用户使用手册

**一. 文件格式**

关于文件格式，我们有两种轨迹文件，一种是只有3列的，一种是有4列的：3列的轨迹文件（actual.trace和exposed.trace）从左到右分别代表：用户戳、时间戳、位置戳；4列的轨迹文件（其他轨迹文件）从左到右分别代表：用户戳、时间戳、位置戳、暴露情况（0为未暴露，1为已暴露）

**PS：用户一定要设计好下面这4个范围参数，否则程序运行可能出错**

两种轨迹文件第一行均为4个范围参数：

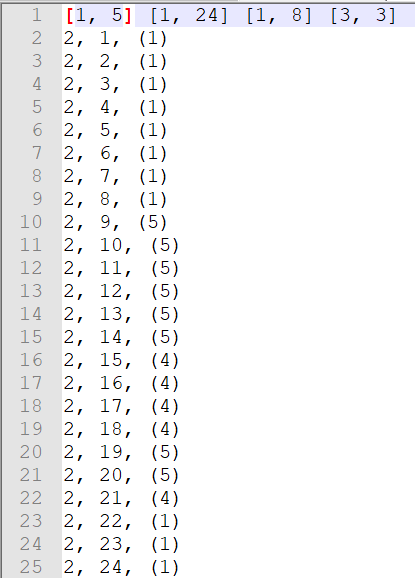
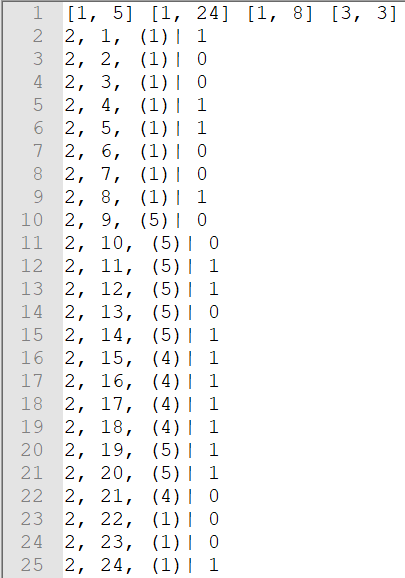
[最小用户戳，最大用户戳]，[最小时间戳，最大时间戳]，[最小位置戳，最大位置戳]，[区域行数，区域列数]

图1-1 图1-2

图1-1为3列的轨迹文件，图1-2为4列的轨迹文件

**二. 程序使用**

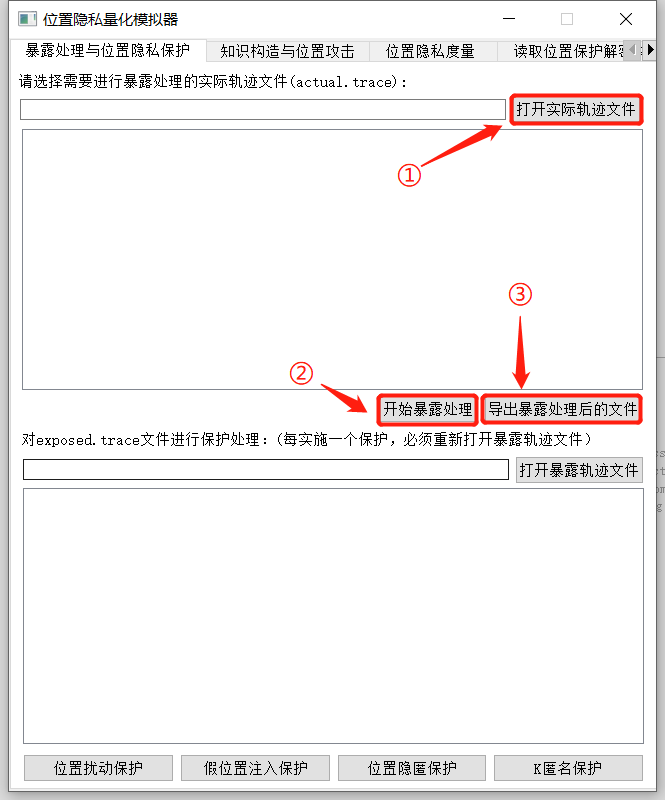
**暴露处理：**

1. 在相应选项卡，先点击“打开实际轨迹文件”按钮

2. 在弹出的窗口中，选择要打开的actual.trace

3. 然后点击“开始暴露处理”按钮，输入记录暴露比（即想要有百分之几的记录暴露），最后点击“导出暴露处理后的文件”按钮

4. 选择要暴露处理以后的数据要存放在哪里，点击确定即可完成



**图2-1**

**暴露处理操作如图所示**

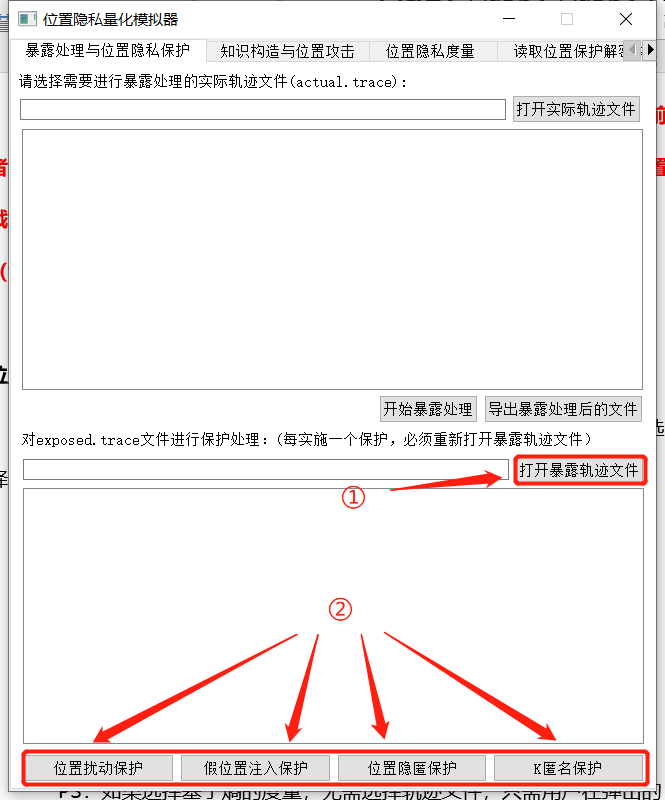
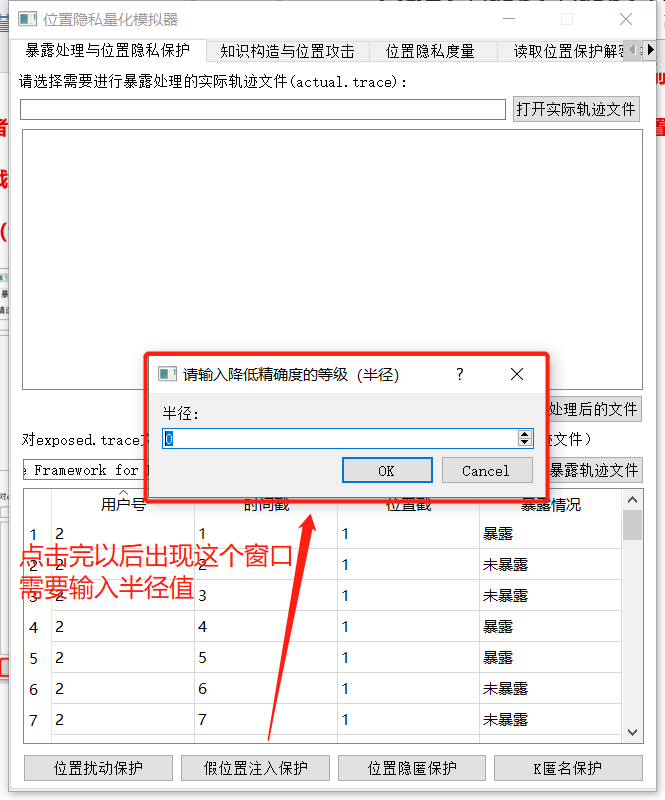
**位置隐私保护：**

1. 选择相应的选项卡，点击打开暴露轨迹文件

2. 在弹出的窗口中，选择所需要进行保护的exposed.trace

3. 然后界面下方有四个按钮，分别对应4种保护，点击即可

4. 四种保护均要求用户自己选择经过保护后的轨迹文件要存放的位置，以及密钥文件要存放的目录。

 **PS：其中，假位置注入保护和K匿名保护需要用户输入保护等级，前者的保护等级r表示假位置可以 从多大的范围选取，这个等级就是以原来位置戳为原点与周围距离为r的矩阵，后者的等级则表示一共需要有多少条记录（包括原纪录）**

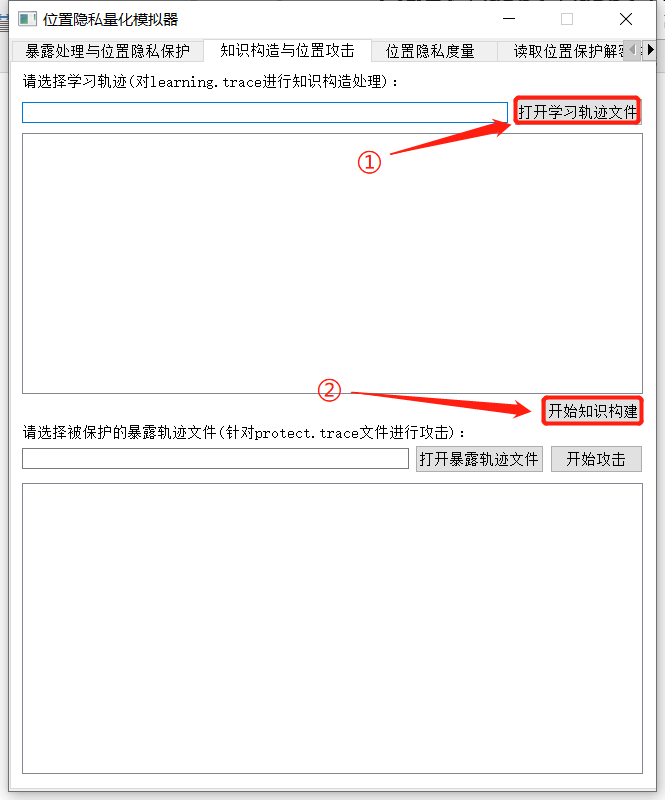
**图2-3 图2-4**

图2-3为位置隐私保护的操作步骤，图2-4为假位置注入保护和K匿名保护需要填写等级的窗口

**知识构造与位置攻击：**

1. 首先进行知识构造，打开学习轨迹文件learning.trace

2. 然后点击开始构造，程序会弹两次窗口，第一次弹窗要求用户选择Knowledge文件即转移概率矩阵需要存放的位置，第二次弹窗要求用户选择PointProbability文件要存放的位置（攻击时需要用到这两个文件）

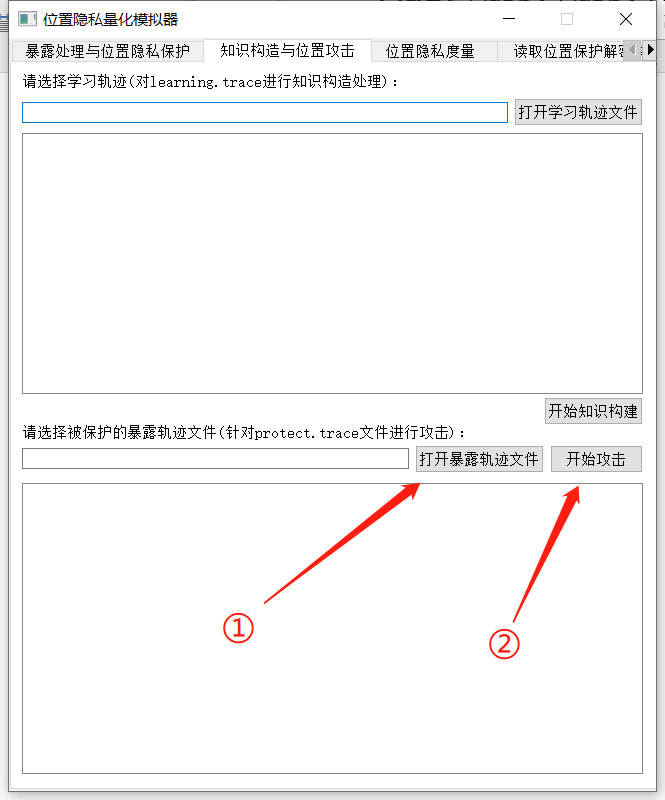


**图2-5**

图2-5为知识构造所需要的步骤

3. 对于攻击操作，首先打开暴露轨迹文件

4. 然后点击开始攻击，之后会三次弹窗，第一次弹窗要求用户选择Knowledge文件，第二次弹窗要求用户选择PointProbability文件，第三次弹窗是让用户选择攻击生成的attack.trace轨迹文件要存放在哪里（度量要用到）



**图2-6**

图2-6为攻击操作需要进行的操作步骤

**位置隐私度量：**

1. 选择相应选项卡，点击“打开实际轨迹文件”，并从弹出窗口中选择actual.trace

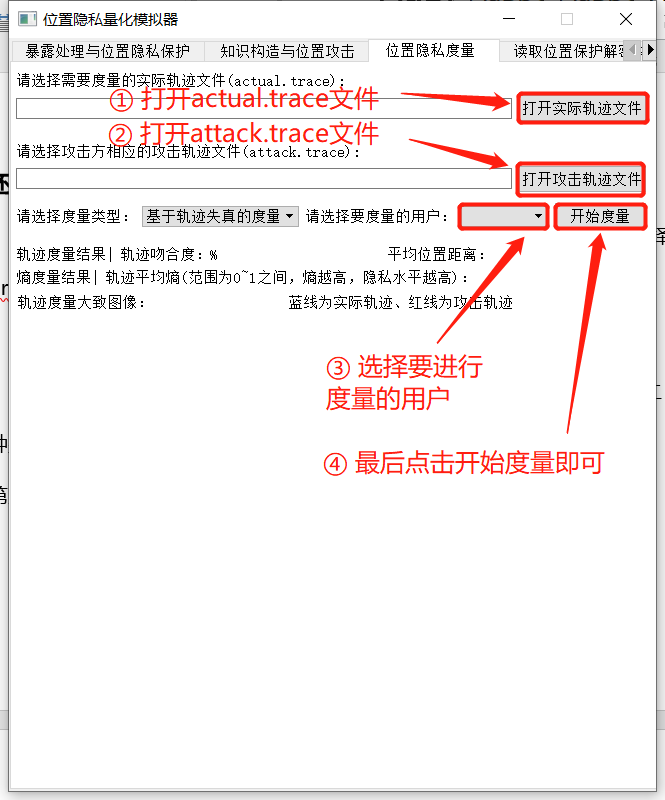
2. 点击“打开攻击轨迹文件”，选择要打开的attack.trace

3. 在左侧的下拉框出选择要进行度量的类型

4. 在右侧的下拉框选择要进行度量轨迹的用户

5. 点击开始度量即可

**PS：如果选择基于熵的度量，无需选择轨迹文件，只需用户在弹出的窗口中选择攻击方的先验知识文件Knowledge**



**图2-7**

图2-7描述了度量所需要的操作

**还原轨迹部分：**

1. 选择相应选项卡，点击“打开被保护轨迹文件”，并从弹出窗口中选择protect.trace

2. 在下拉框出，选择要打开的密钥类型：

密钥类型有3种，第一种是key，用来解密位置扰动所保护的轨迹，第二种是TruePostion，用来解密假位置注入保护和位置隐匿保护锁生成的轨迹，第三种是Kmap，用来解密K匿名保护所生成的轨迹

**PS：请务必选择正确的文件类型，再点击打开位置密钥文件，确保你所打开的文件类型和下拉框所选择的类型对应**

3. 点击相应的还原轨迹的方式，会弹出一个窗口，让用户选择要存放的还原轨迹的位置，选择好后点击确定即可



**图2-8**

图2-8位还原轨迹需要进行的操作