(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103326822 B
(45)授权公告日 2016.02.17

(21)申请号 201310303143.5

(22)申请日 2013.07.18

(73)专利权人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 吴帆 邱富东 陈贵海

(74)专利代理机构 上海交达专利事务所 31201
代理人 王毓理 王锡麟

(51)Int.Cl.
H04L 1/00(2006.01)
H04L 29/06(2006.01)
H04L 9/00(2006.01)

(56)对比文件
CN 101800738 A,2010.08.11,
CN 102546755 A,2012.07.04,
CN 102143129 A,2011.08.03,
CN 101841557 A,2010.09.22,
US 2010156642 A1,2010.06.24,

审查员 高悦

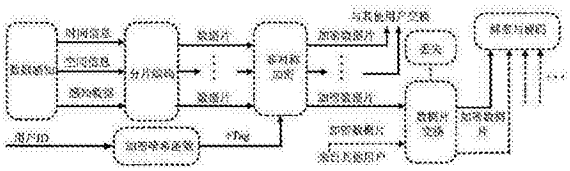
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于数据分片的参与式感知系统隐私保护方法及系统

(57)摘要

一种信息安全技术领域的基于数据分片的参与式感知系统隐私保护方法及系统，由移动设备获取原始感知数据，采用纠删码对原始数据进行分片编码，然后将经哈希函数加密后的移动设备用户标识与分片编码后的数据片进行非对称数据加密，产生用于传输的加密数据片；将加密数据片保留一片并将其余数据片与周围用户进行交换，并在交换后向服务器传输所有加密数据片；最后服务器接收到加密数据片之后通过构建数据片表实现对原始数据的重构。本发明针对参与式感知系统当中用户隐私保护问题，采用对原始感知数据(特别针对多媒体数据)进行分片编码、交换传输的思想，将数据片传送到服务提供商(服务器端)，达到隐私保护的目的，同时该机制增强了系统容错性能，降低了系统开销。



CN 103326822 B

1. 一种基于数据分片的参与式感知系统隐私保护方法，其特征在于，包括以下步骤：

第一步、由移动设备获取原始感知数据，采用纠删码对原始数据进行分片编码，然后将经哈希函数加密后的移动设备用户标识与分片编码后的数据片进行非对称数据加密，产生用于传输的加密数据片；

第二步、将第一步生成的加密数据片保留一片并将其余数据片与周围用户进行交换，并在交换后向服务器传输所有加密数据片；

第三步、服务器接收到加密数据片之后通过构建数据片表实现对原始数据的重构；

所述的交换包括：相遇交换和最小代价交换，其中：

所述的相遇交换是指：所有者将其加密数据片依次发送给移动过程中遇到的其他用户，直到加密数据片生命周期结束，然后由接收到加密数据片的用户周期性地发送给服务器；

所述的最小代价交换是指：在保证尽可能小的系统开销的前提下选取加密数据片交换对象，即设在加密数据片生命周期内，用户 $a_i \in N$ 会与 $|N(a_i)|$ 个用户相遇，对于将要相遇的每一个用户 $a_j \in N(a_i)$ 而言，$p(a_j)$ 表示 a_j 与 a_i 的相遇概率，$c(a_j)$ 表示 a_j 与 a_i 交换一片数据所需要承担的系统开销。

2. 根据权利要求 1 所述的方法，其特征是，所述的相遇概率 $p(a_j)$ 和系统开销 $c(a_j)$ 通过历史数据和移动预测模型获得；

所述的移动预测模型是指：对于每个用户 $a_j \in N(a_i)$，在保证尽可能小的系统开销前提下，选取一个子集 $F \subseteq N(a_i)$ 作为其加密数据片的中继传输节点，并且满足下面的任意一个条件：

条件 1：要求至少遇到 m-1 个用户，即满足：

Objective：$$\min \sum_{a_j \in N(a_i)} c(a_j) p(a_j) x_j$$

Subject to：$$\sum_{a_j \in N(a_i)} p(a_j) x_j \geq m-1, \quad (1);$$

$$x_j \in \{0,1\}, \forall a_j \in N(a_i) \quad (2);$$

上述公式 (1) 保证了用户 $a_i \in N$ 至少遇到 m-1 个其他用户，公式 (2) 表示 x_j 取值范围，$x_j = 1$ 表示 a_j 被选为交换对象，反之则表示没有被选中；

条件 2：要求遇到至少 m-1 个用户的概率至少为 P，$0 \leqslant P \leqslant 1$，即满足：

Objective：$$\min \frac{\sum_{\vec{y}: \sum_{a_k \in N(a_i)} x_k y_k = m-1} \left(\sum_{a_j \in N(a_i)} (c(a_j) x_j y_j) \prod_{a_j \in N(a_i)} p(a_j)^{y_j} \right)}{\sum_{\vec{y}: \sum_{a_k \in N(a_i)} x_k y_k = m-1} \prod_{a_j \in N(a_i)} p(a_j)^{y_j}};$$

Subject to：$$\sum_{t=m-1}^{\sum_{a_k \in N(a_i)} x_k} \sum_{\vec{y}: \sum_{a_k \in N(a_i)} x_k y_k = t} \prod_{a_j \in N(a_i)} \left(p(a_j)^{y_j} \cdot (1-p(a_j))^{1-y_j} \right) \geq P \quad (5);$$

$x_j \in \{0,1\}, \forall a_j \in N(a_i)$ (6);

上述公式 (5) 保证 a_i 遇见至少 m-1 个其他用户的概率至少为 P，满足条件 2 的要求；$\vec{y}$ 为长度为 $|N(a_i)|$ 的向量。

3. 根据权利要求 1 所述的方法，其特征是，所述的第三步具体步骤包括：

3.1) 根据收到的加密数据片，采用非对称解密技术以及对应第一步中用户的私钥，对加密数据片进行解密，得到标识信息和编码后数据片；

3.2) 将标识信息和编码后数据片加入数据片表中，并判断当属于同一条原始数据的编码后数据片至少达到 k 片时，则采用与第一步对应的纠删码解码技术重构出该原始数据 <t, l, d>；

3.3) 将属于该原始数据的编码后数据片从数据片表中删除，并保存所重构出来的原始数据信息 <t, l, d>，直至完成所有加密信息片的解密，得到所有原始感知数据。

4. 一种实现上述任一权利要求所述方法的系统，其特征在于，包括：感知数据分片编码模块、数据片交换模块和数据偏解码重构模块，其中：感知数据分片编码模块与数据片交换模块相连并传输编码加密后数据片信息，数据片交换模块与数据偏解码重构模块相连并传输编码加密后数据片信息。

5. 根据权利要求 4 所述的系统，其特征是，所述的感知数据分片编码模块包括：纠删码编码单元、标识信息生成单元、非对称加密单元，其中纠删码编码单元是对原始数据进行切分编码，标识信息生成单元是根据用户信息生成用于数据充足的唯一标识，非对称加密单元是对编码后数据片和标识信息进行加密，防止信息窃听。

6. 根据权利要求 4 所述的系统，其特征是，所述的数据片交换模块包括：数据片交换单元，该单元负责确定数据片的转发对象集合，并将编码加密后的数据片转发给该集合对象。

7. 根据权利要求 4 所述的系统，其特征是，所述的数据偏解码重构模块包括：非对称解密单元、纠删码解码重构单元，其中非对称解密单元与前面的非对称加密单元相对应，负责加密数据的解密，纠删码解码重构单元与前面的纠删码编码单元相对应，负责编码数据片的解码重组。

基于数据分片的参与式感知系统隐私保护方法及系统

技术领域

[0001] 本发明涉及的是一种信息安全技术领域的方法及系统，具体是一种基于数据分片的参与式感知系统隐私保护方法及系统。

背景技术

[0002] 参与式感知系统(Participatory Sensing Systems)指利用众多移动通信设备的内置传感器件来进行数据的感知、收集、分析及反馈应用的新型数据服务模式。随着通信技术、传感器技术和移动设备技术的发展，内嵌众多感知器件的手持移动设备得到迅速普及，由此使得参与式感知系统成为当今研究热点。其主要面临两大难题：一是参与用户的隐私数据保护问题：感知数据通常都会带有空间、时间等信息，如果直接由感知用户发送到服务提供商，容易泄露当前用户隐私，比如身份信息、家庭及工作地点、旅游路线、甚至是生活方式及习惯等，反之，隐私信息无法得到有效保护将会直接影响参与者的参与热情，阻碍参与式感知系统的发展；二是缺少针对多媒体数据类型的参与式感知，例如对视频、音频及图像的获取、传输及处理存在很多问题。

[0003] 基于以上的观察，本发明提出一种基于数据分片编码、交换传输思想的隐私信息保护机制，该机制适用于参与式感知系统，特别是针对多媒体数据类型具有较好的隐私保护效果，同时，该机制可以极大的提高系统整体的容错性能，降低移动设备的系统开销。

[0004] 经过对现有技术的检索发现，中国专利文献号 CN101808095，公开日 2010-08-18，公开了一种分布式存储环境下的加密副本组织方法，将系统数据的管理单位数据块分成多个大小相等数据段，系统仍以块为单位进行管理，客户端以数据段为单位对数据进行加密，这样就能对数据块提供更细粒度的控制。由于数据块是被分段加密的，故各个密文数据段之间不具有相关性，可以被并行的加解密，避免了小数据量的读写就对整个数据块进行加解密带来的巨大开销；对于大数据量的读，将读请求进行分组，将不同的分组请求并行的发送到维护着被请求文件数据块副本的各个存储节点，并行读取各个分组，提高读数据的效率。该技术实现了在分布式存储环境下应用加密技术和副本技术，所提出的加密副本组织方法极大的提高了读写数据的效率。但该技术是基于分布式存储环境下、适用于大数量的一种加密手段，但对于具有高移动性、低数据处理能力、小数据量的参与式感知系统是完全不适用的。

发明内容

[0005] 本发明针对现有技术存在的不足，提出一种基于数据分片的参与式感知系统隐私保护方法及系统，针对参与式感知系统当中用户隐私保护问题，采用对原始感知数据（特别针对多媒体数据）进行分片编码、交换传输的思想，将数据片传送到服务提供商（服务器端），达到隐私保护的目的，同时该机制增强了系统容错性能，降低了系统开销。

[0006] 本发明是通过以下技术方案实现的：

[0007] 本发明涉及一种基于数据分片的参与式感知系统隐私保护方法，包括以下步骤：

[0008] 第一步、由移动设备获取原始感知数据，采用纠删码对原始数据进行分片编码，然后将经哈希函数加密后的移动设备用户标识与分片编码后的数据片进行非对称数据加密，产生用于传输的加密数据片。

[0009] 第二步、将第一步生成的加密数据片保留一片并将其余数据片与周围用户进行交换，并在交换后向服务器传输所有加密数据片。

[0010] 所述的交换包括：相遇交换和最小代价交换。

[0011] 所述的相遇交换是指：所有者将其加密数据片依次发送给移动过程中遇到的其他用户，直到加密数据片生命周期结束，然后由接收到加密数据片的用户周期性地发送给服务器。

[0012] 所述的最小代价交换是指：在保证尽可能小的系统开销的前提下选取加密数据片交换对象，即设在加密数据片生命周期内，用户 $a_i \in N$ 会与 $|N(a_i)|$ 个用户相遇，对于将要相遇的每一个用户 $a_j \in N(a_i)$ 而言，$p(a_j)$ 表示 a_j 与 a_i 的相遇概率，$c(a_j)$ 表示 a_j 与 a_i 交换一片数据所需要承担的系统开销。

[0013] 所述的相遇概率 $p(a_j)$ 和系统开销 $c(a_j)$ 通过历史数据和移动预测模型获得。

[0014] 所述的移动预测模型是指：对于每个用户 $a_j \in N(a_i)$，在保证尽可能小的系统开销前提下，选取一个子集 $F \subseteq N(a_i)$ 作为其加密数据片的中继传输节点，并且满足下面的任意一个条件：

[0015] 条件 1：要求至少遇到 m-1 个用户（满足该条件的问题称之为 MCT-EXP 问题），即满足：

[0016] Objective：$$\min \sum_{a_j \in N(a_i)} c(a_j)p(a_j)x_j$$

[0017] Subject to：$$\sum_{a_j \in N(a_i)} p(a_j)x_j \geq m-1, \quad (1);$$

[0018] $$x_j \in \{0,1\}, \forall a_j \in N(a_i) \quad (2)。$$

[0019] 上述约束条件 (1) 保证了用户 $a_i \in N$ 至少遇到 m-1 个其他用户，约束条件 (2) 表示 x_j 取值范围，$x_j = 1$ 表示 a_j 被选为交换对象，反之则表示没有被选中。

[0020] 条件 2：要求遇到至少 m-1 个用户的概率至少为 P，$0 \leqslant P \leqslant 1$（满足该条件的问题称之为 MCT-PRO 问题），即满足：

[0021] Objective：$$\min \frac{\sum_{\vec{y}:\sum_{a_k \in N(a_i)} x_k y_k = m-1} \left(\sum_{a_j \in N(a_i)} (c(a_j)x_j y_j) \prod_{a_j \in N(a_i)} p(a_j)^{y_j} \right)}{\sum_{\vec{y}:\sum_{a_k \in N(a_i)} x_k y_k = m-1} \prod_{a_j \in N(a_i)} p(a_j)^{y_j}};$$

[0022] Subject to：$$\sum_{t=m-1}^{\sum_{a_k \in N(a_i)} x_k} \sum_{\vec{y}:\sum_{a_k \in N(a_i)} x_k y_k = t} \prod_{a_j \in N(a_i)} \left(p(a_j)^{y_j} \cdot (1-p(a_j))^{1-x_j}\right) \geq P \quad (5);$$

[0023] $$x_j \in \{0,1\}, \forall a_j \in N(a_i) \quad (6)。$$

[0024] 上述约束条件 (5) 保证 a_i 遇见至少 m-1 个其他用户的概率至少为 P，满足条件 2

的要求；$\vec{y}$为长度为 $|N(a_i)|$ 的向量。

[0025] 第三步、服务器接收到加密数据片之后通过构建数据片表实现对原始数据的重构，具体步骤包括：

[0026] 3.1) 根据收到的加密数据片，采用非对称解密技术以及对应第一步中用户的私钥，对加密数据片进行解密，得到标识信息和编码后数据片；

[0027] 3.2) 将标识信息和编码后数据片加入数据片表中，并判断当属于同一条原始数据的编码后数据片至少达到 k 片时，则采用与第一步对应的纠删码解码技术重构出该原始数据＜t,l,d＞；

[0028] 3.3) 将属于该原始数据的编码后数据片从数据片表中删除，并保存所重构出来的原始数据信息＜t,l,d＞，直至完成所有加密信息片的解密，得到所有原始感知数据。

[0029] 本发明涉及一种实现上述方法的系统，包括：感知数据分片编码模块、数据片交换模块和数据偏解码重构模块，其中：感知数据分片编码模块与数据片交换模块相连并传输编码加密后数据片信息，数据片交换模块与数据偏解码重构模块相连并传输编码加密后数据片信息。

[0030] 所述的感知数据分片编码模块包括：纠删码编码单元、标识信息生成单元、非对称加密单元，其中纠删码编码单元是对原始数据进行切分编码，标识信息生成单元是根据用户信息生成用于数据充足的唯一标识，非对称加密单元是对编码后数据片和标识信息进行加密，防止信息窃听。

[0031] 所述的数据片交换模块包括：数据片交换单元，该单元负责确定数据片的转发对象集合，并将编码加密后的数据片转发给该集合对象。

[0032] 所述的数据偏解码重构模块包括：非对称解密单元、纠删码解码重构单元，其中非对称解密单元与前面的非对称加密单元相对应，负责加密数据的解密，纠删码解码重构单元与前面的纠删码编码单元相对应，负责编码数据片的解码重组。

[0033] 技术效果

[0034] 本发明与现有技术相比，其优点包括：能够有效的保护参与式感知系统中用户的隐私信息，防范来自服务提供商和周围参与者的隐私窃取攻击，同时是第一个针对多媒体感知数据的隐私信息保护机制；其次，该方法可以极大的提高系统容错能力，保证系统较高的鲁棒性，同时减少系统通信开销和计算开销。

附图说明

[0035] 图 1 为本发明基于数据分片隐私保护机制总体架构图。

[0036] 图 2 为本发明中各个功能模块及单元关系示意图。

[0037] 图 3 为实施例中 TMU 数据片交换策略示意图。

具体实施方式

[0038] 下面对本发明的实施例作详细说明，本实施例在以本发明技术方案为前提下进行实施，给出了详细的实施方式和具体的操作过程，但本发明的保护范围不限于下述的实施例。

[0039] 实施例 1

[0040] 如图 1 所示，本实施例包括以下步骤：

[0041] 第一步、数据分片编码

[0042] 1.1) 根据用户 $a_i \in N$ 的感知数据 $< t,l,d >$ 和编码率 (k/m)，采用纠删编码方法将感知数据分割为 k 片，然后编码产生 m 片感知数据块 $\{r_{ij} | 1 \leqslant j \leqslant m\}$，其中：$a_i$ 为编号为 i 的用户，N 为所有用户的集合，$< t,l,d >$ 代表一条时间为 t、位置为 l、内容为 d 的感知数据，k 是指：纠删码技术将原始数据切分成 k 片；m 是指：k 片数据经过纠删码编码后产生的数据片数，且 $k \leqslant m$；k/m 表示编码率；r_{ij} 表示用户 a_i 的第 j 片编码后数据片；

[0043] 在本实施例中纠删码采用 RS 码或 Tornado 码实现；

[0044] 1.2) 采用加密哈希算法对每个用户 a_i 生成唯一对应的标识信息 tag，即 $tag \leftarrow H(i,nonce)$，其中：H() 为哈希加密函数，i 为用户 a_i 的编号，nonce 为 [0,1] 之间的随机数；

[0045] 1.3) 采用非对称加密算法对步骤 1.1 得到的感知数据片 $\{r_{ij} | 1 \leqslant j \leqslant m\}$ 和加密用户标识 tag 进行加密，生成用于传输的加密数据片，即 $r'_{ij} = ENCRYPT(r_{ij} || tag, KEY_{pub})$，其中 ENCRYPT(·，·) 为非对称加密函数，|| 为字符串连接操作，KEY_{pub} 为加密公钥，r'_{ij} 为数据片 r_{ij} 对应的加密之后的数据片。

[0046] 第二步：数据片交换传输：为了防止服务提供商直接识别数据所有者的身份信息，从而泄露用户隐私信息，将第一步生成的加密数据片保留一片并将其余数据片与周围用户进行交换，并在交换后向服务器传输所有数据片。

[0047] 在本实施例中，提出了两种数据片交换策略，即相遇交换 (TMU，Transfer on Meet Up) 和最小代价交换 (MCT，Minimal Cost Transfer)。

[0048] 所述的相遇交换是指：所有者将其加密数据片依次发送给移动过程中遇到的其他用户，直到加密数据片生命周期结束，然后由接收到加密数据片的用户周期性地发送给服务器。

[0049] 如图 3 所示，形象地展示了 TMU 数据交换策略的基本思想：设 (图 3 上) 用户 A 从住所行进至办公室，用户 A 的设备目前存储有三片加密的待传输数据片，并且 A 在前进过程中依次与 B、C、D 在 T1、T2、T3 时刻相遇；则根据 TMU 交换策略 (图 3 下)，T1 时刻 A 发送给 B 数据片 A1，由于 B 无数据片可供交换，故 T1 时刻后 A 剩余 2 片，B 得到 1 片 A 的加密数据片，依次类推。

[0050] 虽然 TMU 策略可以很好的解决数据片交换问题，但是 TMU 仍是一种比较盲目的交换对象选择策略。现实环境中，不同的移动设备自身存在较大的差异 (比如能耗、带宽、传输时间、传输费用等)，故不同的移动设备在交换同一数据片时，可能导致不同的系统开销 (统称为 cost)。在这种情况下，TMU 交换策略会造成极大的系统 cost 浪费，由此本实施例中采用了最小代价交换，所述的最小代价交换是指：选取数据片交换对象的同时，能够保证尽可能小的系统开销，即设在数据片生命周期内，用户 $a_i \in N$ 会与 $|N(a_i)|$ 个用户相遇；对于每一个用户 $a_j \in N(a_i)$ 均具有两个属性 $p(a_j)$ 和 $c(a_j)$，其中 $p(a_j)$ 表示 a_j 与 a_i 相遇的概率，$c(a_j)$ 表示 a_j 与 a_i 交换一片数据所需要承担的系统开销，在本发明中 $p(a_j)$ 和 $c(a_j)$ 可通过历史数据和已有的移动预测模型 (Mobility prediction model) 获得。

[0051] 由此，MCT 策略的目标可表述为：对于每个用户 $a_j \in N(a_i)$，在保证尽可能小的系统开销前提下，选取一个子集 $F \subseteq N(a_i)$ 作为其加密数据片的中继传输节点，并且满足下面

条件之一：

[0052] 条件 1：要求至少遇到 m-1 个用户；满足该条件的问题称之为 MCT-EXP 问题；

[0053] 条件 2：要求遇到 m-1 个用户的概率至少为 P(0< = P< = 1)，满足该条件的问题称之为 MCT-PRO 问题；

[0054] 下面针对以上两个问题提出相应的解决方案：

[0055] MCT-EXP 问题解决方案

[0056] MCT-EXP 问题可形式化为 0-1 整数规划问题，建模如下：

[0057] Objective：$\min \sum_{a_j \in N(a_i)} c(a_j)p(a_j)x_j$

[0058] Subject to：$\sum_{a_j \in N(a_i)} p(a_j)x_j \geq m-1,$ (1)；

[0059] $x_j \in \{0,1\}, \forall a_j \in N(a_i)$ (2)。

[0060] 上述约束条件 (1) 保证了用户 $a_i \in N$ 至少遇到 m-1 个其他用户，约束条件 (2) 表示 x_j 取值范围，$x_j = 1$ 表示 a_j 被选为交换对象，反之则表示没有被选中。

[0061] 由于上述 MCT-EXP 问题与传统背包问题极为相似，故可以归约到 0-1 背包问题，归约结果如下：

[0062] Objective：$\max \sum_{a_j \in N(a_i)} c(a_j)p(a_j)(1-x_j)$；

[0063] Subject to：$\sum_{a_j \in N(a_i)} p(a_j)(1-x_j) \leq \sum_{a_j \in N(a_i)} p(a_j) - (m-1),$ (3)；

[0064] $x_j \in \{0,1\}, \forall a_j \in N(a_i)$ (4)。

[0065] 至此，MCT-EXP 问题完全转化为 0-1 背包问题，由于该问题已有成熟的 Fully Polynomial Time Approximation Scheme(FPTAS) 算法，可以在多项式时间内求得较好的近似解，故此处不再详细叙述。

[0066] MCT-PRO 问题解决方案：尽管 MCT-EXP 问题可以找到 FPTAS 算法解决问题，但是 MCT-EXP 问题本身存在缺陷，因为其不能保证用户 ai 与其他至少 m-1 个用户相遇的概率，即不能满足条件 2。因此，提出针对 MCT-PRO 问题的优化策略，使得用户 ai 遇见其他 m-1 个用户的概率至少为 P。

[0067] MCT-PRO 问题可形式化表示如下：

[0068] Objective：$\min \dfrac{\sum_{\vec{y}:\ \sum_{a_k \in N(a_i)} x_k y_k = m-1} \left(\sum_{a_j \in N(a_i)} (c(a_j)x_j y_j) \prod_{a_j \in N(a_i)} p(a_j)^{y_j} \right)}{\sum_{\vec{y}:\ \sum_{a_k \in N(a_i)} x_k y_k = m-1} \prod_{a_j \in N(a_i)} p(a_j)^{y_j}}$；

[0069] Subject to：$\sum_{t=m-1}^{\sum_{a_k \in N(a_i)} x_k} \sum_{\vec{y}:\ \sum_{a_k \in N(a_i)} x_k y_k = t} \prod_{a_j \in N(a_i)} (p(a_j)^{y_j} \cdot (1-p(a_j))^{1-y_j}) \geq P$ (5)；

[0070] $x_j \in \{0,1\}, \forall a_j \in N(a_i)$ (6)。

[0071] 上述约束条件 (5) 保证 ai 遇见至少 m-1 个其他用户的概率至少为 P，满足约束条件 (2) 的要求；$\vec{y}$ 为长度为 |N(a$_i$)| 的向量，约束条件 (6) 与约束条件 (2)、(4) 相同。

[0072] 经过分析，上述问题为 NP 难问题，无法在多项式时间内求的最优解，由此提出一种多项式贪心算法解决 MCT-PRO 问题，该算法分为两个步骤完成，步骤一称为发现临界用户，步骤二称为确定目标集合，具体可描述如下：

[0073] 首先，判断条件 |N(a$_i$)| ＜ m-1 是否成立，若成立，则说明集合元素个数少于 m-1，无法满足条件 2 的要求，程序停止，算法无解，其中 |N(a$_i$)| 表示可能与用户 a$_i$ 相遇的用户个数；

[0074] 否则，对于集合 N(a$_i$) 元素按照 p(a$_j$)/c(a$_j$) 降序排序得到序列 $\beta: a'_1, a'_2, \cdots, a'_{|N(a_i)|}$，对 β 序列采用动态规划算法，找出 β 序列中第一次使得约束条件 (5) 得到满足的前 α 个元素；由于 β 序列中前 α 个元素满足 (5)，分析可知，前 γ（γ ≥ α）个元素也一定满足约束条件 (5)，记 α 为临界数，a′ $_\alpha$ 记为临界用户。

[0075] 上述的临界用户发现算法可确定临界用户 a′ $_\alpha$，则对于任意包含 β 序列前 γ ∈ {α，α+1，…，|N(a$_i$)|} 个元素的集合，均可作为 MCT-PRO 问题的可行解。下面是基于临界值 α 提出的目标集合确定算法，用来确定目标集合的规模，即 γ 的值，使得 MCT-PRO 问题的目标函数最小。

[0076] 为确定目标集合规模，将用户集合 N(a$_i$)、集合元素相遇概率 $(p(a_j))_{a_j \in N(a_i)}$ 和系统开销 $(c(a_j))_{a_j \in N(a_i)}$，以及序列 $\beta: a'_1, a'_2, \cdots, a'_{|N(a_i)|}$ 和临界用户 a′ $_\alpha$ 作为算法输入，采用动态规划的思想，找出使得 MCT-PRO 问题目标函数值最小的 γ（γ ≥ α），并取序列 β 的前 γ 个元素加入目标集合 F。该算法是一种多项式时间贪心算法，通过该算法可确定出使得系统开销最小的数据片交换对象集合。

[0077] 第三步：数据片解码重构：原始数据在经过分片编码和交换传输阶段之后，最终汇聚到服务提供商（服务器）。对于每条原始数据，服务器接收到至少 k 片数据之后就可以成功重构出原始数据。本步骤中为所有收到的数据片在内存空间维护一张数据表 (Cache table T)，作为重构算法的输入，具体步骤包括：

[0078] 3.1) 根据收到的加密数据片，采用非对称解密函数以及对应第一步中用户的私钥，对加密数据片进行解密，得到标识信息和编码后数据片；

[0079] 3.2) 将标识信息和编码后数据片加入数据片表中，并判断当属于同一条原始数据的编码后数据片至少达到 k 片时，则采用与第一步对应的纠删码解码技术重构出该原始数据＜t,l,d＞；

[0080] 3.3) 将属于该原始数据的编码后数据片从数据片表中删除，并保存所重构出来的原始数据信息＜t,l,d＞，直至完成所有加密信息片的解密，得到所有原始感知数据。

[0081] 与现有技术相比，本实施例所具有的技术性能的进步以及实验数据指标的提升表现在：首先，本实施例极好的保护了参与式感知系统参与者的隐私信息，达到 k-anonymity 的保护效果，其次，本实施例可良好的运行在移动终端设备之上，极大的增强了参与式感知系统的容错能力，同时，通过算法的设计和优化，有效的降低了移动设备的系统开销。

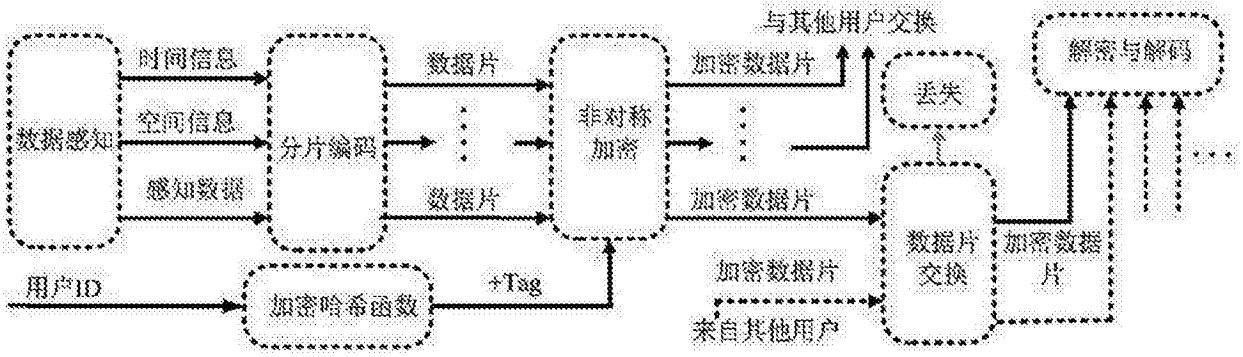

数据感知
时间信息
空间信息
感知数据
分片编码
数据片
数据片
非对称加密
与其他用户交换
加密数据片
加密数据片
丢失
解密与解码
数据片交换
加密数据片
用户ID
加密哈希函数
+Tag
加密数据片
来自其他用户

图 1

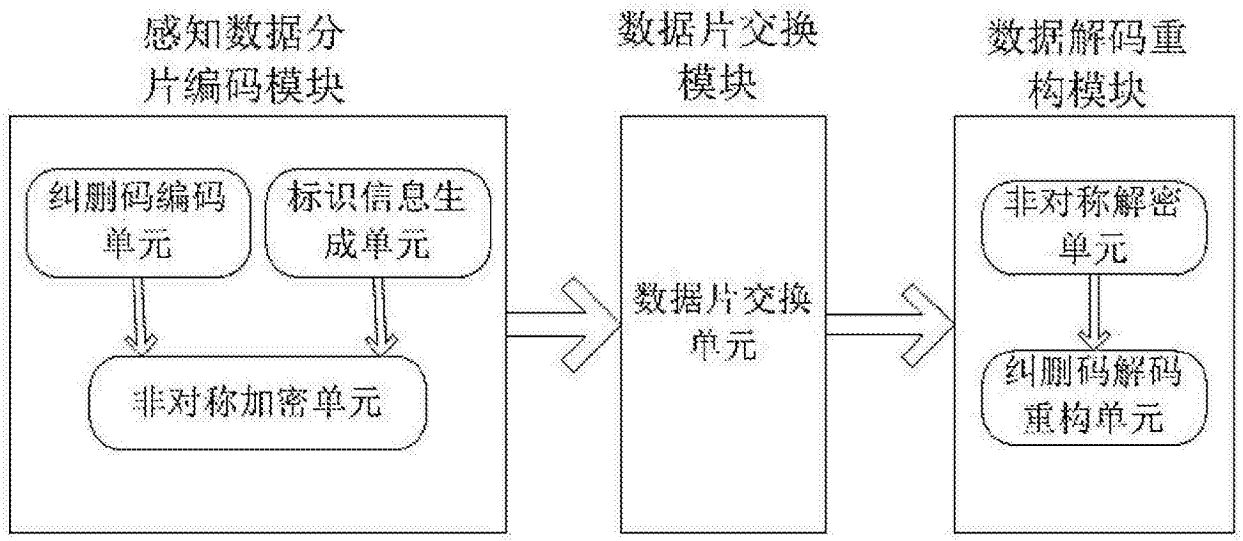

感知数据分片编码模块
数据片交换模块
数据解码重构模块
纠删码编码单元
标识信息生成单元
非对称加密单元
数据片交换单元
非对称解密单元
纠删码解码重构单元

图 2

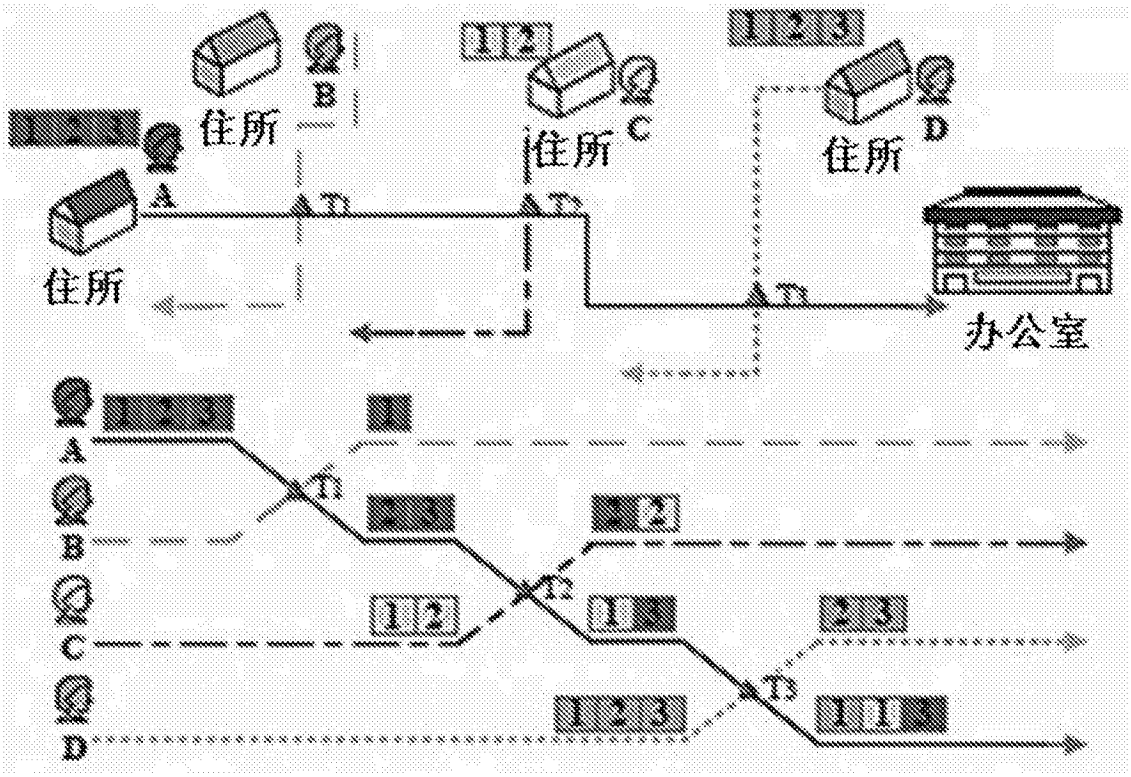


图 3