基于Lyapunov优化的隐私感知计算卸载方法

赵 星* 彭建华 游 伟
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：移动边缘计算(MEC)中计算卸载决策可能暴露用户特征，导致用户被锁定。针对此问题，该文提出一种基于Lyapunov优化的隐私感知计算卸载方法。首先，该方法定义卸载任务中的隐私量，并引入隐私限制使各MEC节点上卸载任务的累积隐私量尽可能小；然后，提出假任务机制权衡终端能耗和隐私保护的关系，当系统因隐私限制无法正常执行计算卸载时，在MEC节点生成虚假的卸载任务以降低累积隐私量；最后，建立隐私感知计算卸载模型，并基于Lyapunov优化原理求解。仿真结果表明，基于Lyapunov优化的隐私感知卸载算法(LPOA)能使用户的累积隐私量稳定在0附近，且总卸载频率与不考虑隐私的决策一致，有效保护了用户隐私，同时保持了较低的平均能耗。

关键词：移动边缘计算；计算卸载；卸载决策；隐私保护；Lyapunov优化
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2020)03-0704-08
DOI: 10.11999/JEIT190170

A Privacy-aware Computation Offloading Method Based on Lyapunov Optimization

ZHAO Xing PENG Jianhua YOU Wei
(*National Digital Switching System Engineering R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: The decision on computation offloading to Mobile Edge Computing (MEC) may expose user's characteristics and cause the user to be locked. A privacy-aware computation offloading method based on Lyapunov optimization is proposed in this paper. Firstly, the privacy of task is defined, and privacy restrictions are introduced to minimize the cumulative privacy of each MEC node; Then, the fake task mechanism is proposed to balance the terminal energy consumption and privacy protection, reducing the cumulative privacy of MEC node by generating a fake task non-feature task when offloading is not performed due to privacy restrictions; Finally, the privacy-aware computing offloading decision is modeled and solved based on the Lyapunov optimization. Simulation results validate that the Lyapunov optimization-based Privacy-aware Offloading Algorithm (LPOA) can stabilize user's privacy near zero, and the total offloading frequency is consistent with the decision that don't consider privacy, effectively protecting user's privacy while maintaining a low average energy consumption.

Key words: Mobile Edge Computing (MEC); Computation offloading; Offloading decision; Privacy protection; Lyapunov optimization

1 引言

随着物联网的快速发展和各类智能终端的广泛使用，网络中的数据流量激增；5G新应用场景对网络的时延和处理能力提出了更高的需求，对用户隐私也有更多更严格的限制[1]，现有移动网络及云服务模式难以应对。MEC[2]通过将计算资源部署在网络边缘，就近为用户提供计算任务，有效改善网络环境和降低传输时延。计算卸载技术[3]作为MEC的关键技术，将终端的计算密集型应用卸载到邻近MEC节点上，利用MEC节点丰富的计算资源和充足能源处理任务，缩短任务处理时延和降低终端能耗。

计算卸载技术包括卸载决策、计算资源部署和

收稿日期：2019-03-21；改回日期：2019-08-20；网络出版：2019-09-02
*通信作者： 赵星 ndsc_zx@163.com
基金项目：国家重点研发计划网络空间安全专项(2016YFB0801605)，国家自然科学基金创新群体项目(61521003)，国家自然科学基金(61801515)
Foundation Items: The National Key R&D Program Cyberspace Security Special (2016YFB0801605), The National Natural Science Foundation Innovative Groups Project of China (61521003), The National Natural Science Foundation of China(61801515)

移动性管理[4]，其中卸载决策是指终端感知网络环境并结合自身优化目标，选择最优的计算任务处理方式，具体优化的目标包括降低任务处理时延[5]、在满足时延限制条件下降低终端能耗[6]、权衡任务处理时延与终端能耗[7]。目前针对MEC计算卸载的安全与隐私问题研究较少，多是从加密、认证等数据安全和访问控制角度防护卸载的数据内容[8]，并未充分考虑卸载决策中的隐私问题，对用户卸载的行为习惯、使用模式所导致的隐私泄露研究[9]则更少。

文献[10]通过分析现有卸载决策发现，终端在信道条件较好时尽可能上传计算任务，攻击者可据此通过监听MEC节点上的任务卸载情况反推用户的使用模式和无线环境，甚至实现对终端的定位；文献[11]据此进一步分析了物联网场景计算卸载的位置隐私和使用模式隐私，建立隐私模型综合考虑隐私、能耗和计算时延，并用增强学习算法求解最优的计算卸载和本地处理频率；文献[12]分析了物联网场景中用户的位置隐私威胁，基于越远的服务节点越能保护用户位置隐私的原理定义隐私量，建模权衡计算卸载中隐私保护与电池能耗的关系，并利用深度决策后状态学习算法快速求解最优的卸载决策。文献[13]分析低时延场景下卸载任务跟随用户迁移的轨迹隐私问题，假定攻击者已知目标用户的移动模式，且可入侵MEC节点监听卸载任务的迁移路径，基于极大似然法匹配锁定目标用户。上述文献并未分析用户卸载任务的特征及频率导致的隐私泄露问题，而由于终端和用户的对应关系，用户使用终端应用的行为习惯会通过卸载到MEC节点上的任务类型和频率间接暴露用户的存在。

本文提出一种基于Lyapunov优化的隐私感知计算卸载方法。首先，基于任务卸载概率的显著性定义其隐私量，在卸载模型中引入隐私限制，降低MEC节点的累积隐私量；然后，提出假任务机制，在计算任务因隐私限制而无法正常卸载时在MEC节点上生成虚假任务，既降低了MEC节点的累积隐私量，也使得目标用户对外的卸载总频次保持稳定；最后，建立隐私感知计算卸载模型并用基于Lyapunov优化的隐私感知卸载算法(Lyapunov optimization-based Privacy-aware Offloading Algorithm, LPOA)快速求解。实验结果表明，LPOA能有效降低终端的平均能耗，并保持各MEC节点的累积隐私量靠近0值，使目标用户的外在表现与其他用户相似，防止攻击者的推测和锁定。

2　系统模型及问题分析

本节介绍了多MEC节点场景计算卸载的基本系统模型，定量描述了影响卸载决策的任务处理时延和终端能耗，并分析了现有卸载决策中存在的隐私泄露风险。

2.1　系统模型

由多个MEC节点组成的MEC池如图1所示，多个MEC节点部署于相应的基站或AP上，为邻近的终端用户提供服务，终端可通过连接的基站或AP卸载计算任务。

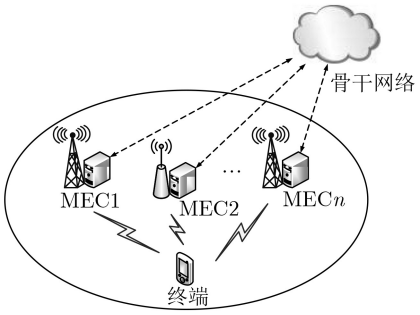


图 1 系统模型

假设整个网络为时隙系统，单位时隙为Δ ms。在每个时隙t内，终端随机产生一个可卸载的任务$T(t)\in\boldsymbol{T}$，其中$\boldsymbol{T}=\{T_1,T_2,\cdots,T_{|\boldsymbol{T}|}\}$是不同卸载任务的集合。假定每个卸载任务平均包含$b$ Byte，终端处理每个字节的数据需要β个CPU循环[14]。每个任务均有时延门限$\xi(t)$，若在规定的时延门限内本地执行或计算卸载都无法完成任务，则任务丢弃。

终端本地处理任务的最大CPU频率为$f_{\max}$，向MEC节点卸载任务的最大天线发射功率为$p_{\max}$。假设终端的CPU频率可以根据不同的卸载决策而改变[15]，时隙t内的CPU频率为$f(t)$，则任务本地处理的时延为$D_{\mathrm{L}}(t)=b\cdot\beta/f(t)$，任务处理的CPU的能耗为$E_{\mathrm{L}}(t)=\kappa\cdot f^3(t)\cdot D_{\mathrm{L}}(t)$，其中$\kappa$表示CPU的能耗系数[16]。

MEC池包含N_{MEC}个MEC节点，假定时隙t内终端向第k个MEC节点执行计算卸载。无线信道参数为：上行链路带宽W，信道噪声功率密度N_0，信道增益为$h_k^2(t)$，终端的发射功率$p_k(t)$。假定MEC节点有充足的计算资源和足够大的发射功率，处理卸载任务的时间和向终端发送处理结果的时延可忽略不计，则计算卸载的时延为$D_k(t)=b/[W\cdot\log_2(1+h^2{}_k(t)\cdot p_k(t)/(W\cdot N_0))]$，传输能耗为$E_k(t)=p_k(t)\cdot D_k(t)$。

综上所述，在时隙t内计算任务$T(t)$的处理时延为$D(t)=I_{\mathrm{L}}(t)\cdot D_{\mathrm{L}}(t)+\sum_{k=1}^{N_{\mathrm{MEC}}}I_k(t)\cdot D_k(t)$，其中$I_{\mathrm{L}}(t)$和$I_k(t),k=1,2,\cdots,N_{\mathrm{MEC}}$为指示函数，$I_{\mathrm{L}}(t)$表示计算任务是否在本地执行，$I_k(t)$表示计算任务是否卸载到第$k$个MEC节点上。

计算任务$T(t)$的处理能耗为$E(t)=I_{\mathrm{L}}(t)\cdot E_{\mathrm{L}}(t)+\sum_{k=1}^{N_{\mathrm{MEC}}} I_k(t)\cdot E_k(t)+I_{\mathrm{D}}(t)\cdot E_0$，其中$I_D(t)$为指示函数，表示计算任务否被丢弃，$E_0$是相应的丢弃代价。计算任务被丢弃一般是由于给定时间门限$\xi(t)$太小或者终端所处位置无线环境较差，导致本地处理和计算卸载都无法满足时间限制。每个时隙t的任务只有本地处理、卸载和丢弃这3种决策结果，因此有

$$I_{\mathrm{L}}(t)+\sum_{k=1}^{N_{\mathrm{MEC}}} I_k(t)+I_{\mathrm{D}}(t)=1 \tag{1}$$

2.2 问题分析

MEC可统计用户卸载的计算任务及其频率为网络资源部署、网络内容缓存等提供数据支撑。由于用户使用习惯的不同，每个用户u的卸载任务种类及其频率也不相同，若攻击者通过其他手段掌握了目标用户(如Bob)的常用卸载任务及其大致卸载概率，则可监听MEC节点上任务卸载情况并推测Bob是否存在于某一MEC节点下。

由于边缘节点的防护资源有限，相比于云数据中心更容易被攻击者发现漏洞并突破，且由于边缘网络的同质性，攻击者发现一个漏洞就可从整个边缘网络监听收集卸载结果，攻击成本低、收益大，攻击结果是否准确可交给后续进一步验证。

利用目标用户卸载频率相对于该任务的平均卸载概率的显著性，可量化计算任务的隐私属性，即用量化的显著性表示计算任务所蕴含的隐私量。采用卸载概率的比值关系反映目标用户的显著性，对于时隙t产生的卸载任务$T(t)$，可定义其隐私量$q(t)$为

$$q(t)=\ln\frac{p^{\mathrm{B}}_{T(t)}}{\bar{p}_{T(t)}} \tag{2}$$

其中，$p^{\mathrm{B}}_{T(t)}$和$\bar{p}_{T(t)}$分别是Bob的任务$T(t)$卸载概率和其他用户的任务$T(t)$平均卸载概率。

若$T(\tau)$为Bob的特征任务，由于$p^{B}_{T(t)}>\bar{p}_{T(t)}$，则$q(t)>0$隐私量为正；反之，则$q(t)<0$，隐私量为负。系统从0到$t$时刻，终端卸载到第$k$个MEC节点的任务的累积隐私量为

$$Q_k(t)=\sum_{\tau=0}^{t} I_k(\tau)\cdot q(\tau) \tag{3}$$

从攻击者的角度分析，若$Q(t)$不断累加，并超过一定的判决阈值θ，则可判断锁定的用户大概率为Bob；若$Q(t)$的值起伏波动，且不超过θ，则可判断锁定的用户不是Bob。阈值θ选取越大，需累积的隐私量越多，判定的结果越可靠；θ选取越小，达到阈值的卸载次数越少，但判定的结果越不准确。

3 隐私感知的计算卸载方法

本节首先提出假任务机制，降低MEC节点上隐私量累积的同时使总卸载频次不变；然后，建立隐私感知计算卸载模型，尽可能减小每个MEC节点的累积隐私量的同时最小化终端平均能耗；最后，基于Lyapunov优化原理简化模型并求解。

3.1 假任务机制

引入隐私度量及隐私约束后，终端可通过感知当前环境下卸载任务暴露自身特征的可能性，针对性地在卸载决策中增加隐私约束，使各MEC节点监听累积的隐私量始终较低。单纯采用此防护方法会导致如下新问题：(1)隐私限制导致较多本地卸载，增大终端能耗，与计算卸载的初衷不符；(2)若攻击者知道此防御方法，较低的对外卸载频率可作为一个新特征被其分析利用，知道用户采用了防护手段而优先锁定并进一步实施其他攻击手段。

本节提出假任务机制，若时隙t的计算任务本应卸载到MEC节点，却因考虑隐私限制而本地处理或丢弃时，在某一MEC节点产生虚假任务，使最终的卸载次数和不考虑隐私的决策结果保持一致，且为了尽可能降低暴露在MEC节点上的隐私量，产生的虚假任务应为Bob卸载概率最小的任务。具体实现中，终端可通过控制指令触发MEC中非特征任务的运行，而非传输完整的卸载任务，减少传输能耗。

用指示函数$I_{\mathrm{Ck}}(t)$表示t时刻是否有在第k个MEC节点上产生虚假任务，$I_{\mathrm{Ck}}(t)$应满足

$$\sum_{k=1}^{N_{\mathrm{MEC}}} I_{\mathrm{Ck}}(t)=\{I_{\mathrm{L}}(t)+I_{\mathrm{D}}(t),0\} \tag{4}$$

由式(3)、式(4)可得第k个MEC节点累积到时隙t的量化隐私$Q_k(t)$为

$$Q_k(t)=Q_k(t-1)+I_k(t)\cdot q(t)+I_{\mathrm{Ck}}(t)\cdot q_0 \tag{5}$$

其中，q_0为假任务的隐私量，$q_0=\min\{\ln p^{\mathrm{B}}_T/\bar{p}_T\}, T\in\boldsymbol{T}$。

3.2 隐私感知的计算卸载模型

每个时隙t，用户根据观察所得的各MEC的无线信道增益$h^2(t)$和自身记录的各MEC节点当前的隐私量$Q(t)$，做出最优的卸载决策$\alpha(t)\in A$，则隐私感知的计算卸载模型为

$$\left.\begin{aligned}
&\mathcal{P}_\infty:\ \min_{\alpha(t)\in A}\ \lim_{t\to+\infty}\frac{1}{t}\mathbb{E}\left[\sum_{\tau=1}^{t}E(\tau)\right]\\
&\text{s.t. 式(1), 式(4)}\\
&\quad D(t)\ \le\ \xi(t) && \text{(6a)}\\
&\quad Q_k(t)\to 0,\ k=1,2,\cdots,\ N_{\mathrm{MEC}} && \text{(6b)}\\
&\quad I_{\mathrm{L}}(t),[I_k(t),I_{\mathrm{Ck}}(t)]_{k=1}^{N_{\mathrm{MEC}}},\ I_{\mathrm{D}}(t)\in[0,1] && \text{(6c)}\\
&\quad 0\le\ f(t)\ \le f_{\max}\ \cdot\ I_{\mathrm{L}}(t) && \text{(6d)}\\
&\quad 0\le p_k(t)\le p_{\max}\cdot I_k(t),\ k=1,2,\cdots,N_{\mathrm{MEC}} && \text{(6e)}
\end{aligned}\right\} \tag{6}$$

其中，式(1)、式(4)、式(6c)描述了各指示函数的限制，式(6a)表示任务处理时延限制，式(6d)、(6e)表示终端CPU频率和天线功率限制，式(6b)为各MEC节点的隐私限制，其隐私量越靠近0，用户被锁定的风险也越小，决策集合$A=\left\{I_{\mathrm{L}}(t), f(t),[I_k(t),p_k(t),I_{\mathrm{C}k}(t)]_{k=1}^{N_{\mathrm{MEC}}},I_{\mathrm{D}}(t)\right\}$。

模型$\mathcal{P}_\infty$是一个马尔科夫决策过程(Markov Decision Process, MDP)[6]，系统的状态和动作较多，若用MDP算法求解，需将系统状态量化为有限个确定状态，存在量化误差；且一般的MDP算法复杂度较高，无法满足实时通信的需求；此外，MDP算法需终端保存各状态对应的最优动作，占用终端存储空间。

基于Lyapunov优化[17]方法简化和求解模型，可将难于求解的无限时域最小平均代价问题转化为每个时隙的最小值问题，算法复杂度低且可调节参数达到近似最优解。将每个MEC节点的累积隐私量变化看作一个虚拟队列$\boldsymbol{Q}(t)=(Q_1(t),Q_2(t),\cdots,Q_{N_{\mathrm{MEC}}}(t))$，每个时隙$t$均可能有卸载任务到达某一MEC节点使得虚拟队列值改变，为使各MEC节点的累积隐私量稳定在0值附近，则需使虚拟队列$\boldsymbol{Q}(t)$保持平稳，引入Lyapunov函数描述此特性，对每个时隙t有

$$L(t)=\frac{1}{2}\sum_{k=1}^{N_{\mathrm{MEC}}}Q_k(t)^2 \tag{7}$$

两个相邻时隙间的Lyapunov漂移为

$$\begin{aligned}\Delta L(t)&=L(t+1)-L(t)\\&=\frac{1}{2}\sum_{k=1}^{N_{\mathrm{MEC}}}\left[I_k(t)\cdot q(t)+I_{\mathrm{C}k}(t)\cdot q_0\right]^2\\&\quad+\sum_{k=1}^{N_{\mathrm{MEC}}}Q_k(t)\cdot\left[I_k(t)\cdot q(t)+I_{\mathrm{C}k}(t)\cdot q_0\right]\\&\le B+\sum_{k=1}^{N_{\mathrm{MEC}}}Q_k(t)\cdot\left[I_k(t)\cdot q(t)+I_{\mathrm{C}k}(t)\cdot q_0\right]\\&=\widetilde{\Delta}L(t)\end{aligned} \tag{8}$$

其中，B为正常数，上界为$q(t)^2/2$, $\widetilde{\Delta}L(t)$为$\Delta L(t)$的近似值。

若只追求Lyapunov漂移最小，即使累积隐私量稳定在0附近满足了式(6b)，则会导致更多的本地执行(不卸载暴露隐私)，增大能耗而违背模型$\mathcal{P}_\infty$的优化目标。因此将能耗作为惩罚机制，使每个时隙中的Lyapunov漂移和惩罚最小的决策是模型$\mathcal{P}_\infty$的最优解。

模型$\mathcal{P}_\infty$的目标函数可简化为$\min\ \widetilde{\Delta}L(t)+V\cdot E(t)$，其中$V$为正常数，用于调节每个时隙$t$中漂移与惩罚的权重关系，$V$越大，每个时隙的惩罚也就越小，最终的平均能耗也就越小，但各MEC节点的累积隐私量无法稳定在0值附近。

3.3 算法描述

每个时隙t中，先计算本地处理计算任务的最优的CPU频率$f^*(t)$(上标*表示最优解，下同)和将计算任务卸载到第k个MEC节点的最优天线功率$p_k^*(t)$，具体步骤如策略1所示。

策略1

步骤 1　若确定本地处理计算任务，且$\beta\cdot b/f_{\max}\le\xi(t)$，则最优的CPU频率为$f^*(t)=\beta\cdot b/\xi(t)$，对应的最低能耗为$E_{\mathrm{L}}^*(t)=\kappa\cdot[f^*(t)]^3\cdot\xi(t)$；

步骤 2　若确定将计算任务卸载到第k个MEC节点，且$(2^{b/W\xi(t)}-1)\cdot WN_0/h_k^2(t)\le p_{\max}$，则最优的天线功率为$p_k^*(t)=(2^{b/W\xi(t)}-1)\cdot WN_0/h_k^2(t)$，对应的最低能耗为$E_k^*(t)=p_k^*(t)\cdot\xi(t)$。

在每个时隙t中，先观察当前无线信道增益$\{h_k^2(t)\}_{k=1}^{N_{\mathrm{MEC}}}$以及任务截止时间$\xi(t)$，根据策略1计算各MEC节点对应的最优发射功率$p_k^*(t),k=1,2,\cdots,N_{\mathrm{MEC}}$和最优CPU频率$f^*(t)$，得到可卸载的候选MEC节点集合$M(t)$

$$M(t)=\{1\le k\le N_{\mathrm{MEC}}|p_k^*(t)\le p_{\max}\} \tag{9}$$

若$M(t)=\varnothing$或集合中功率最小值$p_{k\min}^*(t)$对应的最小卸载能耗$E_{k\min}^*(t)$大于本地处理的能耗$E_{\mathrm{L}}^*(t)$，此时无论是否考虑隐私约束，终端都不会将计算任务卸载到MEC节点，无需控制生成假任务，时隙t决策完毕。

若上述情况不满足，即计算任务本应卸载到MEC节点上，因考虑隐私限制而本地处理或丢弃，此时选取最优的MEC节点生成一个假任务，由策略2求得此时的最优决策$\alpha^*(t)$。

策略2

步骤 1　考虑卸载到MEC节点的情况，计算使得$Q_k(t-1)\cdot q(t)+VE_k^*(t)$取得最小值时的MEC节点$k_{\min}$；

步骤 2　考虑生成假任务的情况，计算使得式$Q_k(t-1)\cdot q_0$取得最小值时的MEC节点$k_{\min}^{\mathrm{C}}$；

步骤 3　若　$Q_{k_{\min}}(t-1)\cdot q(t)+VE_{k_{\min}}^*(t)<Q_{k_{\min}^{\mathrm{C}}}(t-1)\cdot q_0+V\cdot\min\{E_{\mathrm{L}}^*(t),E_0\}$，则卸载到第$k_{\min}$个MEC节点；

步骤 4　若　$f^*(t)<f_{\max}$　且$Q_{k_{\min}^{\mathrm{C}}}(t-1)\cdot q_0+VE_{\mathrm{L}}^*(t-1)<Q_{k_{\min}}(t)\cdot q(t-1)+VE_{k_{\min}}^*(t)$，则执行本地处理，并在第$k_{\min}^{\mathrm{C}}$个MEC节点上生成假任务；

步骤 5　若步骤3、步骤4均不成立，则丢弃任务，并在第$k_{\min}^{\mathrm{C}}$个MEC节点上生成假任务。

基于策略1、策略2，利用LPOA求最优解，具体流程如表1所示。

4 仿真分析

本节利用MATLAB数值仿真方法验证上述模型和算法的有效性，假设MEC侧可检测到20种卸载任务，且这些任务服的卸载概率服从Zipf分布，即$p_{T_i} \propto 1/k_i^{\rho}$，其中$k_i$表示对应任务$T_i$的流行程度排序，$\rho=2$。网络模型参数设置如表2所示。

4.1 算法对比

本文的对比算法包括：(1)Basic算法，不考虑隐私约束，优化目标为每个时隙t的终端能耗最小；(2)Naive算法，在Basic算法基础上考虑隐私约束，每个时隙t内寻求不超过隐私阈值且能耗最小的卸载方式；(3)Naive-Chaff算法，在Naive算法基础上引入假任务机制，依据贪心思想在累积隐私量最大的MEC节点上生成假任务。

表 1 LPOA

初始化：设置各MEC节点的累积隐私量$Q(t)=0$

(1) **For** t=1,2, $\cdots$,T **Do**

(2) 观察当前无线信道增益$\{h_k^2(t)\}_{k=1}^{N_{\mathrm{MEC}}}$和任务截止时间$\xi(t)$;

(3) 根据策略1计算$f^*(t), E_{\mathrm{L}}^*(t), \left[p_k^*(t), E_k^*(t)\right]_{k=1}^{N_{\mathrm{MEC}}}$;

(4) 根据式(9)获得MEC节点候选集$M(t)$;

(5) If $(M(t)=\varnothing) \,||\, \left(E_{\mathrm{L}}^*(t) < E_{k_{\min}}^*(t)\right)$

(6) If $f^*(t) > f_{\max}$丢弃任务，$E(t)=E_0$;

(7) Else 本地处理，$E(t)=E_{\mathrm{L}}^*(t)$;

(8) End If

(9) Else

(10) 根据式(2)求得隐私量$q(t)$;

(11) 根据策略2求得最优解$\alpha^*(t)$;

(12) 根据$\alpha^*(t)$执行卸载并根据式(5)更新隐私量$Q(t)$;

(13) End If

(14) **End For**

表 2 参数设置

参数	取值
单位时隙长度l_s	1 ms
信道增益h_k^2服从指数分布，均值$\overline{h_k^2}$	–90 dB
信道增益h_k^2服从指数分布，量化步长$\delta_{h_k^2}$	$\overline{h_k^2}/100$
上行链路带宽W	1 MHz
噪声功率密度N_0	10^{-19} W/Hz
CPU最大频率$f_{\max}$	1.5 GHz
能耗系数κ	10^{-28}[16]
终端天线最大发射功率$p_{\max}$	1 W
任务大小b	10^3 bit
处理1 bit数据所需CPU循环数β	700
任务截止时间$\xi(t)$服从均匀分布	$\{0.1l_s, 0.2l_s, \cdots, l_s\}$
任务丢弃代价E_0	$10\cdot\kappa\beta b f_{\max}^2$

首先分析隐私威胁和攻击成功的可能性，仿真参数设置为：$\theta=5, V=10^3, N_{\mathrm{MEC}}=2$。选择1次实验中任一MEC节点的前2000次卸载结果，3种算法的累积隐私量变化如图2(a)、图2(b)所示。由图2(a)可知，Basic算法经过很少的卸载后隐私量就可超过设定的阈值，且隐私量随着时间t不断增加，无论攻击者如何设置判决阈值θ都能满足，存在明显的用户特征和隐私暴露风险。图2(b)表明Naive-Chaff算法和LPOA都能把该MEC节点上探测的隐私量控制在阈值以下，LPOA虽与隐私阈值θ无关，但仍能始终将隐私量变化控制在0值附近较小的范围内，有效保护用户的隐私。

在上述参数设置下累积执行$t=10^5$个时隙，各算法卸载结果隐私量的均值和方差如图2(c)所示(为避免无线信道和计算任务的随机性导致误差，此实验及后续仿真结果都是1×10^4次蒙特卡洛实验结果的均值)。各算法的隐私量均值在门限值$\theta=5$以下且方差也较小，Naive和Naive-Chaff算法的均值为4，始终靠近门限值；LPOA的均值始终靠近0，表明其控制目标用户的卸载表现最接近普通用户，难以被攻击者锁定。

在上述参数设置下，不同时隙个数和对应的平均能耗如图3所示，由于无线信道和计算任务的随机性，本文4种算法都需经历较长时隙(约10^4 ms)后才达到稳定状态。由图3(b)可知由于3种算法的卸载决策的不同，其最终达到稳定状态的时间也略有差异，但和Basic算法达到稳定状态所需的时间相近。可认为上述参数设置下，影响系统稳定性的主要因素是无线信道的随机性，后续实验使用10^5 ms作为系统稳定时间。

图3(b)前100 ms的卸载决策中LPOA的能耗较高，这是由于在开始卸载的短时间内各MEC节点上的隐私量空间足够，隐私限制不影响卸载决策，Naive和Naive-Chaff算法的卸载决策和Basic算法几乎一致，因此平均能耗很小；而随着时间不断增长，LPOA的平均能耗最小，仅次于不考虑隐私的Basic算法，在保护隐私的同时，有更好的节能表现。

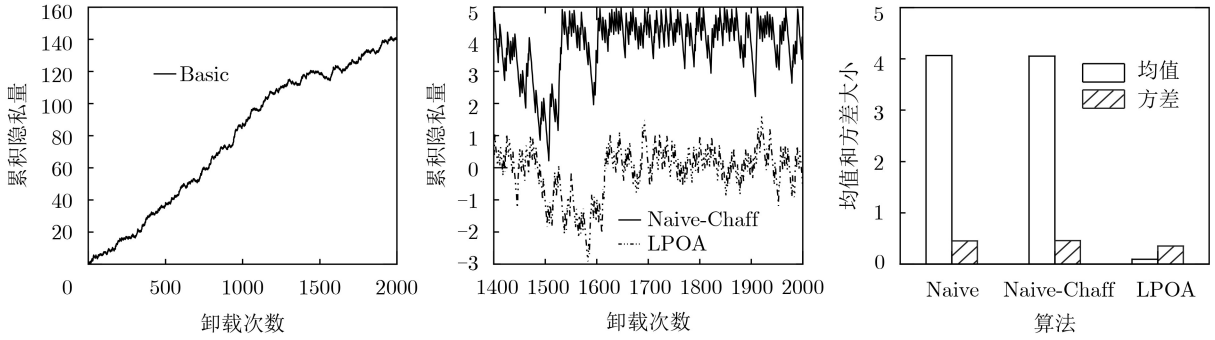
上述实验分析了各算法平均能耗和隐私量的变化情况，图4则具体分析了各算法的卸载决策结果的占比。由图4(a)可知，Naive和Naive-Chaff算法在约80%的时隙里卸载决策与Basic相同，高于LPOA的约50%，但由图4(b)可知，Naive和Naive-Chaff算法的丢弃频率最高，导致其平均能耗比

LPOA高。由于假任务机制，Naive-Chaff相比Naive算法执行了更多的卸载和更少的本地执行，平均能耗进一步降低。Naive-Chaff和LPOA的真假任务卸载频率之和与Basic算法的卸载频率相同，表明假任务机制可使用户的外在表现和普通用户更为一致。

4.2 参数分析

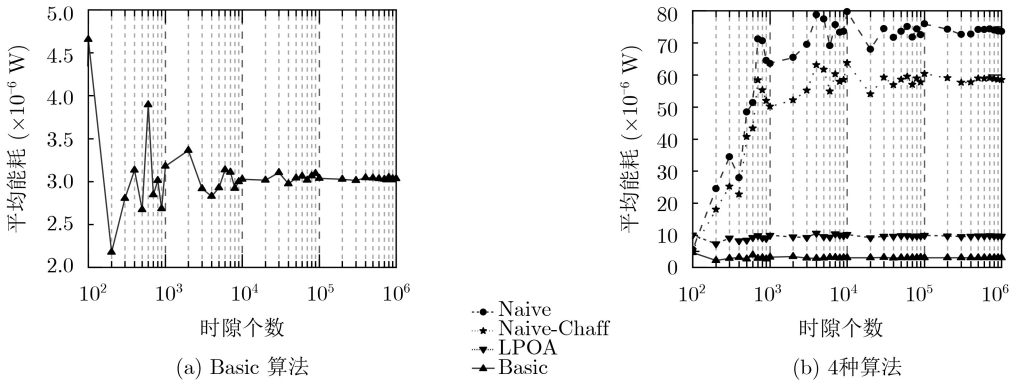
图5描述了参数V对算法效果的影响。由图5(a)可知，随着V不断增大，LPOA的隐私量无法始终稳定在0附近，当$V > 10^5$时稳定状态的隐私量会显著增大，无法再保护用户隐私。图5(b)表明稳定状态下的隐私量方差随着V不断增大而增大，且会出现较大波动，说明由于增量权重降低，隐私量无法保持较好的稳定性。图5(c)中表明随着V增大，每次卸载决策中能耗代价的权重更大，最终的平均能耗也更低。$V > 10^5$时V的继续降低不会导致LPOA的平均能耗的明显减少，但却会导致稳定状态下累积隐私量显著增大，因此，选择$V < 10^5$时LPOA有更好的效果。

MEC节点的数量对整个系统也有较大的影响，更多的MEC节点提供了更优的无线环境和更多的卸载选择，有利于降低平均能耗和保护用户隐私。图6反映了默认参数设置下MEC节点数量对系统的影响，随着MEC数量的增多，4种算法的平均能耗和隐私量方差都会降低，表明MEC的多样性



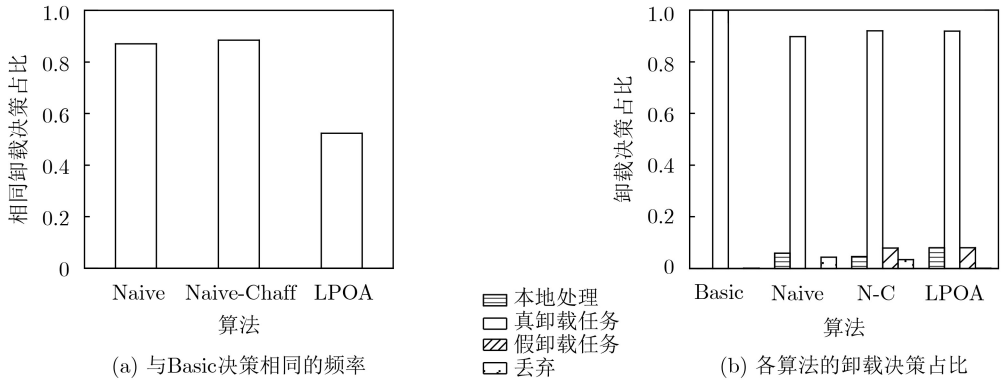
(a) Basic算法　(b) Naive-Chaff算法和LPOA　(c) 隐私量均值和方差

图 2 隐私量变化分析



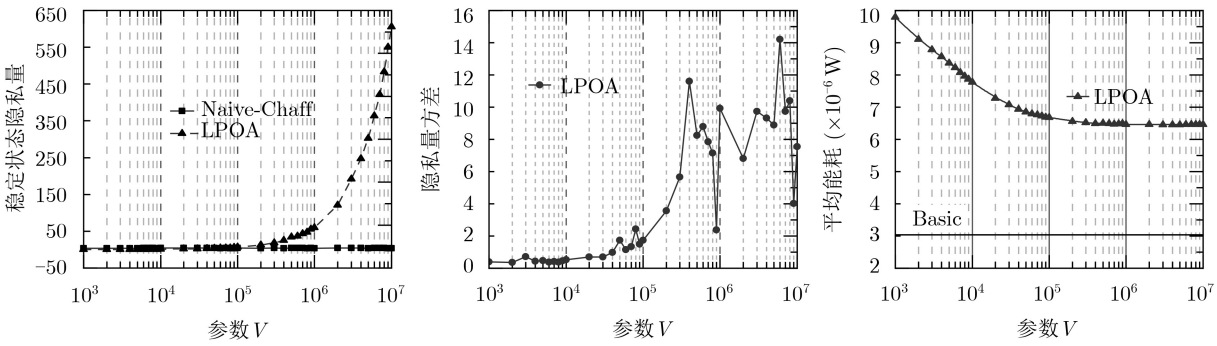
(a) Basic 算法　(b) 4种算法

图 3 不同时隙个数下平均能耗对比



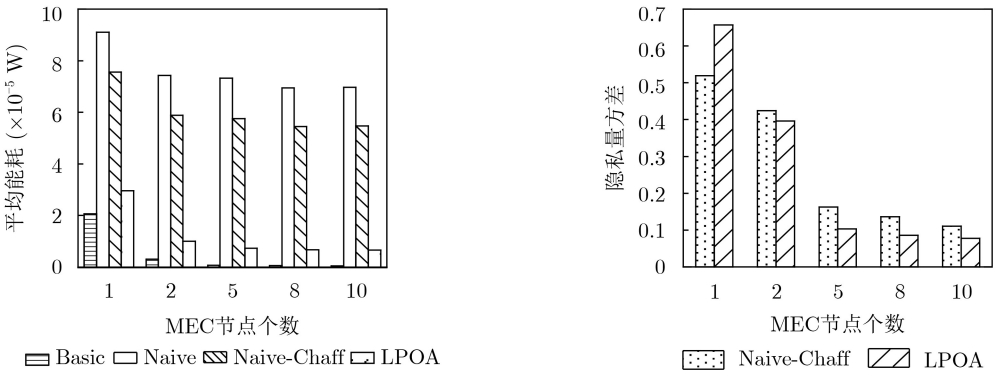
(a) 与Basic决策相同的频率　(b) 各算法的卸载决策占比

图 4 各算法的卸载决策



(a) 稳定隐私量大小 (b) 稳定状态下隐私量方差 (c) 平均能耗

图 5 变量V的影响



(a) 平均能耗 (b) 隐私量方差

图 6 MEC数量的影响

会改善平均能耗和隐私量稳定性，但5个MEC节点已经能达到较好的效果，再多的MEC节点对系统的提升不大。

5 结束语

MEC场景中用户卸载任务的特征性可能暴露其隐私信息，单纯限制用户任务卸载可导致新的隐私和能耗问题。本文提出一种基于Lyapunov优化的隐私感知计算卸载方法，通过限制各MEC节点的累积隐私量以保护用户隐私，同时提出假任务机制，使用户对外的总卸载次数保持稳定，降低了用户被攻击者锁定的可能性。仿真实验表明，LPOA能在每个时隙求解模型的最优解，计算复杂度低，在保证较高隐私安全的同时维持了较低的终端能耗。

参 考 文 献

[1] JI Xinsheng, HUANG Kaizhi, JIN Liang, *et al*. Overview of 5G security technology[J]. *Science China Information Sciences*, 2018, 61(8): 081301. doi: 10.1007/s11432-017-9426-4.

[2] ABBAS N, ZHANG Yan, TAHERKORDI A, *et al*. Mobile edge computing: A survey[J]. *IEEE Internet of Things Journal*, 2018, 5(1): 450–465. doi: 10.1109/JIOT.2017.2750180.

[3] FLORES H, HUI Pan, TARKOMA S, *et al*. Mobile code offloading: From concept to practice and beyond[J]. *IEEE Communications Magazine*, 2015, 53(3): 80–88. doi: 10.1109/MCOM.2015.7060486.

[4] MACH P and BECVAR Z. Mobile edge computing: A survey on architecture and computation offloading[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(3): 1628–1656. doi: 10.1109/COMST.2017.2682318.

[5] MENG Xianling, WANG Wei, WANG Yitu, *et al*. Delay-optimal computation offloading for computation-constrained mobile edge networks[C]. 2018 IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 2018: 1–7. doi: 10.1109/GLOCOM.2018.8647703.

[6] MAO Yuyi, ZHANG Jun, and LETAIEF K B. Dynamic computation offloading for mobile-edge computing with energy harvesting devices[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(12): 3590–3605. doi: 10.1109/JSAC.2016.2611964.

[7] ZHANG Guanglin, ZHANG Wenqian, CAO Yu, *et al*. Energy-delay tradeoff for dynamic offloading in mobile-edge computing system with energy harvesting devices[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(10): 4642–4655. doi: 10.1109/TII.2018.2843365.

[8] ZHANG Peiyun, ZHOU Mengchu, and FORTINO G.

Security and trust issues in Fog computing: A survey[J]. *Future Generation Computer Systems*, 2018, 88: 16–27. doi: 10.1016/j.future.2018.05.008.

[9] NI Jianbing, ZHANG Aiqing, LIN Xiaodong, *et al*. Security, privacy, and fairness in fog-based vehicular crowdsensing[J]. *IEEE Communications Magazine*, 2017, 55(6): 146–152. doi: 10.1109/MCOM.2017.1600679.

[10] HE Xiaofan, LIU Juan, JIN Richeng, *et al*. Privacy-aware offloading in mobile-edge computing[C]. 2017 IEEE Global Communications Conference, Singapore, 2017: 1–6. doi: 10.1109/GLOCOM.2017.8253985.

[11] MIN Minghui, WAN Xiaoyue, XIAO Liang, *et al*. Learning-based privacy-aware offloading for healthcare IoT with energy harvesting[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 4307–4316. doi: 10.1109/JIOT.2018.2875926.

[12] HE Xiaofan, JIN Richeng, and DAI Huaiyu. Deep PDS-learning for privacy-aware offloading in MEC-enabled IoT[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 4547–4555. doi: 10.1109/JIOT.2018.2878718.

[13] HE Ting, CIFTCIOGLU E N, WANG Shiqiang, *et al*. Location privacy in mobile edge clouds: A chaff-based approach[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(11): 2625–2636. doi: 10.1109/JSAC.2017.2760179.

[14] MAO Yuyi, YOU Changsheng, ZHANG Jun, *et al*. A survey on mobile edge computing: The communication perspective[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(4): 2322–2358. doi: 10.1109/COMST.2017.2745201.

[15] LIN Xue, WANG Yanzhi, CHANG N, *et al*. Concurrent task scheduling and dynamic voltage and frequency scaling in a real-time embedded system with energy harvesting[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2016, 35(11): 1890–1902. doi: 10.1109/TCAD.2016.2523450.

[16] ZHANG Weiwen, WEN Yonggang, GUAN K, *et al*. Energy-optimal mobile cloud computing under stochastic wireless channel[J]. *IEEE Transactions on Wireless Communications*, 2013, 12(9): 4569–4581. doi: 10.1109/TWC.2013.072513.121842.

[17] NEELY M J. Stochastic Network Optimization with Application to Communication and Queueing Systems[M]. San Rafael, Calif.: Morgan & Claypool Publishers, 2010: 1–211.

赵　星：男，1990年生，博士生，研究方向为移动通信网安全、隐私保护技术.

彭建华：男，1966年生，教授、博士生导师，主要研究方向为无线移动通信网络、信息安全.

游　伟：男，1984年生，博士，讲师，主要研究方向为移动通信网络安全、新一代移动通信网络技术.