网络系的两个专业方向的选课打通，同学们可以选任一开课的网络工程系的老师。小学期的课程设计的内容和具体题目一般是在第一次上课，教师与学生讨论过后确定。现已有部分老师列出了题目，共同学们选课参考。
小学期期间，可以申请使用物联网实验箱等实验设备。

覃振权

联邦学习中的通信与数据压缩技术

作为一种前沿新兴技术，联邦学习为我们解决大数据时代“数据孤岛”问题提供了一种新的兼顾数据隐私保护和数据协同计算的方法，但与其他机器学习技术（如深度学习、强化学习等）相比仍不够成熟，还有待进一步研究推动。

在联邦学习的典型训练过程中各个参与方需要把加密数据等信息传输到中央服务器进行联合训练，也就是用分布在大量客户端上的训练数据来训练高质量的集中模型，这样不仅需要很大的通信成本，而且每个客户端的网络连接都不可靠且相对较慢。因此，数据传输与通信可能会成为联邦学习的主要发展瓶颈。目前，对于网络通信连接这个研究方向，很多学者开始对如何降低联邦学习中的通信成本（如网络带宽等）进行了探讨。但是问题在于，我们能否在此基础上降低更多通信成本，或者采用这些降低通信成本的方法是否可以保证联邦学习的准确性，如果无法保证模型的准确性，那么只单纯降低通信成本没有意义。

小学期目标：

（1） 按照给定的文档搭建联邦学习仿真环境，分析代码结构，并能够围绕通信效率进行优化。
（2） 阅读指定的论文，并据此查重其他相关文献，围绕通信效率设计优化算法。

郭成

题目 1：基于垂直分割数据的纵向联邦学习方案设计
要求：对于分布在少量大型数据机构间拥有不同属性的数据，设计一种高效的联邦学习方案，可以在不泄露隐私并且保证模型准确度的情况下实现跨数据机构的联合训练。在此种场景下，数据集体量大，参与节点个数少，网络情况良好，且均拥有较高算力。

题目 2：基于水平分割数据的海量节点高效横向联邦学习方案设计
要求：对于分布在众多数据节点间拥有相同属性的数据，设计一种高效的联邦学习方案，可以在不泄露隐私并且保证模型准确度的情况下实现跨海量数据节点间的联合训练。在此种场景下，单一数据源数据量小，数据来源多，网络不稳定，且数据节点计算能力弱。

题目 3：BS 架构下的智能人脸识别系统设计
要求：设计相应的 web 程序，在视频监控场景下，通过计算机视觉技术，对画面中出现的特定人物进行识别，发现检测目标后，在前端页面显示实时画面以及人物的详细信息（未发现人物则显示固定背景），支持多摄像头。

题目 4：视频监控场景下的异常动作检测
要求：通过传统计算机视觉或者深度学习技术，及时发现视频画面中的异常行为（如激

烈打斗，大幅度的异常动作，疑似破坏，下蹲以及倒地等等）并进行报警，可自行设置 2 到 3 项检测目标以及相应的检测标准。若使用深度学习算法，可借助百度 AI Studio 平台完成。检测程序应该尽可能降低误报率，即报警内容均具有高度的可信性。

孙伟峰

1. 工业互联网中 EdgeAI 调研、设计及性能评测
边缘计算中需要边缘智能，以边缘智能在数据处理、调度、任务卸载等方面的应用和改进为对象，做方案的设计及评价。一些具体的题目可以为：“工业互联网数据智能处理、存储及表示”、“基于学习的 5G 基站部署及节能控制模拟”、“面向异构边缘网络的联邦学习优化及性能比较”
2. 分布式存储一致性及安全
在分布式环境下，如何保证安全，关键词包括区块链、联邦学习、入侵检测等。具体的题目可以为：“”基于区块链和联邦学习的风险自适应访问控制方案”、“基于神经网络的入侵检测方案设计及测试”、“轻量级不解密计算在数据库中的实现”
3.具体的动手模拟或实现
面向一些应用，做方案的模拟，用到 EdgeCloudsim，NS-3 等模拟器。可能的题目可以为“基于 EdgeCloudsim 的***方案模拟比较”、“基于 NS-3 的多层并行传输性能模拟”、“基于大量公交信息的用户画像及预测系统设计及实现”

万良田

集群无人机在作战系统中具有如下优势：数量多且覆盖范围广，具备较强态势感知、压制和摧毁敌方防空系统能力；抗毁能力强，部分无人机损失后，集群无人机仍可完成任务；单架无人机的成本远低于传统防空导弹，可增加敌方防御成本；作战灵活性强，可与多种飞机和武器协同。随着机动组网、编队控制、自主协同等关键技术不断突破，集群无人机将逐步具备对地、对海、对空侦察甚至攻击能力，将对未来航空装备体系构成和作战样式产生重大影响[3]。2018 年 8 月，美国防部发布《2017-2042 财年无人系统综合路线图》中，“集群能力”被列为无人系统的 15 项关键技术之一。国内外已经或计划开展飞行验证的集群无人机平台，按美国防部的划分标准属于 1-3 等级无人机（分别对应：重 0-9、9.5-25、小于 600 千克，飞行高度小于 370、1100、5500 米，空速小于 185、463、463 千米／时），综合通信、导航、控制众多学科新技术。例如：中国电子科技集团公司开展 119 架集群无

人机编队飞行试验（如图 1 所示）和美国国防部战略能力办公室开展 103 架“灰山鹑”集群无人机试验（如图 2 所示）等。

图 1 中国电子科技集团公司蜂集群无人机实验

图 2 美国“灰山鹑”集群无人机试验

传统敌方目标信号分选识别技术缺陷

敌方信号分选识别是集群无人机侦察干扰一体化的关键步骤，高效可靠的分选技术是侦察系统信息处理分析的前提和保障。现代战争具有形式多样化的特点，战场电磁环境变得越来越复杂，在时域和频域上，雷达信号的交叠现象越来越频繁，集群无人机对敌方雷达信号的分选分析越来越困难。同时，电子反侦察技术不断发展，雷达参数多变，体制复杂化也给集群无人机雷达信号分选系统带来极大的挑战，信号分选中的虚警、漏警等问题直接关系到了侦察系统的可用和有效性[6]。常见的雷达侦察系统主要提取脉冲信号的脉冲描述字，单个辐射源的到达角（DOA）、脉宽（PW）和载频（RF）信息以一定的规律波动，对不同的辐射源具有较好的区分度。集群无人机利用机器学习中的聚类算法，对 DOA、PW 和 RF 参数进行聚类处理达到稀释脉冲流的效果，最后通过对稀释后的脉冲流进行解交织处理，分离各参数较相近的辐射源，以此实现雷达信号的分选识别，采用多门限模糊聚类算法对 4 部雷达信号进行分选，结果如图 5 和图 6 所示。

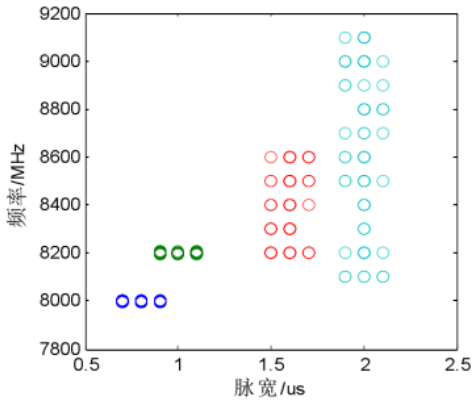

图 5 多门限模糊聚类

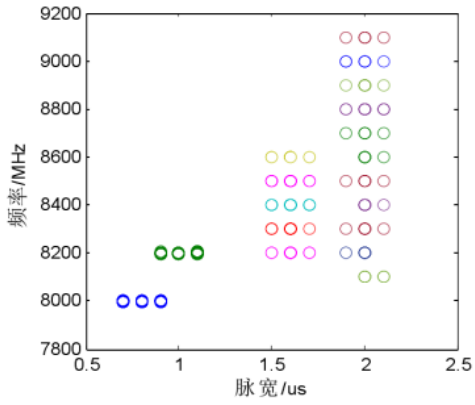

图 6 传统模糊聚类

现阶段对低信噪比、复合调制目标信号的分选识别已经成为制约敌方目标信号分选的瓶颈问题。很多学者提出了基于敌方雷达信号多参数联合分选的深度学习分选算法，深度学习算法相比于传统算法，具有自学习、自适应的优点，可拟合复杂线性关系，具有很强的综合信息能力，且鲁棒性和容错性强，在雷达信号分选上取得了很好的成果。然而**目前的深度学习算法都是基于单个无人机接收数据进行敌方雷达目标的分选识别，无法发挥集群无人机的“群智”以及大覆盖范围的优势，无法充分学习提取侦察区域的敌方目标以及环境信息。**

具体研究内容：

集群无人机数量多、覆盖范围广，传统基于单个无人机的敌方目标分选算法仅仅通过简单的信息融合难以充分利用集群无人机的数量优势。同时无法利用集群无人机覆盖的其他侦察区域的敌方目标以及环境信息来提升目标区域敌方目标的分选识别准确率。上述问题已成为深度学习提升集群无人机对敌方目标分选和识别的瓶颈问题。

针对低信噪比下传统信号分选算法性能下降的问题，研究基于深度迁移学习的雷达信号分选识别算法，在一定覆盖范围内，将其他区域已训练好的模型迁移到目标域，提升对重要目标的分选识别精度。

前期工作：前段时间硕士同学已经把 FRCNN 算法用于雷达信号的分选，并且取得了较好的性能，但是这是基于单个无人机接收数据来做的，没有利用集群无人机数量上和覆盖范围广的优势。

本课程设计需要大家掌握迁移学习的基本原则以及算法，并将其应用到雷达信号的分选中，利用其他区域集群无人机接收的数据来训练模型，将训练好的模型应用到当前区域以提高当前区域的信号分选准确率。这里要注意其他区域的数据不能与当前区域的数据相同或者类似，要利用从其他区域学习到的特征，提高当前区域的精度。

赵亮

有两个主题：1. 医学数据分析，包括肺部和脑部影像数据分割、融合、疾病预测，感染性疾病病理数据分析。2. 跨模态生成，包括文本到图片生成，语音到图片生成等。用到的主要技术理论包括深度学习，数据融合。