基于k-匿名的隐私保护计算卸载方法

赵 星* 彭建华 游 伟 陈 璐
(中国人民解放军战略支援部队信息工程大学 郑州 450001)

摘 要：针对移动边缘计算(MEC)中用户的卸载任务及卸载频率可能使用户被攻击者锁定的问题，该文提出一种基于k-匿名的隐私保护计算卸载方法。首先，该方法基于用户间卸载任务及其卸载频率的差异性，提出隐私约束并建立基于卸载频率的隐私保护计算卸载模型；然后，提出基于模拟退火的隐私保护计算卸载算法(PCOSA)求得最优的k-匿名分组结果和组内各任务的隐私约束频率；最后，在卸载过程中改变用户原始卸载频率满足隐私约束，最小化终端能耗。仿真结果表明，PCOSA算法能找出用户所处MEC节点下与用户卸载表现最相近的k个用户形成匿名集，有效保护了所有用户隐私。

关键词：移动边缘计算；计算卸载；卸载决策；隐私保护；k-匿名
中图分类号：TN918; TP393 **文献标识码**：A **文章编号**：1009-5896(2021)04-0892-08
DOI: 10.11999/JEIT191046

A Privacy-preserving Computation Offloading Method Based on k-Anonymity

ZHAO Xing PENG Jianhua YOU Wei CHEN Lu
(*People's Liberation Army Strategic Support Force Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Users' offloading tasks and offloading frequencies in Mobile Edge Computing(MEC) may cause users to be locked out. A privacy-preserving computation offloading method based on k-anonymity is proposed in this paper. Firstly, based on the differences between offloading tasks and their frequencies, privacy constraint is proposed to establish a privacy-preserving computation offloading model based on offloading frequency; Then, a Privacy-preserving Computation Offloading algorithm based on Simulated Annealing (PCOSA) is utilized to obtain the optimal k-anonymous groups and the privacy constraint frequency of each task; Finally, the user's original offloading frequencies are changed to meet the privacy constraint while minimizing terminal energy consumption. Simulation results validate that the PCOSA can find out k users with the closest offloading performance to form anonymous sets, which protects effectively the privacy of all users.

Key words: Mobile Edge Computing(MEC); Computation offloading; Offloading decision; Privacy protection; k-anonymity

1 引言

随着智能终端和物联网的普及，各类终端应用不断涌现，为用户带来丰富娱乐体验的同时也消耗了终端更多的计算资源和能耗[1]。移动边缘计算(Mobile Edge Computing, MEC)[2]是第5代移动通信网络(5G)[3]的重要支撑技术，通过将计算资源部署在网络边缘，空间上邻近终端用户，降低服务时延的同时也可减少终端能耗。计算卸载技术[4]作为MEC的关键技术之一，通过无线链路将计算密集型终端应用传输至邻近的MEC节点处理，利用MEC服务器充足的计算资源和能源减少终端处理任务的时延和能耗，有效提高了服务质量和用户体验。计算卸载决策指终端感知无线环境并结合自身卸载任务特性，基于不同的优化目标(降低终端能耗[5]、减少任务处理时延[6]和权衡能耗与时延[7])，选择最优的任务处理方式(本地处理、卸载到MEC节点或丢弃)。

收稿日期：2019-12-30；改回日期：2020-07-27；网络出版：2020-08-21
*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)

目前针对MEC安全和隐私问题的研究多是从加密、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]研究现有卸载决策发现终端在信道条件较好时会尽可能上传计算任务以减少自身能耗，攻击者可据此通过监听MEC节点上的任务卸载情况，反推出用户的使用模式和所处无线环境，甚至实现对终端的定位；文献[11]进一步分析了物联网场景中卸载决策的隐私，建立隐私模型综合考虑隐私、能耗和计算时延，基于增强学习求解；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，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]基于上述研究进一步基于任务卸载概率的显著性定义计算任务的隐私量，以此建立隐私保护计算卸载模型并求出隐私约束下的最优平均能耗。然而上述研究均考虑单个用户的隐私保护，基于计算任务的卸载频率相对于统计流行度的显著性度量用户的隐私属性，没有充分考虑不同MEC区域用户群体的不同导致隐私度量偏差。此外在多用户场景中，直接采取单用户隐私保护会使整体能耗的线性增高，降低整体服务质量。

为实现多用户场景下协同隐私保护并最小化整体能耗，本文提出一种基于k-匿名的隐私保护计算卸载方法。首先，分析卸载决策中的隐私威胁和多用户场景中防护难点，提出基于卸载任务及卸载频率的隐私约束，限制k个用户的各卸载任务实际卸载频率相近；然后，提出基于k匿名的隐私保护计算卸载模型，并用基于模拟退火的隐私保护计算卸载算法(Privacy preserving Computation Offloading algorithm based on Simulated Annealing, PCOSA)快速求得最优分组。实验结果表明，PCOSA能最小化终端能耗，且每个卸载任务都有k个用户的卸载特征相似，使攻击者无法区分出目标用户。

2　模型分析

2.1　系统模型

目前比较常见的边缘系统模型如图1所示[14]，MEC节点部署于一定区域内的多个基站或无线热点之后，为接入网络的多个终端用户提供计算卸载服务。假设系统为单位时隙Δ ms的时隙系统，在每个时隙t内，终端可随机产生一个可卸载的任务$T(t)$，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[15]，每个任务均有时延门限$\xi(t)$，需在规定时延门限内处理完任务，否则只能丢弃。时隙t的计算任务的卸载结果可以是本地处理、卸载到MEC节点或丢弃，分别用指示函数$I_{\mathrm{L}}(t)$, $I_{\mathrm{M}}(t)$和$I_{\mathrm{D}}(t)$表示。

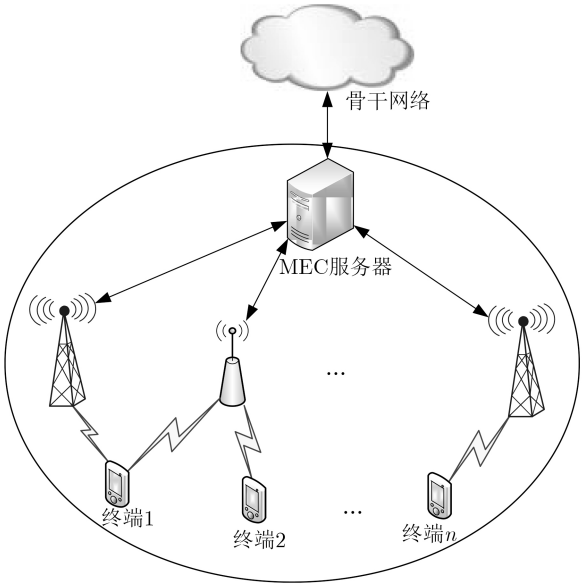


图 1 系统模型

考虑本地处理情况，假设终端的CPU频率可以根据不同的卸载决策而改变(最大值为$f_{\max}$)，时隙t内的CPU频率为$f(t)$，则可计算得时延为$D_{\mathrm{L}}(t)=b\cdot\beta/f(t)$，终端的能耗为$E_{\mathrm{L}}(t)=\kappa\cdot f^3(t)\cdot D_{\mathrm{L}}(t)$，其中$\kappa$表示CPU的能耗系数[16]。

计算任务本地处理的最优CPU频率为$f^*(t)=\beta\cdot b/\xi(t)$，若可以本地处理(即$f^*(t)\le f_{\max}$)，则本地处理的最低能耗为$E_{\mathrm{L}}^*(t)=\kappa\cdot[f^*(t)]^3\cdot\xi(t)$。

考虑卸载到MEC节点情况，假定MEC控制N_{AP}个无线接入点覆盖1个服务区域，各无线接入设备与终端的无线信道相互独立，时隙t中第i个无线接入点的参数为：上行链路带宽W_i，信道噪声功率密度N_0^i，信道增益为$h_i^2(t)$，终端的发射功率$p_i(t)$(最大值为$p_{\max}$)。

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。则根据模型可计算得卸载到MEC节点处理任务的时延为$D_{\mathrm{M}}^i(t)=b/[W_i\cdot\log_2(1+h_i^2(t)\cdot p_i(t)/(W_i\cdot N_0^i))]$，终端的传输能耗为$E_{\mathrm{M}}^i(t)=p_i(t)\cdot D_{\mathrm{M}}^i(t)$。终端的最优天线功率为$p^*(t)=\min\left\{(2^{b/W_i\xi(t)}-1)\cdot W_iN_0^i/h_i^2(t)\right\}$，其中$i=1,2,\cdots,N_{\mathrm{AP}}$，当可以卸载到MEC节点(即$p^*(t)\le p_{\max}$)，最低能耗为$E_{\mathrm{M}}^*(t)=p^*(t)\cdot\xi(t)$。

2.2　隐私威胁

基于加密及认证等防护措施，假定系统中终端、基站或热点、MEC服务器均可信，攻击者直

接截获卸载任务并分析其所述用户身份信息难度很大。由于MEC系统应用层的相对开放性，攻击者可利用侧信道攻击[17]的方式推测、监听MEC服务器上卸载的计算任务及卸载频率。由于用户使用终端的习惯不同，每个用户常用的终端应用及其卸载频率也一般不同，若攻击者通过其他手段掌握了目标用户的部分先验信息(如用户经常性卸载的计算任务及其大致卸载概率)，则可通过监听MEC节点上任务卸载情况并推测目标用户所在MEC节点。

用户所有可卸载的计算任务集合记为T，用户卸载概率较高的计算任务集合记为$T_{\mathrm{U}}, T_{\mathrm{U}} \in T$(频率太低的卸载任务随机性较大，攻击验证难度较大，因此不作考虑，θ_p为考虑保护卸载任务的隐私保护门限)，T_{U}中各任务的卸载概率为P_{U}，任务数量记为N_{T}。若攻击者已掌握某一用户u的卸载情况T_u, P_u，且能入侵MEC系统监听各用户的任务卸载情况(由于身份加密，攻击者无法直接判断出用户的真实身份)，则攻击者可统计MEC节点上一段时间内各用户的实际卸载频率$\widetilde{P}_{\mathrm{U}}$，若存在一个用户的$\widetilde{P}_{\mathrm{U}}$与$P_u$接近，则可判断该用户大概率为目标用户$u$，进一步进行后续的攻击和分析。参与判定的卸载任务越多(即N_{T}越大)，卸载频率越接近，则攻击者锁定目标用户u成功的概率越大。

3 基于k-匿名的隐私保护计算卸载方法

本节针对2.2节中分析的用户隐私威胁和多用户场景隐私保护的挑战，提出基于k-匿名的协同隐私保护计算卸载模型，然后基于模拟退火算法求解最优分组，并给出隐私约束下平均能耗最低的卸载流程。

3.1 问题建模

利用多用户场景下用户间的相似性，可不独立保护每个用户的隐私，而是基于k-匿名原理[18]，使MEC节点覆盖范围内存在k个用户的实际卸载频率$\widetilde{P}_{\mathrm{U}}$相似，从而使攻击者无法从$k$个卸载行为相近的用户中区分出所攻击的目标用户$u$，整体保护$k$个用户的隐私。

为满足k-匿名，各用户计算卸载的隐私约束由式(1)所示，对于任意时隙t和任务用户i都存在k–1个用户j满足

$$\frac{\left|p_m^i(t)-p_m^j(t)\right|}{\overline{p}_m} \le \overline{N}_{\mathrm{T}} \cdot \theta,\ \ i \ne j,\ \ T_m \in T_i \cup T_j \quad (1)$$

其中，$\overline{N}_{\mathrm{T}}$为$k$个用户$T_{\mathrm{U}}$的并集的元素个数，$m$为需共同防护的计算任务，$\overline{p}_m$为$k$个用户的平均卸载概率，$\theta$为卸载频率最大可偏离的隐私保护阈值。$\theta$越小则各用户的卸载频率越接近，隐私约束越严，用户可根据自身需求设置相应θ值，实现个性化的隐私保护效果；$\overline{N}_{\mathrm{T}}$越大，需防护的计算任务越多，则单个计算任务的隐私限制越小，而N_{T}越小，任务数量越少，越严格的卸载频率限制才能更好地保护隐私。

每个时隙t中，每个用户根据观察所得的无线信道增益$h_i^2(t)$和各计算任务的原始卸载频率P_{U}，做出最优的卸载决策$\alpha(t) \in A$，多用户场景下基于卸载频率的隐私保护计算卸载模型为

$$\left.\begin{aligned} &\min_{t\to\infty}\ \frac{1}{t}\sum_{\tau=1}^{t}\frac{1}{N}\sum_{i=1}^{N}E_i(\tau)\\ &\text{s.t.}\quad D_i(t) \le \xi_i(t),\ i=1,2,\cdots,N \qquad (2a)\\ &\qquad I_{\mathrm{L}}^i(t)+I_{\mathrm{M}}^i(t)+I_{\mathrm{D}}^i(t)=1,\ i=1,2,\cdots,N \quad (2b)\\ &\qquad I_{\mathrm{L}}^i(t), I_{\mathrm{M}}^i(t), I_{\mathrm{D}}^i(t) \in \{0,1\},\ i=1,2,\cdots,N \quad (2c)\\ &\qquad \text{式(1)} \end{aligned}\right\} \quad (2)$$

其中优化目标为N个用户的平均能耗最低，式(2a)为用户i在时隙t时任务处理时间约束，式(2b)、式(2c)给出了指示函数的限制。

3.2 基于模拟退火的隐私保护计算卸载算法

为求解上述模型，本节提出基于模拟退火的隐私保护计算卸载算法(Privacy preserving Computation Offloading algorithm based on Simulated Annealing, PCOSA)， PCOSA算法分为两步，PCOSA I完成MEC节点下现有用户的分组及确定每组内防护任务数$\overline{N}_{\mathrm{T}}$及各卸载任务的隐私约束频率$\overline{P}$, PCOSA II中各用户根据$\overline{P}$的约束完成实时的计算卸载过程。

为满足式(1)，k个用户的分组中，每个用户都需改变卸载任务(如任务m)的卸载频率至区间$[\overline{p}_m \cdot (1-\overline{N}_{\mathrm{T}} \cdot \theta)/2,\ \overline{p}_m \cdot (1+\overline{N}_{\mathrm{T}} \cdot \theta)/2]$范围内，定义改变原始卸载频率而导致的偏离代价为

$$\begin{aligned} &\mathrm{cost}(u_1,u_2,\cdots,u_k)\\ &=\sum_{i=1}^{\overline{N}_{\mathrm{T}}}\sum_{j=1}^{k}\min\left(\left|p_{j,i}-\frac{\overline{p}_i}{2}\cdot\left(1-\overline{N}_{\mathrm{T}}\cdot\theta\right)\right|,\right.\\ &\qquad\left.\left|p_{j,i}-\frac{\overline{p}_i}{2}\cdot\left(1+\overline{N}_{\mathrm{T}}\cdot\theta\right)\right|\right) \end{aligned} \quad (3)$$

其中，$p_{j,i}$表示第j个用户第i个计算任务的卸载频率。

将N个用户每k个分为一组，共有$N!/k!$种不同的分组方案，当N较大时常规算法无法在多项式时间内求得最优分组的解，即为NP难问题。本文基于模拟退火算法快速求解分组结果，PCOSA I先计算所有k个用户分组的代价，然后随机初始化一种分组情况并计算其总代价，最后基于SA求解总代价最小的最优分组，其流程如表1所示。PCOSA

I基于SA算法求出用户的最优分组，其时间复杂度和模拟退火的参数相关，迭代次数N_{SA}满足$T\times\lambda^{N_{\mathrm{SA}}}\to T_{\min}$，在表1循环体中求偏离代价须执行次数为$\overline{N}_{\mathrm{T}}$和$N/k$的二重循环，因此PCOSA I的时间复杂度为$O(N_{\mathrm{SA}}\times\overline{N}_{\mathrm{T}}\times N/k)$，为尽量求得最优分组解，迭代次数$N_{\mathrm{SA}}$一般较大，且用户较多时$N/k$的值也较大，算法整体时间复杂度较高。但用户分组一般发生在用户接入网络或重新分组时，时延较不敏感，且MEC服务器也有较强的计算处理能力。

PCOSA II基于上述k-匿名分组结果及各分组中卸载任务的隐私约束频率，使每个用户在每个时隙中根据感知的无线环境、卸载任务特性，做出满足时延和隐私限制下能耗最优的卸载决策。

用N_{O}表示截止时隙t时用户已经卸载的总次数，变量$N_m, N_m\in N$表示其中任务m的卸载次数，$\overline{p}_{n,m}$为用户n中任务m的隐私约束频率，则$\overline{p}_{n,m}\times(1+\overline{N}_{\mathrm{T}}\cdot\theta)$表示其隐私上界。用户$n$的任务$m$满足隐私约束下剩余的可卸载次数为

$$N_m^{\mathrm{P}}=\mathrm{floor}(N_{\mathrm{O}}\times\overline{p}_{n,m}\times(1+\overline{N}_{\mathrm{T}}\cdot\theta))-N_m \tag{4}$$

具体卸载中，若只考虑卸载频率约束，则会导致开始时卸载了$E_{\mathrm{M}}^*(t)$较大的任务，后续$E_{\mathrm{M}}^*(t)$较小时却无法卸载。为此，继续利用SA算法中的Metropolis准则，根据$E_{\mathrm{M}}^*(t)$, $E_{\mathrm{L}}^*(t)$和N_m^{P}的大小关系，时隙t时以概率式(5)执行本地处理。

$$P=\exp\left(aN_m^{\mathrm{P}}\frac{E_{\mathrm{M}}^*(t)}{E_{\mathrm{L}}^*(t)}\right) \tag{5}$$

其中，参数a调节具体实验中最终指数函数数值，根据具体环境中$E_{\mathrm{M}}^*(t)$, $E_{\mathrm{L}}^*(t)$的值设定最优的a。根据式(5)可知剩余可卸载次数越多，本地处理能耗越低且卸载能耗越高，则本地处理的决策概率越大，从而实现长时间内平均卸载能耗最小。

上述步骤解决了隐私约束上界和能耗最优的问题，对于任务自身频率小于分组隐私均值的情况，需整体上降低用户的卸载频次N_{O}，使得本来出现概率较低的任务的卸载频率变高，而卸载次数越少则用户总卸载能耗越大。为此，利用假任务机制，在任务本可以卸载($E_{\mathrm{M}}^*(t)<E_{\mathrm{L}}^*(t)$)却因隐私约束而无法卸载时，根据式(6)选择实际卸载频率最小于隐私约束下界任务T_{F}，在MEC节点上产生该任务的假任务，提高其卸载频率。

$$T_{\mathrm{F}}=\min\left\{\frac{N_m}{N_{\mathrm{O}}}-\overline{p}_{n,m}\times(1-\overline{N}_{\mathrm{T}}\cdot\theta), m\in T_n\right\} \tag{6}$$

综上，PCOSA II的整体流程如表2所示。具体实现中，可在用户接入网络时的认证消息中加入其计算任务及平均卸载频率的信息，不增加额外的信令开销，也保证了安全性(若认证流程已经被攻击者攻破，则再防护卸载隐私毫无意义)。MEC根据接入用户及其任务卸载频率，完成k-匿名分组，再将分组结果通过认证应答信令发送给用户。

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，模型设置如表3所示。

为模拟用户使用终端习惯的特殊性，仿真实验中为每个用户不断随机生成卸载频率为[0,0.3]之间的卸载任务，直至所有任务卸载频率之和为1，因

表 1　PCOSA I 算法流程

输入：用户数N，各任务的卸载概率P_{U}，分组大小k，隐私保护门限θ_p，隐私保护阈值θ

输出：分组结果及组内各卸载任务的平均频率

(1) 根据式(3)计算所有k个用户分组的代价
(2) 将N个用户随机排列，按顺序每k个为一组作为初始解now
(3) While $T>T_{\min}$
(4)　new ←随机交换可行解now中两个用户位置
(5)　$\Delta\leftarrow\mathrm{cost(now)}-\mathrm{cost(new)}$
(6)　If $\Delta\geq 0$
(7)　　now ← new
(8)　Else
(9)　　now ←以$\mathrm{e}^{\Delta/T}$的概率将new赋值
(10)　$T=T\cdot\lambda$
(11) End While
(12) 通过将最优解now按顺序每k个为一组得到最优分组X

表 2　PCOSA II 算法流程

初始化：卸载总次数N_{O}=0；
任务累积卸载次数$N=0$

(1) 观察用户当前的$h_i^2(t), i=1,2,\cdots,N_{\mathrm{AP}}$和$\xi(t)$；
(2) 计算最优的$f^*(t)$, $E_{\mathrm{L}}^*(t)$, $p^*(t)$, $E_{\mathrm{M}}^*(t)$；
(3) If $p^*(t)>p_{\max}$无法卸载
(4)　If $f^*(t)>f_{\max}$ 丢弃任务，$E(t)=E_0$；
(5)　　Else 本地处理，$E(t)=E_{\mathrm{L}}^*(t)$；
(6) Else
(7)　根据式(4)计算可卸载任务数N_m^{P}
(8)　flag初始化为1，根据式(5)为flag赋值0；
(9)　If flag==1
(10)　　执行卸载，$E(t)=E_{\mathrm{M}}^*(t)$
(11)　　N_{O}和N_m均累加1；
(12)　Else
(13)　　本地处理，$E(t)=E_{\mathrm{L}}^*(t)$；
(14)　　根据式(6)生成假任务

此各用户的防护任务集合T_{U}、卸载频率P_{U}及任务数量N_{T}均不一样，隐私保护门限$\theta_p=0.05$。

实验的对比算法包括：(1)Basic算法，不考虑隐私约束式(1)，追求能耗最优的卸载决策，作为其他算法能耗表现的基准；(2)单用户隐私保护算法(Single User Privacy-preservation Algorithm, SUPA)，独立保护每个用户的隐私，使集合T_{U}的实际卸载频率都低于用户的原始频率P_{U}，隐私偏离度也设置为θ；(3)基于贪心思想的k-匿名算法(Greedy-based K-Anonymity Algorithm, GKAA)，基于贪心思想，每次分组选择偏移量最小的分组作为最优解的子集，对剩余用户执行同样操作，直至所有用户都分完组，其余步骤同PCOSA II。

4.1 算法对比

首先分析PCOSA的隐私保护效果和能耗，随机选取一用户分析其各任务的卸载结果如图2所示，参数设置为$N=60,k=3,\theta=0.2,T=10^5$。PCOSA I算法所得分组结果的均值卸载频率为组内各用户的隐私约束频率，PCOSA II算法改变了各计算任务的原始卸载频率，使其实际卸载频率均在隐私保护阈值θ的范围内，满足了k-匿名的隐私保护效果。

表 3 模型参数设置

参数	取值
单位时隙长度l_s	1 ms
信道增益h_i^2服从指数分布，均值$\overline{h_i^2}$	–90 dB
信道增益h_i^2服从指数分布，量化步长$\delta_{h^2}^i$	$\overline{h_k^2}/1000$
上行链路带宽W_i	1 MHz
噪声功率密度N_0^i	10^{-19} W/Hz
CPU最大频率$f_{\max}$	2 GHz
能耗系数κ	10^{-28}
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	10^3
任务截止时间$\xi(t)$服从均匀分布	$\{0.01l_s,0.02l_s,\cdots,l_s\}$
任务丢弃代价E_0	$10\cdot\kappa\beta b f_{\max}^2$

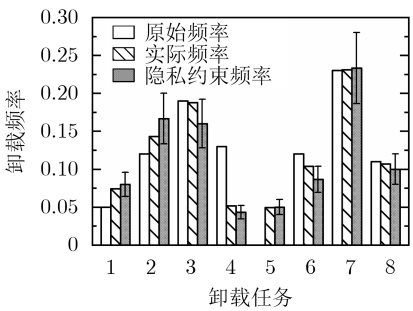


图 2 各任务卸载频率对比

原始频率高于隐私约束频率的任务，为最优化用户能耗，实际频率一般只略低于隐私约束上界；而原始频率低于隐私约束频率的任务，由于实际频率的提高受假任务机制影响，最终效果会有不同，原始频率越低的任务实际频率越靠近隐私约束频率。

由于无线环境的随机性，以及用户本身卸载任务的不确定性，需要较长时间系统才能达到稳定状态，图3描述了参数为$N=60,k=3,\theta=0.2$时，最小平均能耗随时隙T大小的变化情况。在时隙较小时，隐私约束的影响较大，直到$T=10^4$后能耗大小才保持稳定。为消除单次实验结果的误差，本实验及后续实验的结果都是10^3次蒙特卡罗实验的均值，且设置$T=10^5$。由图3可知，Basic算法由于不考虑隐私约束平均能耗最低，SUPA中每个用户独立满足隐私限制而消耗了最多终端能耗；k-匿名的分组隐私保护使GKAA和PCOSA能耗均小于SUPA，更优的分组结果使得PCOSA的最终能耗比GKAA下降了28%，比SUPA下降了60%。因此，PCOSA可在保护用户隐私的同时有效降低用户的平均能耗。

图4进一步分析了卸载决策中各结果的占比，不考虑隐私约束的Basic算法拥有最高的卸载频率，几乎所有计算任务都被卸载到MEC节点，因此卸载能耗最低；GKAA和PCOSA由于假任务机制和群体协同，比SUPA有更高的卸载占比和更低的本地处理与丢弃，GKAA比SUPA多卸载了26%的计

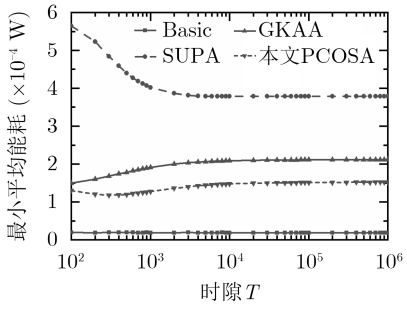


图 3 不同时隙T最小平均能耗对比

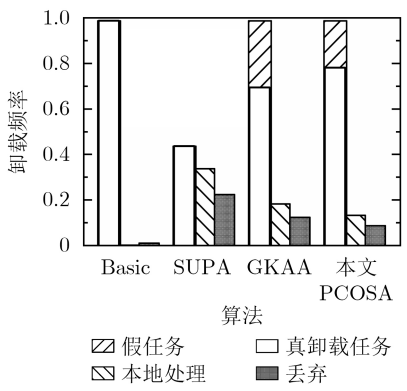


图 4 各算法卸载结果对比

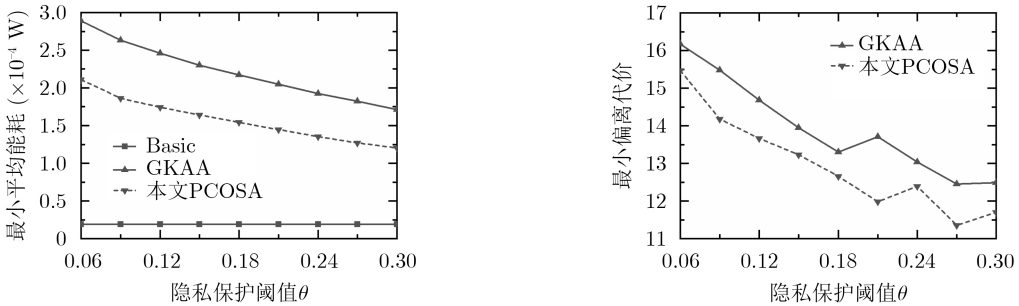
算任务，而PCOSA进一步比GKAA多卸载了9%的计算任务进一步降低了终端能耗。此外，GKAA和PCOSA算法的真假卸载任务之和与Basic算法的卸载频次保持一致，进一步保护了用户隐私。

4.2 参数分析

本小节进一步分析各算法参数对其效果的影响，图5分析了隐私保护阈值θ的影响，随着θ的增大，隐私限制变小，因此如图5(a)所示GKAA和PCOSA的最小平均能耗均不断降低；同时更小的隐私限制使分组结果中用户的卸载频率有更大的变化范围，使最小偏离代价降低。从图5(b)也可看出，当θ增大到一定程度时，最小偏离代价也可能不再降低，导致图5(a)中最小平均能耗降低变缓。

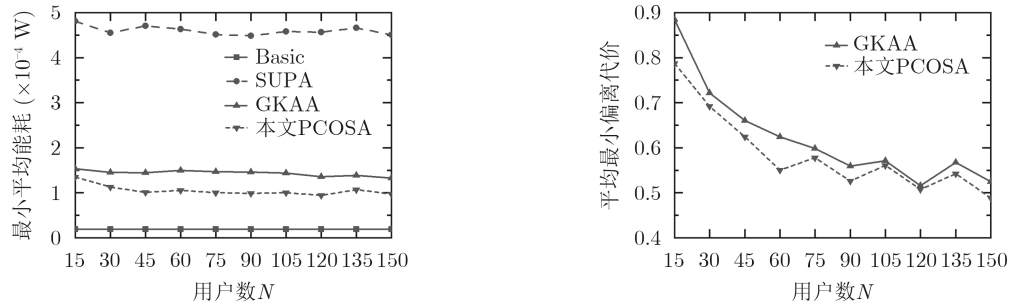
图6描述了用户数N的影响，理论分析知更多的用户意味着分组时能找到卸载表现更接近的用户，形成更好的隐私保护效果同时平均能耗也更低。图6(b)表明随着用户数N的增加，平均每个分组的最小偏离代价不断降低。由于数据源中用户各任务卸载频率的随机性，由图6(a)可知用户数对最小平均能耗影响并不大，只随着用户数增加而略微下降。

图7反映了分组大小k的影响，更多的组内用户数导致了用户间更大的差异性，使图7(b)中的平均最小偏离代价相应增大，从而导致图7(a)中的平均能耗变大。但更多的组内用户使卸载特征相似的用户更多，实现了更好的隐私保护效果，即牺牲了一定的终端能耗而换取更好用户隐私保护效果。



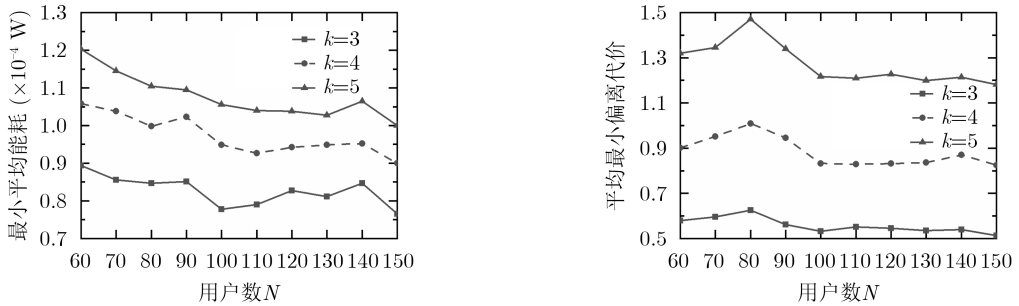
(a) 最小平均能耗　　(b) 最小偏离代价

图 5 隐私保护阈值θ的影响



(a) 最小平均能耗　　(b) 平均最小偏离代价

图 6 用户数N的影响



(a) 最小平均能耗　　(b) 平均最小偏离代价

图 7 分组大小k的影响

5 结束语

本文针对MEC计算卸载中用户不同任务卸载频率可能暴露其隐私的问题，提出一种基于k-匿名的隐私防护方法，利用多个用户形成卸载行为相近的群组，共同防护组内用户的隐私。提出基于模拟退火的PCOSA I算法高效求出最优的分组结果及其隐私约束频率，并根据PCOSA II算法步骤实现每个时隙内具体的卸载过程。仿真结果表明，采用k-匿名原理的多用户隐私防护机制可有效防止单个用户卸载特征被攻击者锁定攻击，且保持较低的平均卸载能耗。后续可继续深入研究MEC计算卸载中的其他隐私威胁和隐私量化方式，并结合5G具体应用场景进行分析和验证。

参 考 文 献

[1] NI Jianbing, LIN Xiaodong, and SHEN X S. Toward edge-assisted internet of things: From security and efficiency perspectives[J]. *IEEE Network*, 2019, 33(2): 50–57. doi: 10.1109/MNET.2019.1800229.

[2] YOUSEFPOUR A, FUNG C, NGUYEN T, *et al*. All one needs to know about fog computing and related edge computing paradigms: A complete survey[J]. *Journal of Systems Architecture*, 2019, 98: 289–330. doi: 10.1016/j.sysarc.2019.02.009.

[3] 徐璠, 吴慧慈, 陶小峰. 5G网络空间安全对抗博弈[J]. 电子与信息学报, 2020, 42(10): 2319–2329. doi: 10.11999/JEIT200058.

XU Jin, WU Huici, and TAO Xiaofeng. 5G cyberspace security game[J]. *Journal of Electronics & Information Technology*, 2020, 42(10): 2319–2329. doi: 10.11999/JEIT200058.

[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] 张海波, 李虎, 陈善学, 等. 超密集网络中基于移动边缘计算的任务卸载和资源优化[J]. 电子与信息学报, 2019, 41(5): 1194–1201. doi: 10.11999/JEIT180592.

ZHANG Haibo, LI Hu, CHEN Shanxue, *et al*. Computing offloading and resource optimization in ultra-dense networks with mobile edge computation[J]. *Journal of Electronics & Information Technology*, 2019, 41(5): 1194–1201. doi: 10.11999/JEIT180592.

[6] 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.

[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] 赵星, 彭建华, 游伟. 基于Lyapunov优化的隐私感知计算卸载方法[J]. 电子与信息学报, 2020, 42(3): 704–711. doi: 10.11999/JEIT190170.

ZHAO Xing, PENG Jianhua, and YOU Wei. A privacy-aware computation offloading method based on Lyapunov optimization[J]. *Journal of Electronics & Information Technology*, 2020, 42(3): 704–711. doi: 10.11999/JEIT190170.

[14] WANG Shangguang, ZHAO Yali, XU Jinliang, *et al*. Edge server placement in mobile edge computing[J]. *Journal of Parallel and Distributed Computing*, 2019, 127: 160–168. doi: 10.1016/j.jpdc.2018.06.008.

[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] 黄开枝, 潘启润, 袁泉, 等. 一种侧信道风险感知的虚拟节点迁

移方法[J]. 电子与信息学报, 2019, 41(9): 2164–2171. doi: 10.11999/JEIT180905.

HUANG Kaizhi, PAN Qirun, YUAN Quan, *et al*. A virtual node migration method for sensing side-channel risk[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2164–2171. doi: 10.11999/JEIT180905.

[18] SWEENEY L. k-anonymity: A model for protecting privacy[J]. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002, 10(5): 557–570. doi: 10.1142/S0218488502001648.

赵　星：男，1990年生，博士生，研究方向为移动通信网络安全、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.

陈　璐：女，1989年生，博士生，研究方向为移动通信网络安全、MEC安全防护技术.

责任编辑：马秀强