不失一般性，在该场景下，划分出设备远程控制、自动预警、视频监控、数据分析四大业务，每个业务对安全和时延的需求各不相同；同时，从国家工业信息安全漏洞库中挖掘出典型工控漏洞 10 条。将不同业务与不同漏洞组合，即可得到 40 种不同情况。根据对 5G MEC 安全评估体系与方法的分析，在实际应用场景中对 40 种情况下的 MEC 节点进行安全评估，将评估结果与文献[13]提出的云平台评估体系所得出的结果进行比较。在评估过程中，不涉及漏洞的，两种方法中相似的指标做相同评价，特有的指标均做中等评价；涉及漏洞的，本文提出的方法用 MVSS 进行漏洞评估，文献[13]的方法使用 CVSS 给出的漏洞评分，再参考漏洞评分结果进行评估。

MEC 评分结果比较如图 5 所示，展示两种评估方法对 40 种情况的评分结果，横坐标为分数区间，纵坐标为相应分数区间内的数量。本文提出的评估方法在结果上趋向“差”或“好”两个极端，而文献[13]的评估方法得到的结果分布相对均匀。由此可以看出，本文提出的 5G MEC 评估方法能够更加准确地感知在不同业务、不同漏洞背景下的 MEC 安全需求，从而给出更加有效的评估结果，这可以帮助企业迅速定位各类业务环境中需要解决的关键问题。另外，某一漏洞可能对当前业务影响较小，则不必消耗过多资源处理该漏洞。

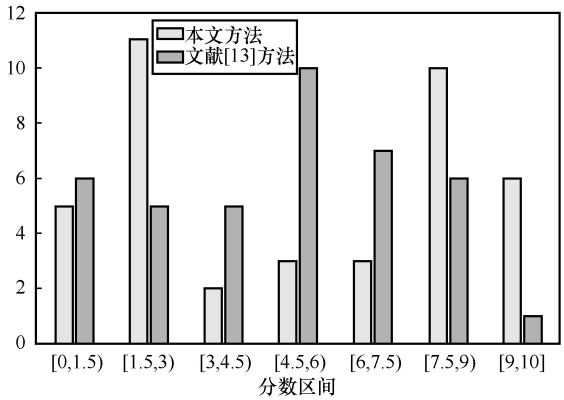



图 5　MEC 评分结果比较

## 4 结束语

5G MEC 为垂直行业应用场景修建了一条“快车道”，使得数据在边缘侧就能得到及时的处理而不用传至云端，在降低业务时延方面有良好的效果，应用前景广泛[28]。同时，MEC 安全能力强，更易受到攻击者青睐。准确量化 MEC 安全能力成为迫切需求。本文结合 5G MEC 安全风险，提出了 5G MEC 安全评估体系，其评估指标全面、真实地反映了 MEC 的安全性。该评估指标在完整包含 MEC 安全风险的同时，考虑了 5G 网络的特征，具有一定的完备性。在此基础上，结合 AHP 和模糊评价设计了 5G MEC 安全评估方法，该方法能给出 MEC 安全量化值，实例结果证明了其有效性。为了使评价结果更加客观，还针对性地提出了 MEC 漏洞评分系统（MVSS），该评分系统能更加准确地评估 MEC 相关漏洞的危害程度，有助于确定安全防护优先等级。用 MVSS 的评分结果作为指标评价的参考是进行安全评估的一种思路，如果在评估过程中遇到未知威胁，可从安全性的角度给对应指标最低评价。本文的初值赋值依赖于该因素从原理上造成的严重后果而确定。当然，在实际工程和不同的应用场景（如消费者业务和企业垂直类业务等）中，同一因素造成的后果是不同的，可根据具体的应用场景灵活调整初值，但这不影响本文提出的评估框架模型的通用性和具体方法论的有效性。

## 参考文献：


[1] AHMAD I, KUMAR T, LIYANAGE M, et al. Overview of 5G security challenges and solutions[J]. IEEE Communications Standards Magazine, 2018, 2(1): 36-43.

[2] 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.

[3] BEBORTTA S, SENAPATI D, PANIGRAHI C R, et al. Adaptive performance modeling framework for QoS-aware offloading in MEC-based IIoT systems[J]. IEEE Internet of Things Journal, 2022, 9(12): 10162-10171.

[4] HOU Y Z, WANG C R, ZHU M, et al. Joint allocation of wireless resource and computing capability in MEC-enabled vehicular network[J]. China Communications, 2021, 18(6): 64-76.

[5] QADIR J, SAINZ-DE-ABAJO B, KHAN A, et al. Towards mobile edge computing: taxonomy, challenges, applications and future realms[J]. IEEE Access, 2020(8): 189129-189162.

[6] ETSI. Mobile edge computing (MEC); framework and reference architecture: ETSI GS MEC003 V2.2.1[S]. 2020.

[7] 3GPP. Security architecture and procedures for 5G system: TS 33.501 V15.4.0[S]. 2020.

[8] AHMAD I, SHAHABUDDIN S, KUMAR T, et al. Security for 5G and beyond[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3682-3722.

[9] TALEB T, SAMDANIS K, MADA B, et al. On multi-access edge computing: a survey of the emerging 5G network edge cloud architecture and orchestration[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1657-1681.

[10] RANAWEERA P, JURCUT A D, LIYANAGE M. Survey on multi-access edge computing security and privacy[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1078-1124.

[11] 刘云毅, 张建敏, 冯晓丽, 等. 5G MEC 系统安全能力部署方案[J]. 电信科学, 2022, 38(11): 143-152.
LIU Y Y, ZHANG J M, FENG X L, et al. 5G MEC system security capability deployment scheme[J]. Telecommunications Science, 2022, 38(11): 143-152.

[12] 张琳, 魏新艳, 刘茜萍, 等. 基于协作信誉和设备反馈的物联网边缘服务器信任评估算法[J]. 通信学报, 2022, 43(2): 118-130.
ZHANG L, WEI X Y, LIU X P, et al. Trust evaluation algorithm of IoT edge server based on cooperation reputation and device feedback[J]. Journal on Communications, 2022, 43(2): 118-130.

[13] 贺海, 刘海峰, 成金爱. 云计算平台安全能力评估体系和评估指标研究[J]. 信息安全研究, 2020, 6(11): 990-995.
HE H, LIU H F, CHENG J A. Research on evaluation system and index of cloud computing platform security capability[J]. Journal of Information Security Research, 2020, 6(11): 990-995.

[14] FIGUEROA-LORENZO S, AÑORGA J, ARRIZABALAGA S. A survey of IIoT protocols: a measure of vulnerability risk analysis based on CVSS[J]. ACM Computing Surveys, 2020, 53(2): 1-53.

[15] 陶耀东, 贾新桐, 吴云坤. 一种工业控制系统漏洞风险评估方法[J]. 小型微型计算机系统, 2020, 41(3): 603-609.
TAO Y D, JIA X T, WU Y K. Industry control system vulnerability risk assessment method[J]. Journal of Chinese Computer Systems, 2020, 41(3): 603-609.

[16] 李舟, 唐聪, 胡建斌, 等. 面向 SaaS 云平台的安全漏洞评分方法研究[J]. 通信学报, 2016, 37(8): 157-166.
LI Z, TANG C, HU J B, et al. Vulnerabilities scoring approach for cloud SaaS[J]. Journal on Communications, 2016, 37(8): 157-166.

[17] ALI B, GREGORY M A, LI S. Multi-access edge computing architecture, data security and privacy: a review[J]. IEEE Access, 2021(9): 18706-18721.

[18] 杨志强, 粟栗, 杨波, 等. 5G 安全技术与标准[M]. 北京: 人民邮电出版社, 2020.

YANG Z Q, SU L, YANG B, et al. 5G security technology and standards[M]. Beijing: Posts & Telecom Press, 2020.
[19] 周艳, 何承东. 5G 安全的全球统一认证体系和标准演进[J]. 移动通信, 2021, 45(1): 21-29.
ZHOU Y, HE C D. Global unified security certification system and standard evolution for 5G security[J]. Mobile Communications, 2021, 45(1): 21-29.
[20] 武志学. 云计算虚拟化技术的发展与趋势[J]. 计算机应用, 2017, 37(4): 915-923.
WU Z X. Advances on virtualization technology of cloud computing[J]. Journal of Computer Applications, 2017, 37(4): 915-923.
[21] 杨爱民, 高放, 边敏华, 等. 基于层次分析—模糊评价的云计算安全评估与对策[J]. 通信学报, 2016, 37(S1): 104-110.
YANG A M, GAO F, BIAN M H, et al. Cloud computing security evaluation and countermeasure based on AHP-fuzzy comprehensive evaluation[J]. Journal on Communications, 2016, 37(S1): 104-110.
[22] FENG N, FU B C, WU H J, et al. Modeling of fuzzy comprehensive evaluation based on cloud model[C]//Proceedings of 2016 14th International Conference on Control, Automation, Robotics and Vision (ICARCV). Piscataway: IEEE Press, 2017: 1-5.
[23] 于亚, 伏玉笋. 工业互联网边缘终端初始接入可信度量方法研究[J]. 物联网学报, 2022, 6(4): 149-157.
YU Y, FU Y S. Research on trust measurement method for initial access of industrial Internet edge terminals[J]. Chinese Journal on Internet of Things, 2022, 6(4): 149-157.
[24] PRATHYUSHA Y, SHEU T L. Coordinated resource allocations for eMBB and URLLC in 5G communication networks[J]. IEEE Transactions on Vehicular Technology, 2022, 71(8): 8717-8728.
[25] KAI S F, ZHENG J H, SHI F, et al. A CVSS-based vulnerability assessment method for reducing scoring error[C]//Proceedings of 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT). Piscataway: IEEE Press, 2022: 25-32.
[26] SPINELLI F, MANCUSO V. Toward enabled industrial verticals in 5G: a survey on MEC-based approaches to provisioning and flexibility[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 596-630.
[27] NOWAK T W, SEPCZUK M, KOTULSKI Z, et al. Verticals in 5G MEC-use cases and security challenges[J]. IEEE Access, 2021(9): 87251-87298.
[28] 马洪源, 肖子玉, 卜忠贵, 等. 5G 边缘计算技术及应用展望[J]. 电信科学, 2019, 35(6): 114-123.
MA H Y, XIAO Z Y, BU Z G, et al. 5G edge computing technology and application prospects[J]. Telecommunications Science, 2019, 35(6): 114-123.

## [作者简介]

**卢秋呈**（1998– ），男，上海交通大学硕士生，主要研究方向为工业通信系统与安全可信。

**唐金辉**（1999– ），男，上海交通大学硕士生，主要研究方向为工业通信系统与安全可信。

**鲍聪颖**（1986– ），女，宁波市永耀电力投资集团有限公司高级工程师，主要研究方向为电力 5G 规划与应用安全。

**吴昊**（1993– ），男，国网浙江省电力有限公司宁波供电公司工程师，主要研究方向为电力 5G 通信与安全。

**伏玉笋**（1972– ），男，博士，上海交通大学助理研究员，主要研究方向为无线通信与系统、无线网联智能系统、工业互联网与安全可信、智能制造等。