

移动边缘计算安全防护研究

陈璐, 汤红波, 游伟, 柏溢
(信息工程大学, 河南 郑州 450001)

摘要: 移动边缘计算 (Mobile Edge Computing, MEC) 通过进一步将电信蜂窝网延伸至其他无线接入网络, 可以有效地解决传统网络中回程链路负载过重、时延较长的问题。但由于 MEC 服务节点暴露在网络边缘, 且计算能力、存储能力和能量受限, 更易受到攻击者的青睐。在分析移动边缘计算面临的安全威胁问题基础上, 针对设备安全、节点安全、网络资源及任务和迁移安全等4个不同的安全主体归纳并阐述了移动边缘计算面临的若干关键问题与挑战, 总结归纳了现有的安全解决方案。最后, 从动态场景下的有限资源防御模型、综合信任基础的资源部署、以用户为中心的服务可靠性保证3个方面, 展望了移动边缘计算安全防护面临的开放性问题和未来的发展趋势。

关键词: 移动边缘计算; 安全; 威胁; 计算卸载; 计算迁移

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021014

Research on security defense of mobile edge computing

CHEN Lu, TANG Hongbo, YOU Wei, BAI Yi
Information Engineering University, Zhengzhou 450001, China

Abstract: Mobile Edge Computing can solve the problem of heavy backhaul link overloaded and long delay effectively by further extending the telecommunication cellular network to other wireless access networks. However, the MEC nodes are exposed to the edge of the network whose computing resource, storage capacity and energy resource are limited, they are more vulnerable to the illegal attacks by attackers. Based on the briefly analysis of the security threats faced by mobile edge computing, some key problems and challenges of mobile edge computing for four different security subjects, device security, node security, network resources and tasks, and migration security are summed up and expounded, and the existing security solutions were summarized. Finally, the open research and future development trend of mobile edge computing security defense on three aspects that limited resource defense model in the dynamic scene, resource deployment based on comprehensive trust and user-centered service reliability assurance are discussed.

Key words: mobile edge computing, security, threats, computing offloading, computing migration

收稿日期: 2020-07-09; 修回日期: 2020-10-28

通信作者: 汤红波, tahobo@sina.com

基金项目: 国家自然科学基金 (61801515, 61941114)

Foundation Item: The National Natural Science Foundation of China (61801515, 61941114)

论文引用格式: 陈璐, 汤红波, 游伟, 等. 移动边缘计算安全防护研究[J]. 网络与信息安全学报, 2021, 7(1): 130-142.

CHEN L, TANG H B, YOU W, et al. Research on security defense of mobile edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 130-142.

1 引言

2014年,欧洲电信标准化协会^[1](ETSI, European Telecommunications Standards Institute)将边缘计算融合进移动网络架构,提出了移动边缘计算(MEC, mobile edge computing)。移动边缘计算^[2]是指在移动网络边缘部署计算能力和存储资源,为移动网络提供IT服务环境和云计算能力,从而为用户提供超低时延和高带宽的网络服务解决方案。与之前提出的移动云计算^[3](MCC, mobile cloud computing)和内容分发网络^[4](CDN, content delivery network)两种技术相比,MEC分布式的部署方案可以很好地实现5G网络架构去中心化的需求,提高网络的灵活性。MEC部署在靠近网络的边缘侧,一方面可以减少与用户(UE)之间的距离,从而降低传输时延;另一方面MEC将计算和存储能力下沉到中下游,通过业务感知和上下文分析用户特征,为移动用户提供精准的计算服务和业务服务,使区域性业务在本地得到解决。除了为普通的移动用户提供高质量的业务需求外,还将渗透到自动驾驶/辅助驾驶、工业制造、远程医疗、智慧城市等特殊物联网(IoT, internet of things)领域中,为传统行业提供新的生机。

在为用户提供优质服务的同时,移动边缘计算同时面临着新的安全挑战。MEC的按需邻接部署使服务器暴露在网络边缘,客观上缩短了攻击者与MEC物理设施之间的距离,为攻击者接触MEC物理设施提供了便捷与机会。与此同时,MEC允许通过开放接口为第三方业务应用提供服务,为恶意用户的攻击提供了便利。攻击者可以通过第三方应用入侵MEC服务器,导致MEC服务器的非法接入、节点入侵、数据泄露、信息篡改等安全威胁^[5]。此外,由于MEC服务器节点的计算资源、存储资源和能量资源有限,攻击者可以通过恶意卸载对特定的MEC服务节点进行卸载攻击,导致资源耗尽使卸载服务无法正常进行。并且,由于MEC服务器具备一定的数据存储能力,恶意节点可能通过入侵服务节点非法获取用户的隐私数据。最后,由于动态环境下移动用户的移动属性,终端用户随时可以动态加入或

退出自治域,移动设备频繁的拓扑改变对网络资源管理产生影响,让攻击者可以利用计算迁移的变化过程开展攻击行为。

对整个MEC网络生态系统而言,安全问题难以罗列穷尽。然而,安全是一切网络服务的底线和前提,在网络资源有限的情况下,仍需保障移动终端用户卸载服务的安全需求。现有的MEC研究中,由于任务卸载产生的能耗和时延不容忽视,能耗-延迟的均衡研究得到了极大关注^[6-24],很少考虑安全问题。因此,本文在分析移动边缘计算面临的安全威胁问题基础上,针对单个攻击者和多个攻击者两种场景,阐述了移动边缘计算的若干关键问题与挑战和现有的安全解决方案,并指出了一些未来可能的研究方向。

2 面临的安全威胁

2.1 威胁分析

移动边缘计算可以在网络边缘为用户提供计算、存储和传输等资源服务,其可以感知用户实时业务需求和位置信息,为边缘用户提供便捷而精确的服务。然而,移动边缘计算面临众多异构终端用户通过无线等方式接入网络,涉及无线传感网、移动计算等多个领域,导致移动边缘计算面临诸多新的安全威胁^[6]。在移动边缘计算中,攻击者可能对MEC网络架构中的不同基础设施进行攻击,如用户设备、服务器节点、网络资源或虚拟机,甚至包括整个边缘数据中心。这种情况类似于互联网中的攻击场景,攻击者可以从“内部”或“外部”对网络基础设施进行攻击,对移动边缘计算产生安全威胁,如图1所示。本节讨论MEC可能面临的安全威胁。

2.2 拒绝服务

拒绝服务(DoS, denial of service): MEC架构中的网络基础设施和虚拟基础设施与云计算的安全威胁不同,MEC环境下的拒绝服务攻击只涉及自治域内的服务区域,但仍会对自治域内或半自治域内的通信和卸载服务产生影响。由于计算节点暴露在网络边缘,易受攻击者的攻击,攻击者可以通过恶意卸载耗尽服务主机的计算、网络等资源,导致服务节点失效,如受感染的僵尸主机向网络中局部MEC服务节点

进行大量任务卸载，造成网络计算能力瘫痪。

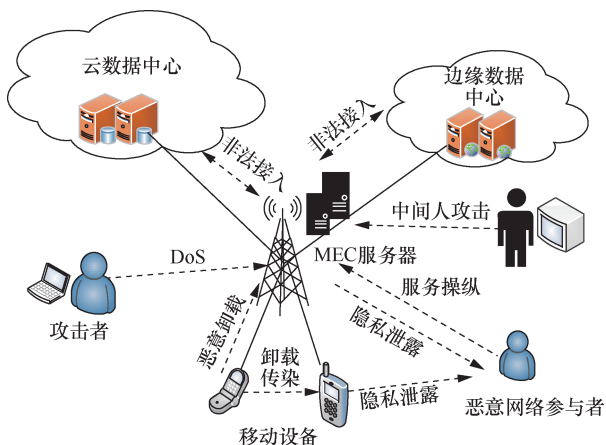


图 1 MEC 面临安全威胁
Figure 1 Security threats of MEC

2.3 滥用资源

滥用资源指攻击者通过对某个特定 MEC 服务器卸载大量计算任务或恶意过渡进行卸载，造成 MEC 中服务器之间的工作负载资源过度供应，导致卸载污染节点服务失效问题，同时可能致使其他用户服务超时，耗尽计算资源。这一过程可能通过感染发起卸载的终端用户，或者通过操纵控制卸载任务的虚拟机来完成。

2.4 隐私泄露

移动边缘计算可以为不同的用户提供差异化的“定制”服务，不仅为用户提供了便利，也使 MEC 的应用不可避免地能够大量访问移动用户和设备的隐私和数据信息。为此，第三方应用可以通过 API 接口获取有关物理和逻辑相关信息，如用户身份、位置和移动轨迹等。通过进一步挖掘这些数据，如利用大数据分析出用户的生活习惯、健康状况、身份职业等隐私信息，这将给用户的个人隐私和网络人身安全带来严峻的挑战。

2.5 服务操纵

恶意攻击者一旦控制了移动边缘数据中心，通过权限升级获取边缘数据中心的控制权，对核心信息进行盗取或篡改，甚至为其他合作者提供虚假的信息（如假的管理信息、历史数据等），这将导致对某个特定的卸载服务形成选择性拒绝服务攻击和选择性信息篡改，从而有针对性地开展目标攻击。

2.6 中间人攻击

用户移动导致移动前提供计算卸载服务的 MEC 服务器不在新的通信范围内而需要重新选择新的 MEC 服务器，从而带来服务区域重定位 (SAR, service area relocation)^[25]问题。该问题可能导致中间人攻击^[26]。攻击者利用服务区重定位的机会，入侵边缘网络设备进行窃听或流量注入等攻击，导致用户隐私受到侵害，或使边缘设备提供错误的迁移服务。

根据以上 5 类移动边缘计算面临的安全威胁，按网络安全主体所面临的关键问题和挑战归纳如表 1 所示。

表 1 移动边缘计算安全威胁
Table 1 Security threats of mobile edge computing

安全主体	拒绝服务	滥用资源	隐私泄露	服务操纵	中间人攻击
设备安全	√		√	√	√
节点安全	√	√			
资源和任务安全	√	√		√	
迁移安全			√	√	√

3 MEC 关键问题与挑战

随着 MEC 技术的不断发展和应用场景的日渐丰富，与传统的云计算、雾计算和内容分发网络等技术相比，所面临的安全问题和挑战不断升级，根据上述移动边缘计算面临安全威胁和网络安全主体，MEC 安全关键问题与挑战可归纳为以下几个方面。

3.1 设备安全

移动边缘计算将电信蜂窝网延伸至无线网络，因此 MEC 涉及大量的移动设备终端，这些设备终端的安全对网络安全带来了新的挑战。一方面设备终端可能受到恶意软件、病毒等网络参与者的恶意攻击，另一方面设备终端过量的卸载请求可能对网络带来危害和影响。另外，存在一种特殊的 MEC 应用场景——终端直通 (D2D, device-to-device) 通信场景中的设备安全问题。D2D 通信方式是指两个对等的用户节点之间直接进行通信的通信方式^[27-31]。在 MEC 中，终端用户通过利用邻近设备的空闲计算资源来提高网络

性能。每个终端用户本身可以进行任务卸载，同时可以作为服务计算节点为其他用户提供计算服务。通过利用无线和移动对等服务，D2D 可以为移动边缘计算提供增强型服务，在密集型计算需求、通信中断恢复和提高吞吐量上提供帮助。通过扩展蜂窝覆盖范围，D2D 尤其在网络基础设施高度拥挤时（如演唱会或大型体育活动现场）或不存在直接通信能力的场景下（受灾害毁坏通信基础设施的地区）进行数据通信，以缓解蜂窝网络的资源紧张压力或解决通信中断情况下的应急保障问题，如图 2 所示。但相比运营商网络，终端设备的防御能力较低且更易遭到攻击。一方面，终端用户设备容易受恶意软件、病毒入侵，导致自身成为被感染的网络节点参与网络行为，可能无法提供正常的空闲资源计算服务，更可能成为新的攻击者和感染源对其他网络节点进行攻击，因此需要设计合理的安全卸载防御机制提高卸载的成功率。另一方面，如何有效设定终端用户节点对卸载服务的参与度是值得研究的一个问题。因为自私的用户终端可能并不愿意将自身的资源给其他人使用，需要运营商设计合适的激励机制，以在节点平衡自身防御开销的情况下提供卸载服务行为，达到整个网络的最大收益。

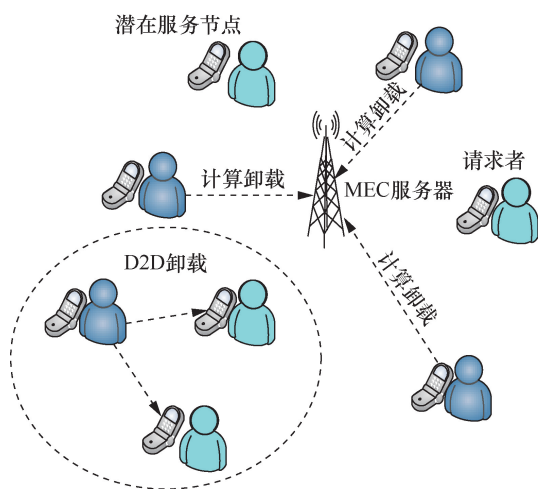


图 2 D2D 通信场景
Figure 2 D2D communication scenario

3.2 节点入侵

在移动边缘计算中，MEC 服务器面临众多异构终端节点的请求，需要为其提供访问、存储、计算和传输等服务，而 MEC 服务器所拥有的这些资源具有动态性、异构性的特点。因此移动边

缘服务器涉及大量终端参与资源访问、提供资源卸载计算和数据传输过程。提供卸载服务的计算节点暴露在网络边缘，又作为连接动态、异构终端用户的第一跳，容易受到恶意网络参与者对服务计算节点的攻击。由于 MEC 计算节点的计算、存储和能量有限，恶意网络参与者可以通过对某个特定计算节点进行过量卸载、恶意卸载而导致计算节点资源耗尽失效，导致终端用户的服务质量降级和中断。特别地，对于移动边缘计算的节点入侵问题需要解决以下两方面问题：一是 MEC 服务节点面临到来的卸载任务时如何判定这个任务或请求的发起者是否可信；二是如何保证声称提供资源的节点能够真正提供对应的计算资源。这一问题可以通过建立合理的终端用户与服务节点之间的信任机制来解决。特别地，信任问题在超可靠性低时延场景中不容被忽视^[32]。例如，在 5G 网络中，由于边缘服务器可能隶属于不同的参与者，如电信运营商、互联网公司、家庭用户等，不存在针对不同利益相关者和异构硬件的集中管理，因此会带来 MEC 计算卸载和计算迁移中的信任问题^[33]。如何建立有效的信任机制以应对节点入侵问题是仍需关注的研究方向。

3.3 资源和任务

增强现实（AR, augmented reality）是超可靠低时延通信的典型使用之一。由于用户设备的能力有限，很难满足严苛的延时要求，需要将计算任务卸载到附近的 MEC 服务器上，借助计算节点的计算能力减少通信延迟和提高计算成功的可靠性。在超可靠低延迟通信（URLLC）和海量机器通信（mMTC）的场景下，多用户多域 MEC 服务协作场景面临的安全威胁将对网络层面有限的资源配置提出新的挑战。

使用 MEC 卸载的服务成功率由 3 部分组成，即排队成功率、传输成功率和计算成功率。其中，排队成功率取决于时延约束条件下排队等待时长和排队方式；传输成功率受信道环境质量和编解码成功率的影响；计算成功率由移动终端设备和服务器 CPU 硬件/软件故障出现的概率所决定。由于每个子任务的输出数据大小通常远小于输入数据，因此忽略下行链路传输引起的时延和失败概率^[34-35]。一方面，如何保证多用户卸载场景下的队列安全

是成功卸载的关键问题。另一方面, Soret 等^[36]指出低时延和高可靠性是相互竞争的两个需求。在网络资源有限, MEC 服务器节点计算、存储和能源有限的前提下, 如何应对多用户卸载场景恶意卸载行为导致网络瘫痪的问题是值得研究的方向。比如, 在图 3 中, UE1、UE2、UE3 根据自己的通信需求做出卸载决策, 然后将计算任务卸载到 MEC 服务器上进行计算。UE1、UE2 被感染为僵尸网络主机, 对 MEC1 服务器展开大量任务卸载行为, UE3 并无卸载任务到 MEC2, MEC2 空闲, 而 MEC1 瘫痪。

3.4 迁移安全

在“万物互联”的愿景下, 5G 可以实现控制端与被控端之间远程跨域互联, 为工业 4.0 提供远程工业控制的全方位支持, 同时可以为远程医疗、远程操作驾驶等高精度、高可靠、高延迟要求的网络业务提供现实的技术支持。这些技术可以使偏远地区的人们享受经济发达地区的医疗技术, 实现社会资源某种程度上的资源共享。在这种场景下, 用户在移动场景下进行计算卸载可能会带来切换 MEC 服务器的问题, 从而带来服务

区域重定位问题。在区域重定位情况下, 移动设备频繁的加入或退出对网络资源管理产生影响, 对实时资源管理提出新的挑战。与此同时, 攻击者瞄准 MEC 节点进行攻击(如中间人攻击), 导致 VM 执行了错误的迁移使 MEC 服务节点失效。具体而言, 动态场景下的卸载污染 MEC 服务器防御挑战来源于以下 3 个方面: 一是计算资源受限, 大量卸载任务迁移至某个特定 MEC 服务器, 导致 MEC 服务器瘫痪; 二是 MEC 自身防御能力有限, 能耗、效率和计算能力有限; 三是动态攻击场景导致攻防博弈资源动态变化, 需要设计资源受限前提下的动态安全防御机制。

4 安全解决方案

针对上述提出的 MEC 安全问题, 本节从设备安全、节点安全、资源和任务和迁移安全 4 个方面总结了现有研究和可能的解决方案。

4.1 设备安全

随着物联网技术的发展, 智慧城市、智能交通等应用将成为 MEC 应用的主战场, 大量智能

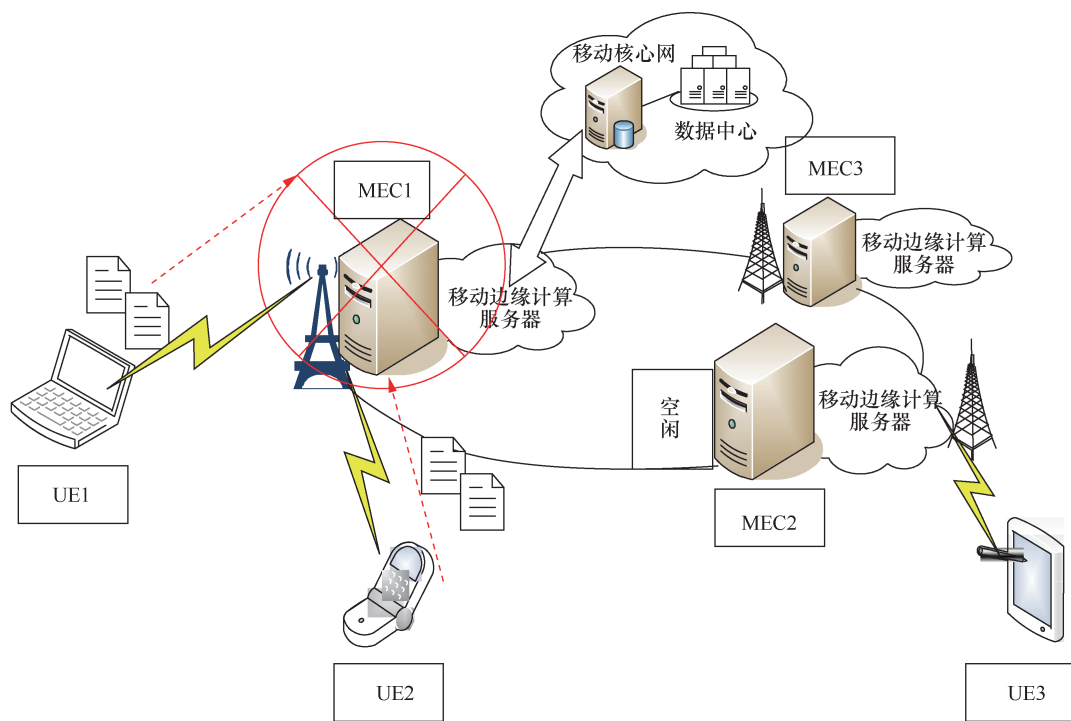


图3 域内多用户卸载场景导致服务节点瘫痪
Figure 3 The multi-user offloading causes service node failure

移动设备(个人穿戴设备、智能手机、自动驾驶车辆)的安全不容忽视^[37]。2016年, Mirai 僵尸网络的出现使近 250 万台物联网设备被感染, 动态脚本的不断更新也不断提高抵御恶意 DDoS 攻击的难度^[38]。对于设备安全带来的安全风险问题的解决方案大致分为 3 类: 一是在大规模用户数量的网络中采用博弈论理论进行研究^[39-41]; 二是从用户固定拓扑上交互动流行病传播的图特征进行研究^[38,42-43]; 三是引入深度学习等人工智能的方法从设备端进行合理卸载决策以平衡网络资源和提高网络服务可靠性进行研究^[44-46]。

文献[41]首先设定了一个联合 MEC 架构的 D2D 通信范例, 并基于平均场博弈理论针对恶意软件的检测和能量消耗代价来确定最佳的网络路径。在该范例中, MEC 服务器作为用户层和云层的中间层, 每个 MEC 服务器用于处理域内的用户终端请求。攻击者可以通过劫持用于用户代理和 MEC 之间的链路启动中间人攻击(MITM), 通过使用有效凭证或特权同用户代理进行交互, 利用恶意软件注入一个假的回复, 将其发送回数据请求者, 以感染用户的设备。Panaousis 等引入了完全信息博弈中的双矩阵博弈, 对攻击者和防御者分别定义收益函数。防御者通过斯塔克尔伯格混合策略选择合适的应答路径找到请求者, 设计了一个反应式路由选择协议应对在理性“攻击者”存在下, 最大化防御者的效用。文献[39]利用生物病毒和计算病毒之间的强相似性, 将传染病模型应用于计算机研究。文献[42]将病毒在网络中的传播精确建模为真实的网络图进行分析。Xu 等^[43]聚焦于存在攻击者前提下无线网络运营商在通信和计算服务的效用最大化。该方法定义了个体用户在预见性可调风险下的参与激励机制, 在引入传染病(SIS, susceptible-infected-susceptible)模型的基础上, 将用户节点分为两种状态。(1) 正常状态: 即可以提供服务和进行请求, 被感染为另一个状态的概率为 β 。(2) 感染状态: 即只能进行请求, 但可以通过请求攻击感染其他节点, 不能进行服务, 并且该节点恢复正常的时间服从指数分布该算法。该方法同时设计了用户提前获取网络状态进行预判参与度的机制, 使用户不仅能对运营商的决策做出最佳反应,

还能对相互依存的安全风险进行博弈。当且仅当用户存在风险(服务器受损请求机会)足够低时, 才会参与对网络其他节点的卸载服务, 从而最大化网络收益。此外, 文献[38]结合了传染病模型和平均场博弈理论, 针对设备安全中的恶意软件传播问题, 设计了基于平均场博弈理论的安全防御机制。Liang 等^[44]对密集环境下多个无线设备向一个边缘服务器进行卸载的情况进行了分析, 提出了一种基于分布式深度学习的设备终端移动边缘计算卸载决策方法, 用梯度下降算法对终端能耗和卸载时延的最优化进行求解。Wu 等^[45]从保护设备隐私安全的角度出发, 通过综合评估、过滤为终端设备选择合适的资源提供者, 提出了一个基于设备安全的感知任务卸载框架, 帮助设备选择合适的卸载策略。He 等^[46]将研究拓展到车联网领域, 综合考虑网络缓存能力和计算能力, 提出了一种深度强化学习的资源优化方法。针对移动边缘计算的设备安全问题, 不仅需要考虑攻击感染的传播模型, 还需要结合终端设备的有限计算资源和防御能力, 引入恰当的数学模型求得特定环境下的网络-用户联合最大收益的防御策略。

4.2 节点安全

对于节点安全, 可通过扩展信任构建模型来应对节点入侵的安全威胁。在移动云计算的领域, 已有大量文献对信任关系的判定对节点安全的影响展开了相关研究^[47-53]。但由于网络设计需求, 移动边缘服务器面临大量异构终端节点通过业务请求接入网络, 为其提供资源访问、存储和计算的通信过程。面对域内恶意网络参与者进行节点入侵前提下成功完成卸载服务计算, 需要建立合理的信任机制帮助服务计算节点筛选合法的卸载用户, 帮助终端用户选择合适的服务计算节点。基于这两点, 需要研究移动边缘计算的信任保障问题以解决接入安全。就前者而言, 在信任度及信任节点的判定问题上, 可以从节点的特殊属性入手进行判定, 如 MEC 服务器节点的流量属性、社交属性等。基于测量理论, Ruan 等^[54]提出了一个基于流量异常度检测的节点信任管理框架, 用于接入应用和计算资源。该方法将信任度分为可信度(trustworthiness)和置信度(confidence), 综合考虑某个节点的输入流量和输

出流量,引入了误差传播理论,并在测量理论的基础上,设计了一个信任管理框架;然后进一步考虑在冗余情况下,分析了信任管理系统为管理员动态分配资源以权衡迁移开销和可靠性之间的动态配置问题。He等^[55]用社交网络的本质属性来优化分配网络资源,利用信道状态、计算能力、容量索引、版本信息、信任状态矩阵作为输入,采用Tensorflow的深度Q学习方法提出了一种新颖的基于信任的大数据增强深度学习方法,考虑了社会关系对于信任度的影响和网络总收益的影响。就后者而言,邓晓衡等^[56]通过对边缘计算单元进行信任属性判定,构建资源和身份信任、行为信任评价机制,根据应用需求研究资源调度算法,联合可用性、访问时间、计算能力等属性综合评估,选择合适的MEC服务器进行任务卸载,主动剔除被污染的卸载计算节点。但实际情况下,综合信任度的评估需要依据完整的历史行为以及资源对不同需求的匹配度和完成情况进行综合计算。此外,He等^[57]重点考虑了基于信任的MEC和D2D的移动社交网络这一具体应用场景。作者提出一个社会信任计划,以提高移动社交网络(MSN, mobile social networks)的安全性。Hussain等^[58]提出了一个可以使用户匿名评价cloudlet的系统,用于存储和管理对LTE部署下移动边缘数据中心声誉。Kantert等^[59]针对不同管理域的服务器共享资源的问题,分别设计了自主和分布式的信任度计算方法,用于服务节点之间信任度的评估和管理。

针对节点失效的故障恢复方法,相关研究者设计了一系列方式进行深入研究。对某个特定MEC服务器卸载大量计算任务或恶意过度进行卸载,造成MEC中服务器之间的工作负载资源过度供应,导致卸载污染节点服务失效问题,Tham和Chattopadhyay^[60]对无线自组织网络(Ad hoc)无线信道容量和链路容量约束竞争关系,将边缘节点间的负载均衡问题表示为一个最大最小优化问题,其目标是在满足无线信道容量和链路争用约束的前提下最小化等待时延。作者使用拉格朗日法和梯度下降法对凸优化问题进行求解,提出了一种分布式且快速收敛的负载均衡算法。Roberto等^[61]针对两个数据服务节点相互交换计

算请求开展合作,以应对其中一个缓冲区超载问题。如果服务请求到达一个请求缓冲区已满的数据中心,数据服务节点在评估后将其转发给另一个合作的数据中心,以减小服务阻塞概率和服务延迟。Ugwuanyi等^[62]设置3种请求模式(过度需求、不安全请求、时间可行性)的资源分配方式,利用银行家算法(Banker算法)保证任务等待序列的安全性,确保不造成僵局以避免死锁的情况发生,但不能对业务的时延进行有效的保证。Satria等^[63]分两种情况对单点失效的故障恢复进行讨论:一是传输范围内有可用邻居MEC节点时直接向备份节点进行传输;二是传输范围无可用邻居MEC节点相邻作为自组织中继节点通过弗洛伊德算法寻找最短路径。该方法的创新点在于分两种情况进行备份计算节点选择讨论,提出了两种MEC服务器故障恢复算法,适用于密集型网络。但弗洛伊德算法复杂度高(O^3),不适合大数据量的计算,并且无法保证严格时延要求下的时延要求,只适用于MEC服务器密集型网络,具有局限性。

MEC现有研究大多聚焦在能耗与时延的资源分配优化问题上,却少有关节点安全和故障恢复机制。对于信任机制的构建,需要建立用户、MEC服务节点、MEC应用和MEC系统之间的信任关系,对终端用户的节点属性、任务属性进行判定,对计算服务节点的计算能力和网络环境状态进行判定,以便为5G开放网络的合法用户提供服务。另外,应该进行安全路由和冗余路径的安全机制设计以应对复杂节点入侵情况下的网络安全威胁。

4.3 卸载服务安全

对于移动边缘计算中有限的网络资源面临卸载攻击时导致的任务卸载失败问题,一方面考虑制定合理的任务排队机制保证队列安全;另一方面合理设计卸载用户占用服务器等网络资源的竞争算法,确保恶意卸载情况下的卸载安全。

在现有研究中,将MEC计算服务器视作先来先服务服务器(FCFS, first come first server)。在传统通信系统中,为保证不同用户的服务需求,每个用户的计算任务以串行方式进行排队。但为

了均衡忙闲时不同计算节点的计算任务, 高效利用资源, 在文献[64]中对每个用户任务到达过程服从泊松过程并且数据包具有相同大小的任务场景下, 提出了基于统计复用的服务器排队方式。虽然文献[65]规定在 URLLC 场景中, 每个短数据包包含 20 个字节, 统计复用的方式可以在保证数据包计算质量的前提下相比单独服务器排队方式减少使用带宽资源, 但在实际情况中, 数据包长短的差异将会给计算排队等待时延带来不容忽视的影响。除了排队方式会影响任务队列长度从而影响卸载时延和服务可靠性以外, 更需要考虑时延约束对于任务排队长度的影响。现有的 MEC 文献中, 绝大多数把平均延迟作为性能指标或服务要求, 关心如何保持平均速度任务队列的稳定性, 即确保有限的平均队列随着时间的推移而变长^[66]。在保持队列长度稳定性研究中, 文献[67]研究了 MEC 架构下网络约束的延迟性能对通信等待时间和计算等待时间、计算服务器稳定性的影响。但在 URLLC 场景下, 需要考虑极端队列长度下的情况。Liu 等^[68]考虑了多用户 MEC 架构下多个计算服务器下的本地计算资源分配问题。通过引用极值理论利用概率约束来统计本地计算和卸载计算的队列长度, 然后利用 Lyapunov 随机性优化^[69]和匹配理论设计一个双时间框架关联卸载资源分配方案, 在每个时隙为用户和服务器的任务卸载和资源分配制定不同的服务策略。模拟结果表明, 在服务器具有不同计算能力前提下, 该方法在部分卸载任务场景下可以降低延迟。在网络安全层面中, 根据业务需求选择 MEC 服务器适当的排队方式, 以达到在时延或能耗约束下的队列安全, 从而保证超可靠低时延场景下的卸载服务成功率是下一步研究的重点。

在恶意网络参与者进行过度卸载或恶意卸载时, 移动设备可能会在网络中彼此竞争有限的计算资源, 以确保自己的服务得到保证。服务器可以与其他服务器竞争争取更多的卸载任务数量, 以更充分地利用网络资源。这个过程类似于市场经济中的价格博弈, 计算资源空闲的服务器可以以较低的服务价格来吸引移动用户设备将任务卸载到服务器上, 而计算资源饱满的服务器可以要求移动用户设备以更高的价格进行卸载, 从而在

反复博弈的过程中使网络计算资源分配达到均衡, 从而达到提高卸载服务安全的目标。博弈论作为数学经典工具已经成熟地运用于无线资源分配问题, 在以提高卸载服务安全为目标的 MEC 多用户卸载的计算资源管理中同样引起了一定的关注^[46,70-75]。博弈论被分为两大分支, 即合作博弈和非合作博弈。对于合作博弈理论, 如联盟博弈, 是以同盟、合作的方式进行博弈, 以共同利益的最大化为目标。非合作博弈研究策略环境下自主决策以谋求实现有效的平衡点。在合作博弈中, 文献[76]引入具有外部性的联盟博弈理论来优化资源分配策略。在管理层, 策略配置管理器根据自适应容量管理器提供的控制信号做出决策, 以最大化 QoE 和实时物联网应用的低延迟要求为优化目标, 提出了先验多标准优化方法, 将目标函数根据重要性进行分类, 设计了双目标优化方法保证 MEC 服务器自适应地提供可用的计算资源以满足物联网应用的服务质量要求。文献[77]旨在有延迟截止时间的应用程序卸载中, 为移动设备选择合适的 MEC 服务器进行卸载, 以使在期限内达到最大化任务处理量。Liu 等设计了基于合作博弈的卸载策略以保障服务质量, 并证明了返回的解决方案是帕累托最优。在非合作博弈中, 文献[78]引入了少数者博弈 (MG, minority game) 理论用于解决 MEC 中分布式资源配置问题。Ranadheera 等不仅聚焦于如何满足用户时延的需求和最小化能耗消耗, 而且从服务器和用户的混合视角解决了用户需求的不确定性和由于信道质量随机性引起的不确定性问题。文章通过将计算卸载问题建模为价格市场, 设计选择机制保证在最少服务器激活状态下满足能源效率和用户的延迟要求。这种方法不需要服务器端任何的先验信息, 可以在分布式环境中与其他服务器非协调的情况下, 以较少的外部信息做出决策。文献[79]针对车联网场景中使用 MEC 进行计算卸载的情况下, 使用分层的 MEC 网络部署架构, 将服务器和车辆用户视为领导者和追随者, 以最大化用户和服务器使用效率为目标, 根据斯塔伯格博弈理论设计了多层级的卸载机制, 并证明了纳什均衡的存在性。博弈论卸载服务安全研究现状如表 2 所示。

博弈论提供了多种理论模型,针对不同的使用场景和优化目标可以为某个特定需求提供理论支持。除了考虑用户卸载决策、服务器端使用效率以外,还需要考虑服务器协作方式下不同 MEC 架构部署下移动边缘计算网络安全环境下的卸载决策和资源分配的部署方式。同时,不同的目标函数设定方法和加权参数的选择也会对总代价计算方式产生不同的影响,并且需要综合考虑每个计算任务的服务质量要求、结合实际进行动态的资源分配方案。

4.4 迁移安全

针对计算迁移可能带来的中间人攻击、分布式拒绝攻击等安全威胁,从两个角度解决计算迁移情况下的 MEC 安全威胁问题:一是挖掘移动性规律,根据用户属性进行移动轨迹预测,提前判别可能的计算迁移目的地 MEC 服务节点,从而避免错误迁移,减小攻击成功可能性;二是结合动态博弈模型,设计有限网络节点的资源消耗情况下的合理迁移卸载防御型。

从用户的移动属性入手,设计动态适应的资源部署方案以应对服务迁移对 MEC 环境下 URLLC 场景产生的影响。为保证用户在移动情况下的计算卸载服务质量,始终保证服务的最佳端到端连接,研究者提出了一种针对互操作分散式移动网络/联合云的 MEC 部署框架——FMC (follow-me cloud)^[80]。FMC 支持跨域联合数据中心 (DC, data center) 的服务移动性。它不仅允许内容在移动时跟随用户,而且允许服务本身始终连接到最佳的接入锚点和移动网关,以确保移动情况下用户计算卸载的服务延迟、可靠性等体验。在 FMC 框架下,为解决服务迁移成本和用户感知质量的权衡问题,现有研究^[76-83]集中采用马尔可夫决策过程 (MDP, Markov decision process) 对服务迁移过程进行建模,制定迁移决

策,在提高用户服务体验的前提下寻求服务迁移成本和收益的平衡点。文献[81]定义了一个一维连续时间马尔可夫决策过程 (CTMDP, continuous time markov decision process),用户在每个状态以相应的概率选择是否移动到远距离边缘服务器,以最优收益函数值为目标,实现 FMC 控制器可以做出最佳的是否需要迁移服务的决策,以提高用户的服务体验。为了普遍使用于实际场景,文献[83-84]提出了二维的 MDP 模型,对移动用户在某一 2D 区域中的移动进行了建模。为了进一步降低计算复杂度,文献[82]使用移动用户和服务器之间的距离作为状态空间,并将用户一维移动性扩展到二维移动性,用旧金山出租车的真实移动轨迹对所提出的新型算法进行了评估,结果表明,实际场景下该方法计算时间明显优于传统基于标准值或迭代的方法。

另外,从如何使用有限的网络节点资源入手建立博弈模型,解决安全防御问题。Wu 等^[85]将攻击者和防御者之间的交互模型看作非零和博弈,通过静态博弈模型和动态博弈模型分别计算纳什均衡,求得防御者的最佳策略,并用 NS-3 验证博弈论防御机制的有效性。同样以防御者选择最优策略为目标,文献[86]基于希尔伯特空间定义个体成本函数和网络成本函数,通过求解纳什均衡得到网络总成本函数的最优解,利用平均场博弈理论求得动态资源消耗和攻击强度下的最佳防御策略。

MEC 可以在 5G 网络下通过计算卸载保证用户移动场景中服务连续性,但同时考虑计算迁移过程中可能带来的安全威胁。保证计算迁移的正确性,合理调配动态场景下防御资源随攻击强度的变化,并结合有限的节点资源,设计有效的域间动态场景移动边缘计算防御机制是下一步研究的重点。

表 2 博弈论卸载服务安全研究现状
Table 2 Research status of service offloading security based on game theory

参考文献	类型	优化目标	理论模型	应用场景
文献[76]	合作	资源利用效率和服务质量	联盟博弈	Edge IoT
文献[77]	合作	最大化期限内任务数量	近线性规划,合作博弈	延迟截止时间
文献[78]	非合作	服务器能耗和服务质量	少数者博弈	分布式场景
文献[79]	非合作	最大化用户和服务器的使用效率	斯塔科尔伯格博弈	车联网

5 开放性问题

5.1 动态场景下的有限资源防御模型

MEC 服务器可以使用户将繁重的计算任务卸载到服务计算节点上,从而减小计算的等待时延和提高计算的成功率。但相比 4G 网络,在移动场景下,由于网络中引入了 MEC 服务器这一新的实体,对用户频繁移动情况下服务连续性保证提出了新的挑战。特别是在存在计算迁移的场景下,如何利用 MEC 服务器资源进行攻防博弈、在多个服务计算节点间设计合理的协作方式,以及综合考虑时延、可靠性、能耗等特殊服务质量要求下的安全防护方案,是需要进一步研究的方向。

5.2 综合信任基础的资源部署问题

5G 允许多种接入模式和多元身份管理,更允许以点对点的模式进行交互管理。这一新的认证方式的转变同样带来了 MEC 计算卸载和计算迁移中的信任问题。如何利用边缘节点网络本质属性进行信任度评价,选择可靠的节点进行计算卸载,是满足超可靠低时延场景中用户服务可靠性要求的关键问题。另外,针对特定的网络架构,从宏观上设计合理的认证框架和资源配置方式,建立完整的信任系统,在满足用户服务质量的前提下提高网络安全防御能力。

5.3 以用户为中心的服务可靠性保证问题

文献[87]指出网络服务提供者需要关注的关键问题是网络可靠性、网络可用性以及网络故障处理能力。5G 时代力求满足“以用户为中心”,服务的可获得性是第一要求。除了满足用户体验速率、业务端到端时延以外,还应重点考虑超可靠低时延中对于可靠性的特殊要求。现有的 MEC 研究中,任务卸载产生的能耗不容忽视,能耗-延迟的均衡研究得到极大的关注,而很少考虑安全问题。对网络的可靠性和可用性设计是基本要求,进一步要考虑运营商连接数量大幅增加、用户终端设备种类更加复杂情况下的网络资源消耗和服务中断故障处理能力,做到在能源消耗不增加的前提下灵活地配置网络资源,以满足以用户为中心的网络安全保障。

6 结束语

移动边缘计算作为数据驱动服务技术,通过

推动计算、存储和本地应用到网络边缘,显著提高了传统通信的网络连接和与终端设备之间的资源利用,从而减小计算时延和提高计算成功率。在 MEC 带来便捷服务的同时,安全成为下一步亟待关注的重要研究方向。目前,针对移动边缘计算的大部分研究处于如何均衡能耗、延迟和开销,而较少关注安全问题。但 MEC 节点由于暴露在网络边缘且服务计算节点的资源有限,容易成为恶意网络参与者的攻击目标。本文从计算卸载面临的安全威胁、关键问题和挑战,以及现有的解决方案等角度出发,阐述了移动边缘计算的安全防御研究现状,并讨论了下一步可能的研究方向。

参考文献:

- [1] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—a key technology towards 5G[J]. ETSI White Paper, 2015, 11(11): 1-16.
- [2] MACH P, BECVAR Z. Mobile edge computing: a survey on architecture and computation offloading[J]. IEEE Communications Surveys & Tutorials, 2017, PP(99):1-1.
- [3] WANG Y, CHEN I R, WANG D C. A survey of mobile cloud computing applications: perspectives and challenges[J]. Wireless Personal Communications, 2015, 80(4): 1607-1623.
- [4] LEIGHTON F T, LEWIN D M. Content delivery network using edge-of-network servers for providing content delivery to a set of participating content providers: U.S. Patent 6553413[P]. 2003.
- [5] ROMAN R, LOPEZ J, MAMBO M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, 78: 680-698.
- [6] KW AK J, KIM Y, LEE J, et al. DREAM: dynamic resource and task allocation for energy minimization in mobile cloud systems[J]. IEEE J Sel Areas Commun, 2015, 33(15): 2510-2523.
- [7] KIM Y, KWAK J, CHONG S. Dual-side optimization for cost-delay tradeoff in mobile edge computing[J]. IEEE Trans Veh Technol, 2018, 67(2): 1765-1781.
- [8] JIANG Z, MAO S. Energy delay tradeoff in cloud offloading for multi-core mobile devices[J]. IEEE Access, 2015, (3): 2306-2316.
- [9] MAO Y, ZHANG J, SONG S H, et al. Power-delay tradeoff in multi-user mobile-edge computing systems[C]//Proc IEEE Global Commun Conf, 2016: 5994-6009.
- [10] MAO S, LENG S, YANG K, et al. Energy efficiency and delay tradeoff in multi-user wireless powered mobile-edge computing systems[C]//Proc IEEE Global Commun Conf. 2017: 1-6.
- [11] XU J, CHEN L, REN S. Online learning for offloading and autoscaling in energy harvesting mobile edge computing[J]. IEEE Trans Cogn Commun Netw, 2017, 3(3): 361-373.
- [12] SUN Y, ZHOU S, XU J. EMM: energy-aware mobility management for mobile edge computing in ultra dense networks[J]. IEEE J

- Sel Areas Commun, 2017, 35(11): 2637-2646.
- [13] KO S, HAN K, HUANG K. Wireless networks for mobile edge computing: spatial modeling and latency analysis[J]. IEEE Trans Wireless Commun, 2018, 17(8): 5225-5240.
 - [14] DENG R, LU R, LAI C, et al. Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption[J]. IEEE Internet Things J, 2016, 3(6): 1171-1181.
 - [15] LEE G, SAAD W, BENNIS M. An online secretary framework for fog network formation with minimal latency[C]//Proc IEEE Int Conf Commun. 2017: 1-6.
 - [16] FAN Q, ANSARI N. Workload allocation in hierarchical cloudlet networks[J]. IEEE Commun Lett, 2018, 22(4): 820-823.
 - [17] MOLINA M, MUÑOZ O, PASCUAL-ISERTE A, et al. Joint scheduling of communication and computation resources in multiuser wireless application offloading[C]//Proc IEEE 25th Annu Int Symp Pers Indoor, Mobile Radio Commun. 2014: 1093-1098.
 - [18] ZHANG H, XIAO Y, BU S, et al. Computing resource allocation in three-tier IoT fog networks: a joint optimization approach combining Stackelberg game and matching[J]. IEEE Internet Things J, 2017, 4(5): 1204-1215.
 - [19] ANG Y, CHANG X, HAN Z, et al. Delay-aware secure computation offloading mechanism in a fog-cloud framework[C]//2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/ SocialCom/ SustainCom). 2018: 346-353..
 - [20] STOJMENOVIC I, WEN S, HUANG X, et al. An overview of fog computing and its security issues[J]. Concurrency and Computation: Practice and Experience, 2016, 28(10): 2991-3005.
 - [21] FORD R, SRIDHARAN A, MARGOLIES R, et al. Provisioning low latency, resilient mobile edge clouds for 5G[C]//2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2017: 169-174.
 - [22] CHOO K K R. Cloud computing: challenges and future directions, trends & issues in crime and criminal justice[R]. 2010.
 - [23] LANDAU S. Highlights from making sense of snowden, part II: what's significant in the NSA revelations[J]. IEEE Security & Privacy, 2014, 12 (1): 62-64.
 - [24] YI S, QIN Z, LI Q. Security and privacy issues of fog computing: a survey[M]//Wireless Algorithms, Systems, and Applications, Bellin: Springer International Publishing, 2015: 685-695.
 - [25] FORD R, SRIDHARAN A, MARGOLIES R, et al. Provisioning low latency, resilient mobile edge clouds for 5G[C]//2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2017: 169-174.
 - [26] STOJMENOVIC I, WEN S, HUANG X, et al. An overview of fog computing and its security issues[J]. Concurrency and Computation: Practice and Experience, 2016, 28(10): 2991-3005.
 - [27] FENG D, LU L, WUY Y, et al. Device-to-device communications in cellular networks[J]. IEEE Commun Mag, 2014, 52(4): 49-55.
 - [28] NISHIYAMA H, ITO M, KATO N. Relay-by-smartphone: realizing multihop device-to-device communications[J]. IEEE Commun Mag, 2014, 52(4): 56-65.
 - [29] TEHRANI M, UYSAL M, YANIKOMEROGLU H. Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions[J]. IEEE Commun Mag, 2014, 52(5): 86-92.
 - [30] FODOR G, DAHLMAN E, MILDH G, et al. Design aspects of network assisted device-to-device communications[J]. IEEE Commun Mag, 2012, 50(3): 170-177.
 - [31] DOPPLER K, RINNE M, WIJTING C, et al. Device-to-device communication as an underlay to LTE-advanced networks[J]. IEEE Commun Mag, 2009, 47(12): 42-49.
 - [32] ANGIN P, BHARGAVA B, JIN Z. A self-cloning agents based model for high-performance mobile-cloud computing[C]//Proc. IEEE 8th Int Conf Cloud Comput (CLOUD). 2015: 301-308.
 - [33] WANG S, XU J, ZHANG N, et al. A survey on service migration in mobile edge computing[J]. IEEE Access, 2018, 6: 23511-23528.
 - [34] CHEN X, JIAO L, LI W, et al. Efficient multi-user computation offloading for mobile-edge cloud computing[J]. IEEE/ACM Trans Netw, 2016, 24(5): 2795-2808.
 - [35] WANG C, YU F R, LIANG C, et al. Joint computation offloading and interference management in wireless cellular networks with mobile edge computing[J]. IEEE Trans Veh Technol, 2017, 61(8): 7432-7445.
 - [36] SORET B. Fundamental tradeoffs among reliability, latency and throughput in cellular networks[C]//Proc IEEE Global Telecommun. Conf (GLOBECOM) Workshops. 2014: 1391-1396.
 - [37] WANG B, LI M, JIN X, et al. A reliable IoT edge computing trust management mechanism for smart cities[J]. IEEE Access, 2020, 8: 46373-46399.
 - [38] MIAO L, LI S. Cyber security based on mean field game model of the defender: Attacker strategies[J]. International Journal of Distributed Sensor Networks, 2017, 13(10): 1550147717737908.
 - [39] KEPHART J O, WHITE S R. Directed-graph epidemiological models of computer viruses[M]//Computation: the Micro and the Macro view. 1992: 71-102.
 - [40] RANADHEERA S, MAGHSUDI S, HOSSAIN E. Mobile edge computation offloading using game theory and reinforcement learning[J]. arXiv preprint arXiv:1711.09012, 2017.
 - [41] PANAOUSIS E, KARAPISTOLI E, ELSEMARY H, et al. Game theoretic path selection to support security in device-to-device communications[J]. Ad Hoc Networks, 2017, 56: 28-42.
 - [42] WANG Y, CHAKRABARTI D, WANG C, et al. Epidemic spreading in real networks: an eigenvalue viewpoint[C]//22nd International Symposium on Reliable Distributed Systems, 2003. Proceedings. 2003: 25-34.
 - [43] XU J, CHEN L, LIU K, et al. Designing security-aware incentives for computation offloading via device-to-device communication[J]. IEEE Transactions on Wireless Communications, 2018, 17(9): 6053-6066.
 - [44] LIANG H, XU F, ANQI F, et al. Distributed deep learning-based offloading for mobile edge computing networks[J]. Mobile Networks and Applications, 2018.
 - [45] WU D, SHEN G, HUANG Z, et al. A trust-aware task offloading framework in mobile edge computing[J]. IEEE Access, 2019, 7: 150105-150119.

- [46] HE Y, ZHAO N, YIN H. Integrated networking, caching, and computing for connected vehicles: a deep reinforcement learning approach[J]. *IEEE Transactions on Vehicular Technology*, 2018, 67(1): 44-45.
- [47] PETRI I, RANA O F, REZGUI Y, et al. Trust modelling and analysis in peer-to-peer clouds[J]. *International Journal of Cloud Computing*, 2012, 1(2-3): 221-239.
- [48] CHEN S, WANG G, JIA W. A trust model using implicit call behavioral graph for mobile cloud computing[M]//*Cyberspace Safety and Security*. Cham: Springer, 2013: 387-402.
- [49] FIGUEROA M, UTTECHT K, ROSENBERG J. A sound approach to security in mobile and cloud-oriented environments[C]//2015 IEEE International Symposium on Technologies for Homeland Security (HST). 2015: 1-7.
- [50] BENNANI N, BOUKADI K, GHEDIRA-GUEGAN C. A trust management solution in the context of hybrid clouds[C]//2014 IEEE 23rd International WETICE Conference. 2014: 339-344.
- [51] JANG M, LEE H, SCHWAN K, et al. SOUL: an edge-cloud system for mobile applications in a sensor-rich world[C]//2016 IEEE/ACM Symposium on Edge Computing (SEC). 2016: 155-167.
- [52] ECHEVERRÍA S, KLINEDINST D, WILLIAMS K, et al. Establishing trusted identities in disconnected edge environments[C]//2016 IEEE/ACM Symposium on Edge Computing (SEC). 2016: 51-63.
- [53] CICIRELLI F, GUERRIERI A, SPEZZANO G, et al. Edge computing and social internet of things for large-scale smart environments development[J]. *IEEE Internet of Things Journal*, 2017, 5(4): 2557-2571.
- [54] RUAN, YEFENG, ARIAN DURRESI, et al. Trust assessment for internet of things in multi-access edge computing[C]//2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). 2018.
- [55] HE Y, LIANG C, YU F, et al. Integrated computing, caching, and communication for trust-based social networks: a big data driven approach[C]//2018 IEEE Global Communications Conference (GLOBECOM). 2018.
- [56] 邓晓衡, 关培源, 万志文, 等. 基于综合信任的边缘计算资源协同研究[J]. *计算机研究与发展*, 2018, 55(3): 449-477.
- DENG X H, GUAN P Y, WAN Z W, et al. Integrated trust based resource cooperation in edge computing[J]. *Journal of Computer Research and Development*, 2018, 55(3): 449-477.
- [57] HE Y, YU F R, ZHAO N, et al. Secure social networks in 5G systems with mobile edge computing, caching, and device-to-device communications[J]. *IEEE Wireless Communications*, 2018, 25(3): 103-109.
- [58] HUSSAIN M, ALMOURAD B M. Trust in mobile cloud computing with LTE-based deployment[C]//2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops. 2014: 643-648.
- [59] KANTERT J, EDENHOFER S, TOMFORDE S, et al. Representation of trust and reputation in self-managed computing systems[C]//2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. 2015: 1827-1834.
- [60] THAM C K, CHATTOPADHYAY R. A load balancing scheme for sensing and analytics on a mobile edge computing network[C]//2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). 2017: 1-9.
- [61] BERALDI R, MTIBAA A, ALNUWEIRI H. Cooperative load balancing scheme for edge computing resources[C]//2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). 2017: 94-100.
- [62] UGWUANYI E E, GHOSH S, IQBAL M, et al. Reliable resource provisioning using Bankers' deadlock avoidance algorithm in MEC for industrial IoT[J]. *IEEE Access*, 2018, 6: 43327-43335.
- [63] SATRIA D, PARK D, JO M. Recovery for overloaded mobile edge computing[J]. *Future Generation Computer Systems*, 2017, 70: 138-147.
- [64] SHE C, YANG C, QUEK T Q S. Joint uplink and downlink resource configuration for ultra-reliable and low-latency communications[J]. *IEEE Transactions on Communications*, 2018, 66(5): 2266-2280.
- [65] 3GPP. Study on scenarios and requirements for next generation access technologies[S]. TSG RAN TR38.913 R14, 2017.
- [66] NEELY M J. Stochastic network optimization with application to communication and queueing systems[R]. 2010.
- [67] KO S W, HAN K, HUANG K. Wireless networks for mobile edge computing: spatial modeling and latency analysis[J]. *IEEE Transactions on Wireless Communications*, 2018, 17(8): 5225-5240.
- [68] LIU C F, BENNIS M, DEBBAH M, et al. Dynamic task offloading and resource allocation for ultra-reliable low-latency edge computing[J]. *IEEE Transactions on Communications*, 2019.
- [69] NEELY M J. Stochastic network optimization with application to communication and queueing systems[R]. 2010.
- [70] DENG M, TIAN H, LYU X. Adaptive sequential offloading game for multi-cell mobile edge computing[C]//2016 23rd International Conference on Telecommunications (ICT). 2016: 1-5.
- [71] ZHENG J, CAI Y, WU Y, et al. Stochastic computation offloading game for mobile cloud computing[C]//2016 IEEE/CIC International Conference on Communications in China (ICCC). 2016: 1-6.
- [72] TEKIN C, VAN DER SCHAAR M. An experts learning approach to mobile service offloading[C]//2014 52nd Annual Allerton Conference on Communication, Control, and Computing. 2014: 643-650.
- [73] XU J, CHEN L, REN S. Online learning for offloading and auto scaling in energy harvesting mobile edge computing[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2017, 3(6): 361-373.
- [74] XU J, PALANISAMY B, LUDWIG H, et al. Zenith: utility-aware resource allocation for edge computing[C]//2017 IEEE International Conference on Edge Computing (EDGE). 2017: 47-54.
- [75] RANADHEERA S, MAGHSUDI S, HOSSAIN E. Computation offloading and activation of mobile edge computing servers: a minority game[EB].

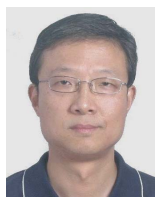
- [76] ALIYU S O, CHEN F, HE Y, et al. A game-theoretic based qos-aware capacity management for real-time edgeiot applications[C]//2017 IEEE International Conference on Software Quality, Reliability and Security (QRS). 2017: 386-397.
- [77] LIU C, LI K, LIANG J, et al. COOPER-MATCH: job offloading with a cooperative game for guaranteeing strict deadlines in MEC[J]. IEEE Transactions on Mobile Computing, 2019.
- [78] RANADHEERA S, MAGHSUDI S, HOSSAIN E. Computation offloading and activation of mobile edge computing servers: a minority game[J]. IEEE Wireless Communications Letters, 2018, 7(5): 688-691.
- [79] ZHANG K, MAO Y, LENG S, et al. Optimal delay constrained offloading for vehicular edge computing networks[C]//2017 IEEE International Conference on Communications (ICC). 2017: 1-6.
- [80] TALEB T, KSENTINI A. Follow me cloud: interworking federated clouds and distributed mobile networks[J]. IEEE Network, 2013, 27(5): 12-19.
- [81] KSENTINI A, TARIK T, CHEN M. A Markov decision process-based service migration procedure for follow me cloud[C]//2014 IEEE International Conference on Communications (ICC). 2014.
- [82] WANG S, URGONKAR R, ZAFER M, et al. Dynamic service migration in mobile edge computing based on markov decision process[J]. IEEE/ACM Transactions on Networking, 2019.
- [83] TARIK T, KSENTINI A. An analytical model for follow me cloud[C]//2013 IEEE Global Communications Conference (GLOBECOM). 2013.
- [84] TALEB T, KSENTINI A, FRANGOUDIS P A. Follow-me cloud: when cloud services follow mobile users[J]. IEEE Transactions on Cloud.
- [85] WU Q, SHIVA S, ROY S, et al. On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks[C]//Proceedings of the 2010 Spring Simulation Conference. Society for Computer Simulation International. 2010: 159.
- [86] MIAO L, WANG L, LI S, et al. Optimal defense strategy based on the mean field game model for cyber security[J]. International Journal of Distributed Sensor Networks, 2019, 15(2).
- [87] KALMANEK C, YANG Y. The challenges of building reliable

networks and networked application services[M]//Guide to Reliable Internet Services and Applications. 2010: 3-17.

[作者简介]



陈璐 (1989-), 女, 河北唐山人, 信息工程大学博士生, 主要研究方向为移动通信网安全、移动边缘计算技术。



汤红波 (1968-), 男, 湖北孝感人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为移动通信网络、新型网络体系结构。



游伟 (1984-), 男, 江西丰城人, 博士, 信息工程大学讲师, 主要研究方向为密码学和移动通信网络。



柏溢 (1975-), 男, 江苏盐城人, 信息工程大学副研究员, 主要研究方向为移动通信网络、新型网络体系结构。