**基于动态空间查询的高级位置呼叫服务软件**

1. 软件背景

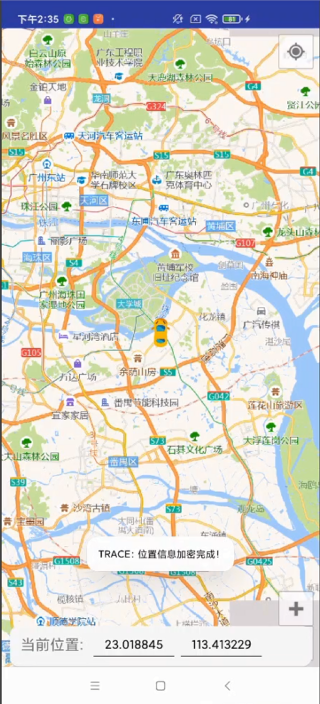
目前，有很多打车软件，比如“滴滴打车”，在后台不断收集用户位置和轨迹，以及隐私偏好数据，其运营公司贩卖这些隐私数据牟利，造成用户和司机位置/轨迹等相关隐私泄露，甚至有可能威胁到用户的生命，财产安全。因此，需要开发能够保护用户隐私安全的打车软件和算法，在不影响可用性的同时，保护用户隐私。

二．软件介绍

本软件用Java语言开发，应用于交通、隐私保护等领域，具有用户登录、乘客发布打车请求、司机接单、抵抗抗协同多采集终端信息关联导致的隐私泄露、抵抗孤立代理间导致的隐私泄露、抵抗多云端应用关联导致的隐私泄露等功能。

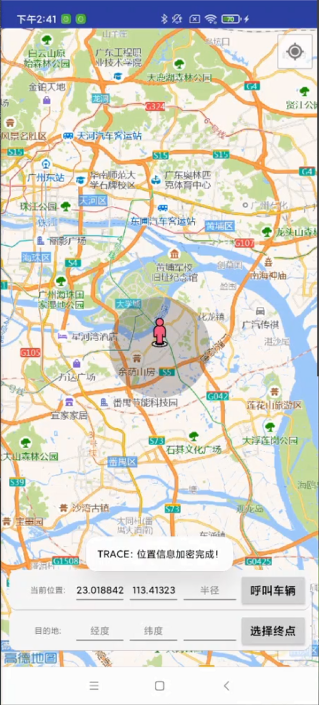
1、司机登录

打开移动端App，选择司机身份，输入账号密码，登录成功；



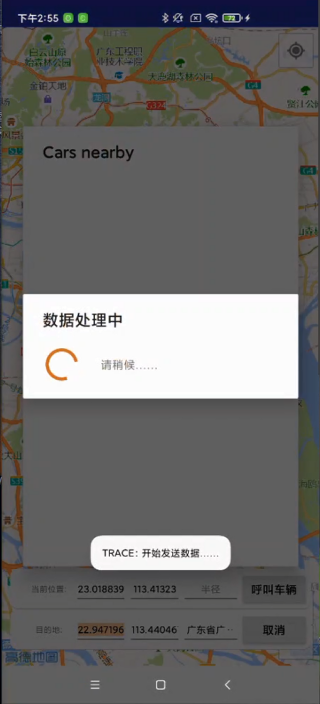
2、乘客登录

打开移动端App，选择乘客身份，输入账号密码，登录成功；



3、乘客发布打车请求

1）乘客在乘客地图界面上手动点击一个点或者手动输入坐标，然后点击pick按钮，点击呼叫车辆按钮发布乘车请求，搜索司机，App界面显示正在处理数据；

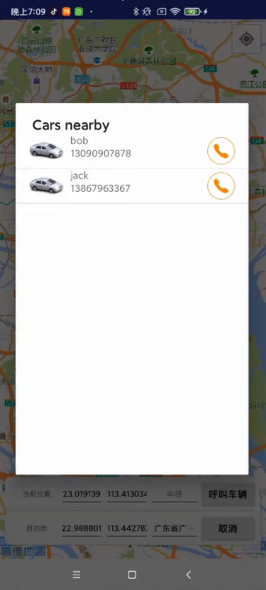


2）匹配到司机移动端App上显示是否接单选择，乘客发布打车请求功能完成。



4、司机接单

1）司机选择接单后，乘客可在界面看到选择接单的司机名称和电话，乘客选择目的司机，在移动端app可看到司机位置信息；

2）乘客选择司机后，目的司机在移动端app可看到乘客位置信息；



三．软件特点

首先，软件为叫车服务提供了一个保护隐私的动态空间，保护消费者和车辆的准确位置，以及服务商的空间划分信息。具体来说，在被发送之前，所有的与位置相关的数据被转换成加密文本，并且在计算过程中没有解密。因此，消费者、车辆、和网约车服务器无法获取对方的敏感信息。此外，即使攻击者可以窃听在用户和服务器之间传输的所有数据包，他们无法获得可用信息。其次，软件实现了精确的空间查询。基于四叉树数据结构和轻量级多方随机掩蔽技术，我们构建了一个快速安全的子区域查询 (FSSQ) 算法，它允许供应商找到车辆所在的子区域，或客户上车/下车点，同时保护用户的位置和叫车服务器的空间分割隐私。同时，基于 FSSQ，一种高效且安全的车辆查询 (ESVQ) 算法允许消费者在上车点附近准确搜索车辆而不泄漏准确的消费者和车辆的位置数据。第三，软件计算效率高，基于加法和乘法的隐私保护空间查询方案。运用四叉树数据结构，空间查询的时间大大减少。

在我们的系统模型中，我们主要关注如何为用户和服务提供商提供准确高效的隐私保护叫车服务。每个用户，例如消费者或司机，配备智能手机，可以与服务器连接，实现网约车服务。具体来说，如上所述，我们的系统由三个部分：1）网约车服务器（RS）；2) 注册消费者 (RC) 3) 注册车辆 (RV)。 RS 是网约车服务商的服务器，主要执行三个功能： a) 实时检测分布乘车行为和注册的密度，b) 前向车辆查询和叫车在用户之间的请求/响应，以及 c) 提供调度车辆信息。 RC 是在 RS 中注册的客户。基于叫车应用，RC可以选择她/他想要的地图上上车/下车地点，并发送用车请求到 RS。RV 是已在 RS 注册的车辆。在叫车服务过程中，RV负责提交它定期向 RS 屏蔽的位置信息，用于 RS 的动态子区域查询。RV 还可以接收RS发来的调度信息。

软件可以保护乘客和司机的位置隐私。保护司机和RV的位置隐私，以及RS的空间视觉信息在服务提供者中至关重要。在我们的安全模型中，我们认为RS是可信的，但又是贪婪的，RC/RV是诚实但好奇的。特别是，RS诚实地削减了加密文本上的操作，并可靠地转发叫车请求和响应，但它对RC的管理和RV的位置信息很好奇。RC和RV不需要发送虚假信息，但RC试图通过叫车响应分析准确的位置，RV希望通过叫车请求获得RC的位置或接收点。此外，在空间查询过程中，RC和RV都希望获得RS的空间划分信息。此外，攻击者可能会篡改和伪造数据，或伪装成合法用户以访问服务。考虑到上述安全问题，软件可以满足以下安全需求：

隐私性：保护用户的位置信息不受RS和其他用户的影响，即在叫车服务期间，RC的接客/下车点应对RS和未使用的 RV保密。并且RV的准确位置不能泄露给RS和RC。也就是说，即使 RS 可以得到所有来自 RC 和 RV 的叫车请求和响应，它只能检测RV 和RC 的接送点的大致区域，而不是准确地点。

机密性：确保 RS 叫车服务期间的敏感数据安全。为了获取RV的密度和乘车行为的分布，RS需要将一个区域划分为多个子区域，并通过收集和分析用户的位置数据优化连续地空间划分。空间划分会泄露具有经济意义的商业秘密，因此，在空间查询过程中，空间划分信息不能泄露。

身份验证：验证加密的叫车请求和响应确实是由合法用户发送的，而不是在传输过程中被修改的，即如果非法用户伪装合法 RV 以窃取 RC 的取车点数据，软件要能够防止恶意操作。此外，所有在 RC、RV 和 RS 之间传输的数据包应进行身份验证，以便用户可以访问真实的和可靠的叫车服务。

软件实现了三个设计目标：

1. 保证安全和隐私保护：如果不考虑安全问题，用户和服务提供者的敏感信息可能会被披露，导致严重的后果。软件可以同时实现保密和认证。
2. 实现动态空间查询结果的准确性：用户经验安全机制提出的一个关键方面。在我们的系统中，动态空间查询是直接影响用户体验的基本功能。因此，查询精度不能在保护隐私的同时降
3. 计算复杂度低：虽然智能手机的性能是在不断改进，但是电池仍然有限。而且，考虑到具有实时性要求的网约车服务和海量用户，软件考虑到了在计算和交互过程中网约车服务器和智能手机能量消耗的控制。