#### 设计（论文）的主要任务及目标

以智能手机、可穿戴设备为代表的移动便携式智能设备的普及，给一些以前极难处理的信息采集任务带来了极大的便利即群智感应系统。如智能交通、环境监测等需要大范围采集数据的任务，利用人群携带的智能设备中的传感器，在处理中心的协调下，可以快捷高效的完成。但由于现实环境中一些不利因素的存在，给群智感应系统的有效运作带来了困难，其中，群智系统中节点隐私信息的保护就是一项必须要克服的困难。当群智系统在采集信息到信息时，在反馈给处理中心时，往往需要附带上一些诸如节点所在位置、时间、节点标识等必要的但设计节点隐私的信息。这就带来了数据在传输和处理过程中可能泄露节点隐私信息的可能。这些信息一旦被恶意利用，则可能造成严重的后果。因此，在群智感应系统中，对节点隐私信息的保护是必不可少的任务之一。本次毕业设计的主要任务就是针对群智系统中的节点隐私信息的保护提出具体的设计以实现保护节点隐私及探测并排除恶意节点的目标。

1. **设计（论文）的主要内容：**

首先提出一个具体的群智感应系统模型，并在此模型中模拟实际的群智感应系统的运作。在此模拟的群智感应系统中设计一套完整的可以保护节点信息的数据加密和路由系统以确保节点的隐私信息不泄露。此设计中使用的模拟环境是道路信息的手机系统，在该系统中，有许多参与采集任务的节点。由于节点具有随机移动性，所以模拟中使用节点主动提出申请和主动传输数据的方式。节点采集到的信息首先并不上传，当其经过一个认为是安全的位置时，将数据交给此处的路由节点。而数据的加密方式，在节点加入系统时，直接与处理中心约定，每个节点都有自己的标识和与其他大多数节点不同的加密方式以防止信息泄露。并且还有为了防止信息被篡改而影响数据采集的有效性的处理机制，即当信息被篡改时，在保证信息未泄露的情况的，能快速探测出篡改信息的恶意节点并将其永久排除出系统。在采集完成后，处理中心在发布任务结果前还要做一些处理，将涉及特定节点的信息隐藏，而只发布那些有用的，但不涉及具体节点的数据。

1. **设计（论文）的基本要求：**

有效性：此设计必须能满足保护节点隐私信息不泄露的最低要求，并且能发现和排除系统中篡改路由信息的恶意节点。

效率性：在满足有效性的条件下，应尽减少对节点资源的占用，通过合适的方法，减少加密解密的数据处理量，缩短路由路径的长度。

1. **主要参考文献：**
2. 金晨辉；郑浩然；张少武；胡斌；史建红；《密码学》
3. 王钲琪；《科技导报》-移动群智感知网络发展面临的挑战
4. 宋乐；《加密技术下的学习安全保障》
5. 王涛春；刘婷婷；刘申；何国栋；《群智感知中的参与者信誉评估方案》
6. **进度安排：**

|  |  |
| --- | --- |
| 相关资料收集 | 1.15-1.28 |
| 需求分析 | 1.29-2.12 |
| 系统设计 | 2.19-2.25 |
| 模拟环境搭建 | 2.26-3.18 |
| 任务分发系统搭建 | 3.25-4.8 |
| 加密传输系统搭建 | 4.9-4.23 |
| 系统有效性和可用性测试 | 4.24-4.29 |
| 论文 | 4.30-5.6 |