

基于隐私度和稳定度的 D2D 数据共享伙伴选择机制

黄章健^{1,2}, 叶帼华^{1,2}, 姚志强^{1,2}

(1. 福建师范大学数学与信息学院, 福建 福州 350117;

2. 福建省公共服务大数据挖掘与应用工程技术研究中心, 福建 福州 350117)

摘要: 设备到设备 (D2D) 数据共享已经成为一种很有前途的卸载蜂窝网络流量的解决方案, 但数据共享伙伴的隐私脆弱性和服务不稳定性影响着共享服务的质量。针对这个问题, 提出一种基于隐私度和稳定度的 D2D 数据共享伙伴选择机制 (PSUS)。首先对提供者的隐私信息进行抽象和概括, 根据提供者的隐私偏好和历史共享记录构建隐私度量的方法, 得出提供者在不同共享服务中的隐私度; 然后基于隐私度来设计数据共享过程, 提供者在隐私偏好约束下缓存数据并在隐私度低的时候参与共享服务以满足提供者的隐私要求; 最后在已满足隐私要求的提供者的基础上, 设计一种多指标评价法来评估提供者的服务稳定性以选择稳定的共享伙伴。通过性能分析, 证明所提机制的可行性。

关键词: D2D 数据共享; 隐私偏好; 隐私度量; 多指标评价

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019060

D2D data sharing partner selection mechanism based on privacy degree and stability degree

HUANG Zhangjian^{1,2}, YE Guohua^{1,2}, YAO Zhiqiang^{1,2}

1. School of Mathematics and Information, Fujian Normal University, Fuzhou 350117, China

2. Fujian Engineering Research Center of Public Service Big Data Mining and Application, Fuzhou 350117, China

Abstract: Device to device (D2D) data sharing has become a promising solution to offload cellular network traffic, but the privacy vulnerability and service instability of data sharing partners affect the quality of shared services. To solve this problem, a D2D data sharing partner selection mechanism based on degree of privacy degree and stability degree (named PSUS) was proposed. Firstly, the privacy information of the provider was abstracted and summarized, and the privacy measurement method was built according to the privacy preferences of the provider and the historical records of shared services, and the privacy degree of the provider in different shared services was obtained. Then, the data sharing process was designed based on privacy degree, and the provider cached data under the constraints of

收稿日期: 2019-04-02; 修回日期: 2019-07-11

通信作者: 姚志强, yzq@finu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61872090, No.61370078)

Foundation Item: The National Natural Science Foundation of China (No.61872090, No.61370078)

论文引用格式: 黄章健, 叶帼华, 姚志强. 基于隐私度和稳定度的 D2D 数据共享伙伴选择机制[J]. 网络与信息安全学报, 2019, 5(6): 31-41.

HUANG Z J, YE G H, YAO Z Q. D2D data sharing partner selection mechanism based on privacy degree and stability degree[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 31-41.

Key words: D2D data sharing, privacy preference, privacy metric, multi-index evaluation

一个典型的 D2D 数据共享群组内, 请求指定数据的用户称为数据需求者, 拥有所需内容且在需求者请求共享服务时提供数据的用户称为数据提供者, 在一次数据共享服务中会有众多的提供者, 提供者向需求者提供数据以减少通信延迟和卸载 BS 的流量。尽管 D2D 数据共享具有显著优势, 但在大规模应用中仍然面临两个重大的技术挑战, 即隐私性和稳定性^[5]。数据共享群组中设备之间直接相连, 彼此的可信度未知。群组内的提供者高度关注自己的隐私, 在组内向需求者传输数据时, 由于考虑自身隐私泄露问题而只提供粗粒度的数据, 大幅降低了数据共享服务的质量; 提供者多为移动用户, 资源受限问题也会影响共享服务的稳定性, 即共享易人为中断或共享时间过长, 降

综上所述, 共享伙伴的隐私性和稳定性都是影响 D2D 数据共享服务质量的重要因素。设计和构建有效的共享伙伴选择机制, 对于保证一定数量的提供者在满足其隐私要求下参与共享服务和需求者稳定的获取所需数据具有重要的研究意义。为保证数据共享服务的隐私性和稳定性, 本文提出一种 D2D 数据共享伙伴选择机制 (PSUS)。通过隐私偏好的设置和历史共享记录度

量出提供者对某次共享服务生成的隐私信息的高度重视程度（即隐私度），由此设计 D2D 数据共享过程以满足提供者的隐私要求；同时基于提供者的声誉、可持续时长、等待时间和传输速率 4 个指标来评估提供者的服务稳定性程度（即稳定度），在满足隐私要求的提供者中优先选择稳定度高的作为共享伙伴，保证数据共享服务的质量。

2 相关工作

目前，国内外研究学者先后在 D2D 数据共享服务中的隐私性和稳定性问题方面提出研究成果。在隐私性方面，Hua 等^[9]对信息交换过程中的隐私保护问题进行研究，提出场景自适应的隐私度量的研究方向。Wishart 等^[10]根据共享数据内容和周围环境对共享数据进行模糊处理，提供者根据现实情况设置数据的模糊程度，还可以控制向谁共享数据，并设置共享的策略和共享数据的详细级别。Franz 等^[11]的方法是在共享群组的所有成员之间协商隐私策略，包括共享哪些数据以及其准确性。也有一些研究者将工作重心放在设计安全的 D2D 数据共享协议上，Wang 等^[12]提出两种隐私保护认证和密钥协议（PPAKA-HAMC 和 PPAKA-IBS），以保证安全和匿名的 D2D 共享服务。Mohseni-Ejyeh 等^[13]提出一种在 D2D 通信中进行安全数据共享的有效协议，该协议可禁止未经授权的提供者参与服务，还可通过授权来操作提供者的历史记录，若恶意行为超过阈值，会惩罚行为不端的提供者。

在 D2D 数据共享服务的稳定性方面，为需求者选择合适的提供者是研究者的主要工作。Yan 等^[14]提出一种用于多媒体传输的社会意识信任框架以从 D2D 中继用户中选择值得信赖的 D2D 协作用户。He 等^[15]提出一个综合评分机制（CSM），它根据历史共享记录、当前传输速率和预期奖励计算每个候选提供者的分数，并且基于

CSM 和匈牙利算法，提出共享激励和提供者选择（CIPS）算法，以优化多个并发需求者的数据提供者的选择。部分常见的伙伴选择方案是基于声誉机制^[7-8]的，但其共性的问题有二：一是声誉更新需要进一步考虑，二是仅依赖声誉值的共享伙伴选择机制存在偏差或不全面，可能导致数据共享服务不稳定。

上述工作多数是考虑隐私性或者稳定性中的一个问题，对 D2D 数据共享伙伴选择的研究缺乏综合性，即在共享群组内考虑隐私的方案中未关注共享服务的稳定性，或者着重于稳定性问题的方案中忽略了提供者的隐私，这都将降低 D2D 数据共享服务的质量。本文所提出的共享伙伴选择机制从隐私性和稳定性两方面出发，提供者只在满足隐私阈值的情况下参与数据共享或者缓存共享数据，并且通过稳定度从已经满足隐私要求的提供者中确定共享伙伴。

3 系统模型

本文考虑需求者通过 BS 协作的方式从多个提供者处获取数据的场景，具体形式如图 1 所示。BS 主要用于管理数据共享群组中的通信，包括用户的接入认证、资源调度时的数据转发和隐私保护等^[16]。在数据缓存方面，BS 因和网络服务器直接相连，因此它可为需求者提供任何所需的数据。另外，一些提供者会主动在自己设备中缓存一些数据以快速响应共享服务。具体来说，通过 D2D 通信方式进行数据共享需要以下步骤：1) 一个需求者向 BS 发起共享请求；2) BS 将数据请求在需求者的 D2D 通信距离内广播给其他 UE，只有那些数据符合要求的提供者才会回应，其他的提供者则保持沉默；3) 如果在预定的时间内没有响应，即需求者周围没有合适的提供者，BS 将直接向需求者发送请求的数据；4) BS 将监控整个数据共享过程，直到共享服务完成。

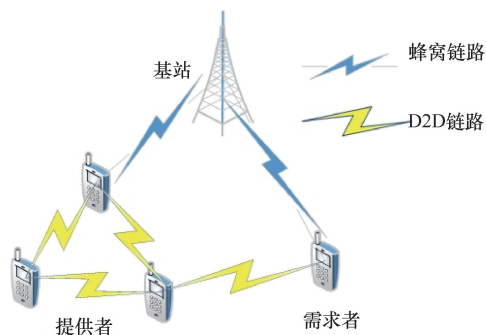


图 1 D2D 数据共享模型

一般来说, D2D 通信的用户多为移动用户且采用无线连接, 这可能给 D2D 的数据共享服务带来一些问题, 包括隐私泄露、数据传输缓慢和共享中断或更改等, 这都影响着共享服务的质量。为了改善这种情况, 本文提出了共享伙伴选择机制 (PSUS)。该机制关注提供者的隐私问题, 利用数据共享服务中提供者对隐私信息的重视偏好并结合历史共享记录为提供者设计隐私度量过程 (PMP), 得出候选提供者的隐私度; 在充分了解提供者的隐私度后, 通过 BS 设计基于隐私度的数据共享过程 (BPP) 并对候选的提供者进行了第一次筛选, 形成满足隐私要求的提供者集合; 为了进一步确保共享伙伴的服务稳定性, 设计多指标评价的方法评估 BPP 中满足隐私要求提供者的服务稳定性, 得出提供者的稳定度后按稳定度从高到低选择共享伙伴, 该过程称为提供者服务稳定性的评价过程 (SEP)。为了直观表示提出的

伙伴选择机制, 用一个六元组 $PSUS = (U, D, PI, PMP, BPP, SEP)$ 来概述。其中, $U = \{u_1, u_2, \dots, u_n\}$ 是所有提供者的集合; $D = \{d_1, d_2, \dots, d_s\}$ 是需求者的集合; PI 是提供者的隐私信息, 同时给出图 2 所示的机制流程。

4 PSUS 的构造

4.1 隐私度量

使用 D2D 连接的 UE 在共享数据时会生成诸如位置、时间、通信持续时间、设备类型、服务请求类型等可用于识别自身的信息^[17], 这些信息在数据共享过程中会暴露提供者的隐私。不同的提供者对于共享服务中的这些信息的重视程度不同, 即可通过这部分信息度量其隐私度的高低, 而隐私度的高低影响着提供者在共享服务中的表现, 所以尽量选择隐私度低的提供者作为共享伙伴以达到满足不同提供者隐私要求的目的, 同时提高共享服务质量。考虑到隐私的主观性, PSUS 为了合理地度量出某提供者的隐私度, 利用提供者在数据共享服务中对生成隐私信息的重视偏好, 同时结合其历史共享记录, 形式化定义并运用数学方法量化提供者的隐私。

定义 1 隐私信息

隐私信息 (PI) 是数据提供者在共享数据时生成的设备类型 (E)、数据服务类型 (S)、共享

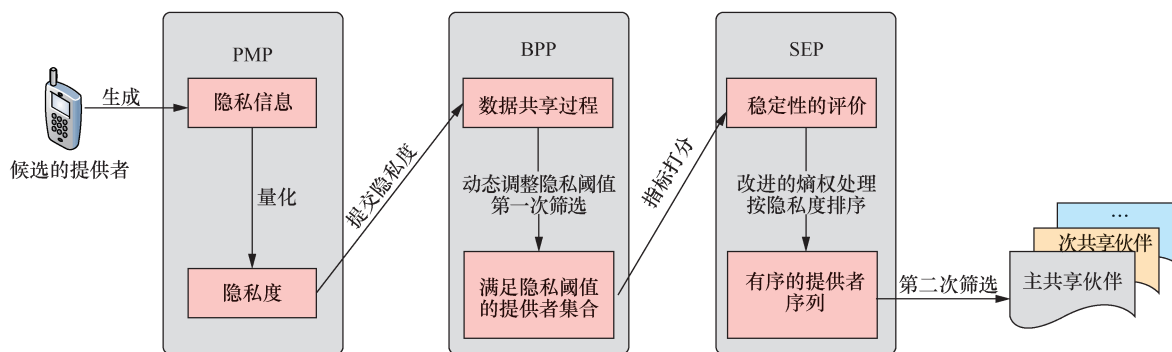


图 2 PSUS 的流程

时间(T)和共享位置(L)的信息,即 $PI = \{E, S, T, L\}$ 。例如,提供者于上午 9:00 在家里使用 iPhone X 手机为某个需求者提供关于银行的一些数据,则本次生成的隐私信息为 $PI = \{\text{iPhone X, 银行数据, 9.00, 家}\}$ 。

定义 2 隐私偏好

隐私偏好(PP)是提供者对生成的隐私信息重视程度的主观倾向,包含设备信息偏好(EP)、数据服务类型偏好(SP)、数据共享时间偏好(TP)和数据共享位置偏好(LP)。

提供者在进行数据共享前,可在设备中设置隐私偏好的内容作为隐私首选项,这相当于一种隐私约束。在进行 D2D 数据共享服务时,提供者的设备会为每个隐私首选项创建一个标志 CI,若一个提供者在某次服务生成的隐私信息满足隐私首选项的约束条件,则设置 $CI=1$,否则设置 $CI=0$,并统计 $CI=1$ 的数量(记为 PI^+)和 $CI=0$ 的数量(记为 PI^-)。PSUS 使用隐私偏好贴合度(PPR)描述隐私信息满足提供者首选项的程度,具体的函数表达式如下。

$$PPR = \frac{PI^+}{N} \quad (1)$$

其中, N 表示隐私首选项的总项数,显然这里取 $N=4$ 且 $PI^+ \leq 4, PI^- \leq 4$ 。

PI 元组中的内容通过共享服务实时生成,每个提供者生成的内容不同,为了方便表述,现将其称为子元素,即每个提供者生成的子元素是不同的。某子元素的生成频率越高,则该子元素对提供者的重要性越高,从而判断该子元素包含的隐私较多。为了更加全面量化提供者的隐私度,本文通过历史共享记录计算出 PI 中各元组子元素的生成频率来实现。生成频率指在一段时间内子元素的出现频次占整个时间段中隐私信息总出现频次的比值。假设提供者 i 在 (t_1, t_2) 生成的隐私信息为 $PI_i = \{E_i, S_i, T_i, L_i\}$, 每个元组下有 l 种子

元素(如 $E_i \in \{E_1, E_2, \dots, E_l\}$), $PI_i^{v,l}$ ($v=1,2,\dots,4$) 表示提供者 i 在 (t_1, t_2) 时间段生成的第 v 个元组下的子元素,则提供者 i 的隐私信息中第 l 种子元素生成频率为

$$P_{PI_i^{v,l}} = \frac{\text{num}PI_i^{v,l}}{\text{sum}PI_i} \quad (2)$$

其中, $\text{num}PI_i^{v,l}$ 表示提供者 i 第 v 个元组中第 l 种子元素的出现频次, $\text{sum}PI_i$ 为整个时间段中提供者 i 隐私信息的总出现频次。

因隐私信息为四元组形式,则提供者 i 各元组下第 l 种子元素的平均生成频率($\text{avg}P_{PI_i}$)为

$$\text{avg}P_{PI_i} = \frac{\sum_{v=1}^N P_{PI_i^{v,l}}}{N} \quad (3)$$

其中, $\sum_{v=1}^N P_{PI_i^{v,l}}$ 表示各元组中第 l 种子元素的生成频率总和。

另外,在 D2D 数据共享群组中,设备与设备是直接相连的,彼此之间可能从未谋面,每个设备之间熟悉度未知,因此提供者在进行共享数据服务时,对隐私信息泄露风险的态度,会对其隐私度产生影响。Jensen 等^[18]为设备与设备之间的交互给出 3 种态度(乐观、中立、谨慎),本文将其对应为提供者在数据共享服务中的隐私风险态度,并用 θ 表示。

综上,PSUS 使用隐私偏好和历史共享记录作为度量因子并考虑隐私风险态度(θ)来量化提供者的隐私,其中使用 PP 得到 PPR,通过历史共享记录得到 $\text{avg}P_{PI_i}$,则提供者 i 的隐私度 Pr_i 为

$$Pr_i = (PPR_i \cdot \text{avg}P_{PI_i})^{\frac{1}{2\theta}} \quad (4)$$

其中, $\theta \in [0,1)$ 表示乐观, $\theta=1$ 表示中立, $\theta \in (1,2]$ 表示谨慎,上述值是模拟隐私风险态度对隐私值的影响,即共享过程中持谨慎态度的提供者的私有信息隐私度应高于其实际值;对本次数据共享

群组熟络的提供者, 持乐观态度的隐私度低于实际值; 而持有中立态度的提供者对于每一次通信都持公平态度, 隐私度和实际值变化应是一致的。因 PPR 和 $avgP_{Pl_i}$ 值均小于 1, 为了避免相乘后的值过小, 这里取其二次根式。

4.2 基于提供者隐私度的数据共享过程

通过上述的隐私度量过程, 得到提供者在某次共享服务中的隐私度后, 由此构建一种动态的 D2D 数据共享过程, 其过程如图 3 所示。

- 1) 需求者向 BS 发起数据共享请求。
- 2) 提供者在数据共享等待期间, 在隐私首选项的约束下主动缓存数据以获得主动缓存收益^[19], 同时提高数据共享服务的速率。
- 3) BS 将数据请求在需求者的 D2D 通信距离内广播给提供者, 数据符合要求的提供者予以回应。
- 4) 提供者的设备生成此次共享服务的隐私信息, 并通过 PMP 获得自己的隐私度。
- 5) 对提供者的数值型隐私值进行泛化: 提供者可通过向 BS 提交隐私度获得一些隐私保护方面的收益, 但直接向 BS 提交隐私值的操作可能会泄露隐私信息。因 $Pr \in [0, 1]$, 以 0.2 为间隔将

其划分为 5 个区间, 将隐私值泛化成集合 {非常低, 低, 中, 高, 非常高} = {VL, L, M, H, VH}。

- 6) 提供者向 BS 提交泛化后的隐私度。

7) BS 将提供者数量与对应的隐私度存入隐私度分布直方图 ($Graph_{U-Pr}$), 根据不同隐私度下提供者的数量动态设置隐私阈值 (α), $\alpha \in [0, 1]$ 。

8) BS 将设置好的隐私阈值发布给组内的提供者。

9) 提供者只在隐私度小于或等于阈值时共享数据, 大于阈值时不参与本次数据共享服务, 形成隐私度符合要求的提供者集合 (U_1)。

10) 满足隐私阈值的提供者通过 D2D 链路发送数据给需求者。

隐私阈值的设置相当于对提供者集合 U 进行一次筛选, 提供者在隐私首选项的约束下主动缓存低隐私度的数据, BS 依据提供者的隐私度分布动态设置隐私阈值, 此时被选择的是低隐私度的提供者集合 U_1 。另外, 在了解自己在本次共享服务中的隐私度后, 提供者可以自主选择在低隐私度的共享服务中提供自己的数据, 不再担心过高的隐私暴露而只提供粗粒度的数据, 这样既保证自己的

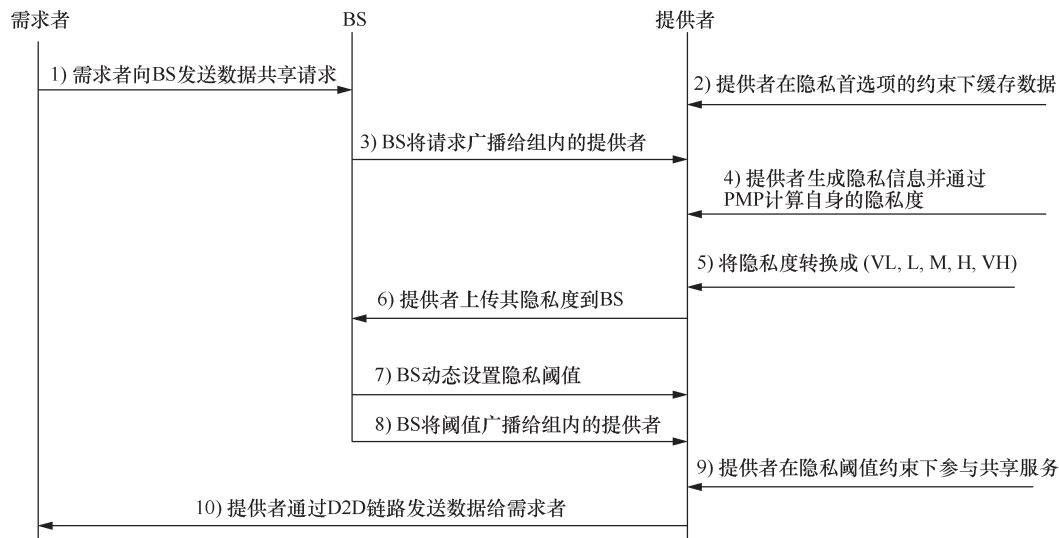


图 3 基于提供者隐私度的数据共享交互过程

隐私安全，又能提高数据共享服务的质量。

4.3 提供者服务稳定性的评价过程

在 D2D 数据共享群组内，不仅提供者的隐私性影响共享服务质量，提供者的服务稳定性也是衡量服务质量的重要指标。通过上文的方法在共享服务期间形成一个满足隐私要求的提供者集合 U_1 ，本节基于提供者的声誉 (R)、可持续时长 (SD)、等待时间 (WT) 和传输速率 (TR) 4 个指标从 U_1 中进一步选择共享伙伴来保证数据共享的稳定性，详细描述如下。

4.3.1 指标的评价值

定义 3 贡献值

贡献值 (CV) 是提供者完成数据共享服务的任务量。假设提供者请求的数据总量为 Q ，BS 接收到需求者请求时，会将 Q 分为 Z 个子任务形式。 $Q_z (z \in \{1, 2, \dots, Z\})$ 表示 z 个子任务的数据量，则提供者 i 在完成 z 个子任务后的贡献值为

$$CV_{i-z} = \frac{Q_z}{Q} \quad (5)$$

定义 4 共享数据评价

共享数据评价 (SDE) 是需求者对提供者共享服务完成质量的评价。其中 $SDE = \{Y, N\}$ ， Y 表示满足需求者要求， N 表示不满足需求者要求。

为鼓励更多提供者参与 D2D 数据共享，对于新加入的提供者，BS 为其设置的初始声誉分为 R ，对于已存在的提供者，在数据共享群组内主要涉及其声誉值的更新，提供者 i 的声誉更新值 R'_i 为

$$R'_i = \begin{cases} R + CV_{i-z} & SDE = Y \\ R - \beta \cdot CV_{i-z} & SDE = N, R'_i \geq R \end{cases} \quad (6)$$

其中， β 为惩罚因子， $\beta \in [0, 1]$ ， β 值越大，惩罚力度越大。

另外，提供者在离开 D2D 共享群组期间声誉应随时间衰减，提供者 i 的声誉衰减为

$$R_i = R'_i e^{-\sigma \Delta t} \quad (7)$$

其中， σ 为声誉衰减因子， $\sigma \in [0, 1]$ ， σ 越大，声誉衰减越快， Δt 为提供者不参与数据共享的时间周期。

这里主要阐述声誉值的更新，因为可持续时长、等待时间和传输速率均可从实际的 D2D 数据共享网络环境中获取。在 D2D 数据共享进行阶段由 BS 监控整个共享服务，每次服务开始前会获取满足隐私要求的提供者上述 4 个指标的实际数据并为其评价打分，分值区间为 $[0, 10]$ ，其中，0 表示提供者在服务中该指标表现最差，10 表示提供者在服务中该指标表现最好。

4.3.2 稳定性的评价

为了直观统一地衡量 4 种指标在稳定性评估中的作用，将提供者集合 U_1 中各指标进行加权求和处理，其结果称为提供者在共享服务中的稳定度，用 St 表示，并用熵权法^[20]确定不同指标的权重大小，其表示的含义是某指标的信息熵越小，则该指标值的变异程度越大，可提供的信息量也就越大，在评价过程中所起作用就越大，赋予的权重理应越高，但传统的熵权法在计算权值时有一定的弊端。为了解决这个问题，PSUS 采用改进的熵权法，具体的步骤如下。

Step1 集合 U_1 中有 n 个提供者， $m(m=4)$ 个指标，则 y'_{ij} 为第 j 个指标下第 i 个提供者的评价 ($i=1, 2, 3, \dots, n; j=1, 2, \dots, m$)，表示稳定性评价矩阵。

$$Y = \begin{bmatrix} y'_{11} & y'_{12} & \dots & y'_{1m} \\ y'_{21} & y'_{22} & \dots & y'_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ y'_{n1} & y'_{n2} & \dots & y'_{nm} \end{bmatrix} \quad (8)$$

Step2 评价矩阵预处理，删除数据完全相同的列。因熵权法是根据指标数据之间的离散性来决定权重大小的，当某指标下的数值完全相同时，那么该指标将无法提供任何有价值的信息，故将

其删除,但若所有指标值均相同,则 D2D 数据共享伙伴的选择变更为 BS 分配。

Step3 对提供者的各指标值进行归一化处理。

$$y_{ij} = \frac{y'_{ij} - \min\{y'_j\}}{\max\{y'_j\} - \min\{y'_j\}} \quad (9)$$

其中, $\min\{y'_j\}$ 是第 j 个指标下的最小值, $\max\{y'_j\}$ 是第 j 个指标下的最大值。

Step4 计算第 j 个指标下第 i 个提供者指标值的比重为

$$p_{ij} = \frac{y_{ij}}{\sum_{i=1}^n y_{ij}} \quad (10)$$

Step5 计算第 j 个评价指标的熵为

$$e_j = -1/\ln(n) \sum_{i=1}^n p_{ij} \ln(p_{ij}) \quad (11)$$

Step6 加入修正因子的 4 项指标的权重值计算。

$$\omega_j = \frac{1 - e_j}{\sum_{j=1}^m (1 - e_j)} \quad (12)$$

$$\omega_j = \frac{1 - e_j + k}{\sum_{j=1}^m (1 - e_j + k)} \quad (13)$$

采用式(13)是因为文献[21]中发现传统的熵权公式(12)在指标熵值 e_j 接近于 1 时, e_j 之间微小的差别也会引起其所对应的权值成倍数地变化,显然这样的权重分配是不合理的,建议式(12)中加入修正因子,即 k 为修正因子,本文取 $k = \frac{1}{m} \sum_{j=1}^m (1 - e_j)$,文献[21]给出了修正因子取上述值的合理证明。

Step7 提供者 i 的稳定度为

$$St_i = \sum_{j=1}^m \omega_j y_{ij} \quad (14)$$

稳定度越高,提供者在数据共享服务中的表

现越好。在得到 U_i 中各提供者的稳定度后,使用快速排序按稳定度从高到低排序提供者序列。根据排序的结果,需求者从 U_i 中选择稳定度最高的作为主共享伙伴,如果该提供者无法提供所有数据,需求者仍会按照稳定度的顺序继续选择次共享伙伴。

5 性能分析

5.1 理论分析

在 D2D 数据共享服务中,共享伙伴的隐私性和服务稳定性都影响着共享服务的质量。本文关注到若一个提供者在满足其隐私要求下参与共享服务和稳定地向需求者共享其所需数据是解决上述问题的关键。因此,基于 D2D 数据共享的网络模型,提出一种共享伙伴的选择机制 PSUS,为需求者合理分配共享伙伴的同时保证提供者的隐私安全和共享服务的稳定。PSUS 关注到提供者在共享服务中的隐私问题,在每次共享服务开始前获取到提供者的隐私度,通过选择隐私度低的提供者参与共享服务可减少隐私泄露。首先,PSUS 依据文献[17]中提出的 D2D 通信会生成部分关于用户隐私信息的概念,在其基础上对其加以概括得到新的隐私信息的定义和提出隐私首选项的设置;又考虑到隐私的主观性,将提供者的隐私偏好、历史共享记录和隐私风险态度作为度量因子,运用数学方法合理地量化提供者隐私,得出提供者的隐私度。其次,PSUS 通过候选提供者的隐私度构建新的数据共享过程,提供者在隐私首选项的约束下主动缓存数据,且在高于 BS 设置的隐私阈值时,不会参与共享服务,这将有效减少 D2D 数据共享组内提供者的隐私度,让提供者在数据共享阶段不再担心过高的隐私暴露而只提供粗粒度的数据。

另外,PSUS 在满足隐私要求提供者的基础上进一步做出工作,为了保证共享服务的稳定性,利用 4 项与提供者有关的指标对其服务稳定性进

行评估且给出符合 D2D 数据共享环境的声誉评分机制。评估稳定性时,不是简单地对指标进行求和,而是采用加权求和的方法,这显然比直接求和更具说服力。为了客观地完成稳定性的评价,PSUS 使用改进的熵权法根据指标的信息熵来合理调整各指标的权重值,比主观的分配权重更加合理。

5.2 实验仿真

本节在 Matlab 软件上对 PSUS 进行仿真分析,实验分为两个部分:基于隐私度的数据共享过程和提供者稳定度的评价过程,分别模拟由 10、30 和 50 个提供者组成的 D2D 数据共享群组, PMP 中各隐私信息类型的参数通过随机函数生成,之后按顺序实施 PMP、BPP 和 SEP 的步骤。

图 4 是分别由 10、30 和 50 个提供者组成的 D2D 数据共享服务中各提供者的隐私度分布,表 1 是 3 个 D2D 数据共享群组中的伙伴选择情况。BS 根据图 4 提供的隐私度分布直方图,动态设置如表 1 所示隐私阈值,以 $n=10$ 的组为例,BS 监控到隐私度处于 VL, L 级别的提供者较多,动态设置隐私阈值为 0.4,则该组提供者在隐私度高于 0.4 时不加入本次数据共享服务。其他两组同理,提供者在隐私度高于 0.6 时不参与共享服务,保证了提供者的隐私安全。另外,按照隐私首选项的主动缓存机制有助于提高数据共享服务的速率且不会过多暴露提供者的隐私。

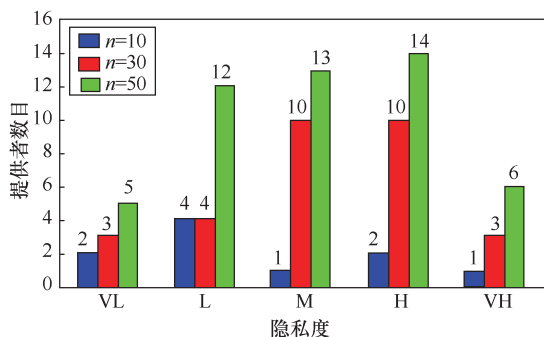


图4 提供者的隐私度分布

以上述实验中 $n=10$ 的 D2D 群组为基础,模拟 6 个已符合隐私要求的提供者的稳定性评价过

程,其中,4 个指标的权重如表 2 所示,各提供者的稳定度如表 3 所示。BS 按照稳定度排序提供者,并依据此顺序为需求者分配共享伙伴。显然,提供者 6 的稳定度比其他提供者高,其表示相比于其他的提供者具有更高的声誉、可持续时长、传输速率和更少的服务等待时间,拥有更高的服务稳定性,它将被首选为数据提供者以保证数据共享的服务质量。但提供者 6 不是唯一的共享伙伴,若需求者在和提供者 6 进行数据共享时,发现 6 无法提供所需的所有数据时,若条件允许,需求者仍会按照稳定度的高低继续和提供者 5 进行通信,以此类推,直至完成需求者的请求。

表 1 D2D 数据共享群组中的伙伴选择情况

提供者数目	隐私阈值	满足阈值的提供者数目
10	0.4	6
30	0.6	17
50	0.6	30

表 2 权重的分配

指标	权重
R	0.35
SD	0.22
WT	0.21
TR	0.22

表 3 提供者的稳定度

提供者序列	稳定度
1	0.52
2	0.16
3	0.61
4	0.21
5	0.71
6	0.88

5.3 性能评估

(1) 隐私性评估

在理论分析部分,预测 PSUS 会有效减少 D2D 数据共享组内提供者的隐私度。为了验证该推测的正确性,本节以 $n=30$ 的 D2D 数据共享群

组为环境, 在相同实验环境下, 使用 PSUS 和未使用 PSUS 的群组内进行平均隐私度 (avgPr) 变化的实验对比。

$$avgPr = \frac{sum_{U_i-Pr}}{num_{U_i}} \quad (15)$$

其中, sum_{U_i-Pr} 表示 U_i 中提供者的隐私度总和, num_{U_i} 表示 U_i 中提供者数目。

图 5 反映随着隐私阈值的增加, D2D 群组内提供者平均隐私度的变化。可以看到, 在使用 PSUS 的 D2D 群组中, 候选提供者的平均隐私度明显低于未使用 PSUS 的 D2D 群组。这是因为 PSUS 中的提供者在满足首选项约束的前提下主动缓存数据, 并只在满足隐私阈值的情况下参与共享服务, 所以参与服务的提供者隐私度较低。而未使用 PSUS 的 D2D 群组在进行数据共享服务时, 30 个提供者都可能被选择为候选且主动缓存数据隐私度未知, 则平均隐私度不随隐私阈值变化并均高于 PSUS。其中, 当隐私阈值为 1 时, 使用 PSUS 群组的候选提供者的数目为 30 个, 但 D2D 群组内提供者的隐私度仍低于未使用 PSUS 的 D2D 群组的原因是主动缓存中隐私首选项约束。图 5 反映 PSUS 的使用可以有效降低 D2D 数据共享群组内的隐私度, 减少因提供者隐私带来的数据共享服务质量下降的问题。

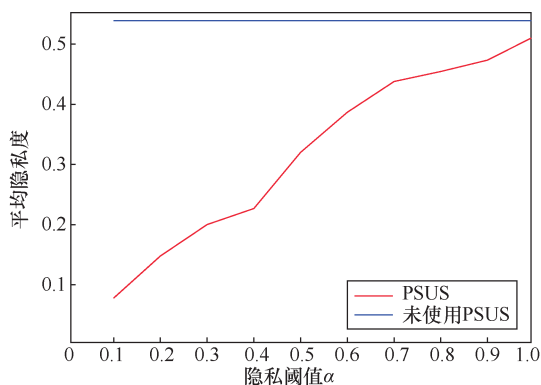


图 5 D2D 数据共享群组内隐私度对比

(2) 稳定性评估

在 D2D 数据共享群组中, 通过 4 个指标充分可靠地评估提供者的稳定性。为了保证对提供者服务稳定性评价的合理性, PSUS 不是简单地对每个指标因子进行简单求和, 而是采用加权求和的方法, 并且通过改进的熵权法根据指标的信息熵大小动态设置权重, 即在指标熵计算阶段加入了修正因子, 其合理性由文献[21]所证明, 克服了传统熵权法的弊端, 同时相对于主观的随机赋权具有较高的可信度和精确度, 也更能满足 D2D 网络环境的复杂性。因为文献[7]和文献[22]中都有对 D2D 群组中移动设备进行评价的方法, 与本文所提评价方法具有可比性, 所以表 4 给出 3 种方法的比较分析, 发现 PSUS 使用的多指标评价比文献[7]具有指标数和权重分配两个优势, 因其并没有对所选指标因子加以权重计算。对于文献[22], 虽然其所选的指标数更多, 也使用了加权求和的评估方法, 但在权重确定方面显然主观分配的方法缺乏合理性, 而比指标数目显然权重的合理分配更加重要。

表 4 3 种评价方法的比较分析

方法	指标数	评估方法	权重确定
文献[7]	3	综合评分	—
文献[22]	5	加权求和	主观分配
PSUS	4	加权求和	改进的熵权处理

6 结束语

针对 D2D 数据共享中伙伴的隐私性和稳定性影响着共享服务质量的问题, 本文提出一种基于隐私度和稳定度的共享伙伴选择机制, 利用设计的隐私度量方法得到提供者的隐私度, 并构建一种基于隐私度的数据共享过程, 保证提供者只在隐私度低的情况下参与共享数据, 同时关注到仅依靠声誉选择共享伙伴的弊端, 在前文满足隐私要求的提供者的基础上, 设计一种多指标评

价的方法来评估提供者的服务稳定性以选择最佳的共享伙伴。通过实验与理论分析中的各种结果,表明所提机制是可行的。当然所提的隐私度量方法和指标评价方法仍存在一定的局限性,未来也将集中于更加简而有效的 D2D 通信中隐私度量方法和更加智能的服务稳定性评估方法的研究。

参考文献:

- [1] PEDHADIYA M K, JHA R K, BHATT H G. Device to device communication: A survey[J]. Journal of Network and Computer Applications, 2019, 129: 71-89.
- [2] WU D, ZHOU L, CAI Y. Social-aware rate based content sharing mode selection for D2D content sharing scenarios[J]. IEEE Transactions on Multimedia, 2017, 19(11): 2571-2582.
- [3] JIANG J, ZHANG S, LI B, et al. Maximized cellular traffic offloading via device-to-device content sharing[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(1): 82-91.
- [4] MILITANO L, ARANITI G, CONDOLUCI M, et al. Device-to-device communications for 5G internet of things[J]. EAI Endorsed Transactions on Internet of Things, 2015, 15(1): 1-15.
- [5] ZHANG A, CHEN J, HU R Q, et al. SeDS: secure data sharing strategy for D2D communication in LTE-advanced networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(4): 2659-2672.
- [6] YU T, ZHOU Z, ZHANG D, et al. Indapson: an incentive data plan sharing system based on self-organizing network[C]//IEEE Conference on Computer Communications. 2014: 1545-1553.
- [7] HE J Z, WANG H B, ZHANG T. Incentive and selection for D2D content sharing: a comprehensive scoring mechanism[C]// 2016 IEEE 13th International Conference on Signal Processing (ICSP). 2016: 1208-1213.
- [8] ZHOU R F, HWANG K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing[C]//IEEE Transactions on Parallel and Distributed Systems. 2007: 460-473.
- [9] 华佳烽, 李风华, 郭云川, 等. 信息交换过程中的隐私保护技术研究[J]. 网络与信息安全学报, 2016, 2(3): 28-38.
HUA J W, LI F H, GUO Y C, et al. Research on privacy protection technology in information exchange process[J]. Journal of Network and Information Security, 2016, 2(3): 28-38.
- [10] WISHART R, HENRICKSEN K, INDULSKA J. Context privacy and obfuscation supported by dynamic context source discovery and processing in a context management system[C]//International Conference on Ubiquitous Intelligence and Computing. 2007: 929-940.
- [11] FRANZ E, SPRINGER T, HARDER N. Enhancing privacy in social applications with the notion of group context[C]//2012 International Conference for Internet Technology and Secured Transactions. 2012: 112-118.
- [12] WANG M, YAN Z. Privacy-preserving authentication and key agreement protocols for D2D group communications[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3637-3647.
- [13] MOHSENI-EJIEH A, ASHOURI-TALOUKI M, MAHDAVI M. A lightweight and secure data sharing protocol for D2D communications[C]//2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC). 2017: 42-47.
- [14] ZHANG A, WANG L, YE X, et al. Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(3): 662-675.
- [15] YAN J, WU D, WANG R. Socially aware trust framework for multimedia delivery in D2D cooperative communication[J]. IEEE Transactions on Multimedia, 2019, 21(3): 625-635.
- [16] HE J, WANG H, CHU X, et al. Incentive mechanism and content provider selection for device-to-device-based content sharing[J]. IEEE Transactions on Vehicular Technology, 2019.
- [17] JAMEEL F, HAMID Z, JABEEN F, et al. A survey of device-to-device communications: research issues and challenges[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 2133-2168.
- [18] JENSEN C D, KORSGAARD T R. Dynamics of trust evolution: auto-configuration of dispositional trust dynamics[C]//International Conference on Security and Cryptography. 2008: 509-517.
- [19] BAI B, WANG L, HAN Z, et al. Caching based socially-aware D2D communications in wireless content delivery networks: a hypergraph framework[J]. IEEE Wireless Communications, 2016, 23(4): 74-81.
- [20] JING L, NG M K, HUANG J Z. An entropy weighting k -means algorithm for subspace clustering of high-dimensional sparse data[J]. IEEE Transactions on Knowledge & Data Engineering, 2007 (8): 1026-1041.
- [21] 张近乐, 任杰. 熵理论中熵及熵权计算式的不足与修正[J]. 统计与信息论坛, 2011, 26(1): 3-5.
ZHANG J L, REN J. The deficiencies and amendments of the calculation formulate of entropy and entropy weight in the theory of entropy[J]. Statistics & Information Forum, 2011, 26(1): 3-5.
- [22] JIN B, JIANG D, XIONG J, et al. D2D data privacy protection mechanism based on reliability and homomorphic encryption[J]. IEEE Access, 2018, 6: 51140-51150.

[作者简介]



黄章健 (1994-), 男, 安徽六安人, 福建师范大学硕士生, 主要研究方向为云计算与安全服务。



叶帼华 (1976-), 女, 福建霞浦人, 福建师范大学副教授, 主要研究方向为大数据安全隐私保护和信息安全。



姚志强 (1967-), 男, 福建莆田人, 博士, 福建师范大学教授、博士生导师, 主要研究方向为大数据安全隐私保护、多媒体安全、应用安全。