# 会议纪要

**会议主题：**Federated Learning-based Cross-layer Security Design for Satellite Networks（基于联邦学习的卫星网络跨层安全设计）

**会议时间：**2024年8月19日19：00至20：20

**会议地点：**西安电子科技大学北校区会议中心303-1会议室

**线下人员：**尹志胜 孙瑞锦 贺靖超 王葳 沈京龙 王秀程 马龙飞 张玉洁 黄蕾 权赟昊 胡陆莹 齐阁 侯毓真 邓川 李青壮 孙兴栋 方忠盛 贾昊燏 张智杰 解思舀 孙路路 郑佩林 郭译凡 许嘉洁 王天宇 陈梦豪 韩松明 尉家豪 王天宇 刘苏 杨双宇

**线上人员：**承楠 王兆薇 邱子仪 尚佳瑶 万佳林 于凡迪 祝馨平

**记 录 人：**王兆薇

**会议内容：**刘永红汇报 Federated Learning-based Cross-layer Security Design for Satellite Networks

**Page 3:**

* **承楠：Satellite Air Ground这个名词是不是有问题，应该是Space-Air-Ground，使用名词要严谨。从这一页关于空天地的介绍中获取不了多少信息量，给出的三点内容、图示以及讲的内容信息量不够大，与论文的核心研究内容关联度不够。**

**Page 4:**

* **承楠：左边的图Party A B C之间是什么关系？**
* **刘永红：等价关系**
* **承楠：图从上往下一般是云边端，这种画法容易让人费解，造成误解。Party在联邦学习里是比较常用的吗？**
* **沈京龙：party也常用，一般是server和client。**

**Page 5：**

* **承楠：你的左边的security risks in federated learning和右边的physical layer security之间是什么关系？中间的逻辑是怎么过渡的？**
* **刘永红：左边提出来需要考虑FL传输中要考虑安全问题，如窃听泄露等，右边是实现安全传输可能用到的物理层安全方法，避免窃听泄露等问题。通过资源分配和波束赋形进一步引入后面实际解决安全问题用的方法。**
* **承楠：右边的第二句话应该找与第一句相并列的内容，比如PLS还能干什么。**

**Page 6:**

* **刘永红**：**我的工作是针对分布式和FL架构的问题，分布式结构符合联邦学习的过程，联邦学习可以进一步加强隐私性，这两个是非常适配的。由隐私性提出FL模型传输过程中存在泄露的安全传输问题，所以想用PLS解决。进一步想到传输过程和联邦学习性能的关系。**
* **承楠：考虑一下Physical Layer Security Transmission是否合适，有语病存在。另外，为什么要研究第三点accuracy与transmission之间的关系，这个研究是返回去促进第二个研究内容的提升呢还是就结束了？**
* **刘永红：从第三个研究可以证明我们PLS与FL研究的有效性，相当于仿真的内容。**
* **承楠：Problem部分第一句同样有病句。并且前后两句有什么逻辑关系吗，是否可以串起来？一句话说不清楚可以按点来写。而且problem并不一定是越general越好，不能清晰表现出要表现什么问题，要再提炼一下。**

**Page 10:**

* **承楠**：**这一行描述，想体现的内容用加粗/红色来强调。**

**Page 11:**

* **承楠：这个neural network是放到什么地方来执行的？输入输出是什么？窃听者信道可以已知吗？**
* **刘永红：输入是信道状态，输出是波束赋形。**
* **尹志胜：上行传输，是在卫星上执行的，卫星相当于FL的server。讲的时候要结合卫星的场景把联邦学习的应用、安全威胁讲清楚。承老师的意思是要有一个宏观的架构，讲清解决的问题是什么，怎么做的。**

**Page 12:**

* **承楠**：**constraint equivalence replacement是新提出来的东西吗？为什么要这样替换？**
* **刘永红：将约束进行等效，就不用考虑惩罚因子了。**
* **王秀程：这个就是一个简单的投影。这种线性的约束方法在其他人的研究中使用过，但是这篇论文的约束没有人这样处理过。**

**Page 13:**

* **承楠：这部分PLS与model parameter是什么关系？**
* **刘永红：这一部分主要是将物理层安全与联邦学习的性能进行串联。**
* **尹志胜：我们是要探索确保联邦学习的模型参数传输过程的安全性之外，还要保证联邦学习本身的一个准确性不受或者仅受很小的损失。这部分要在background中讲清楚。因为PLS本身是对信号的处理，就会对模型参数的传输方式进行了干预，显然FL的性能会受到影响。**
* **刘永红：联邦学习的上传过程不是完全理想的，所以要去探索物理层安全的手段对传输过程的干预会怎么样影响模型参数，因为这个参数直接关系到FL的性能。但是PLS只能得到一个属于信号层面的SINR的值，不能直接对数据进行处理。所以利用SINR和BER的关系将信道层面等效到数据层面的误码率。因为模型参数本身是一个十进制的，但是上传下发使用的是二进制的。所以先将模型参数转到二进制，再以二进制的模型参数的误码的概率去进行掩码的判定。再将处理过的模型参数转回到十进制中，再去进行聚合。**
* **尹志胜：针对FL的研究，主要工作集中于提升模型训练的精度，都假设模型的参数的上传和下发都是准确恢复的，但是实际通信中是受到无线信道传输影响的，且考虑PLS的信号处理，一定会对FL的精度造成影响。那么我们工作就是评估SINR与FL可靠性的关系。**
* **承楠：传输性能与参数的对应这种方式是否可以做？**
* **尹志胜：这里没有编码的东西，是用了一个等效的方法。实际上传肯定是有噪声产生误差的，这个误差是进行了等效的而非实际设计了一个通信系统。这个等效是根据BER反推到信噪比，再通过信噪比确定要生成多大的噪声。**

**Page 14:**

* **承楠：Unsupervised learning method这个名字修改一下**