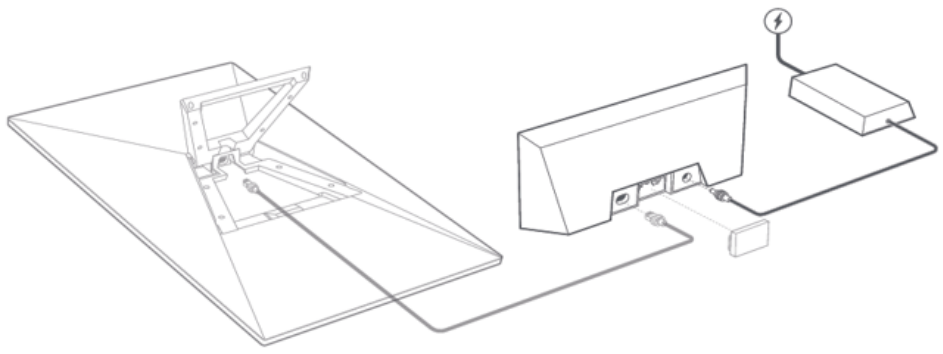
2025-03-27汇报

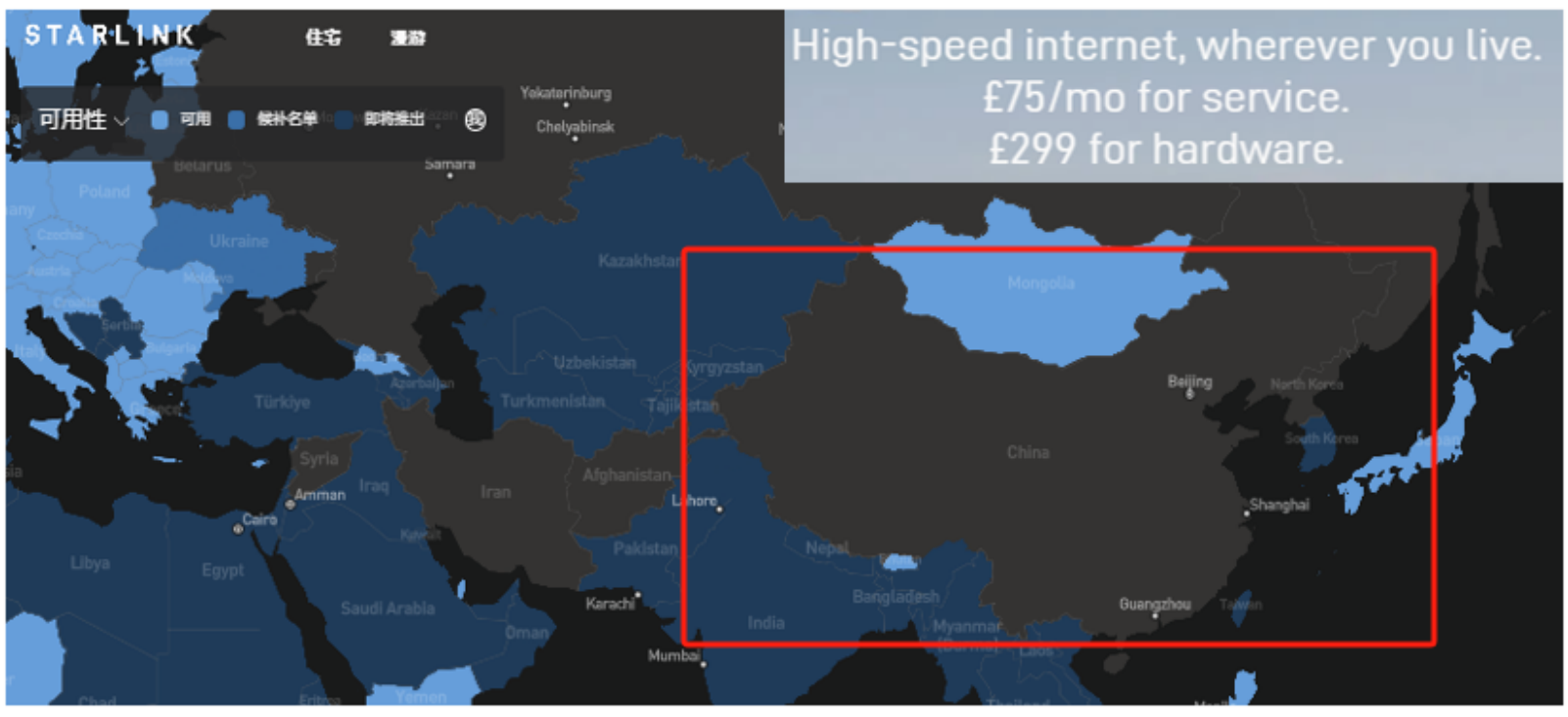
卫星通信系统=>如何接入

星链Starlink=>硬件连接示意



Starlink 4+
Engineered by SpaceX
SpaceX
#50 in Utilities
★★★★★ 4.9 • 57.7K Ratings
Free

国内暂时无法订购

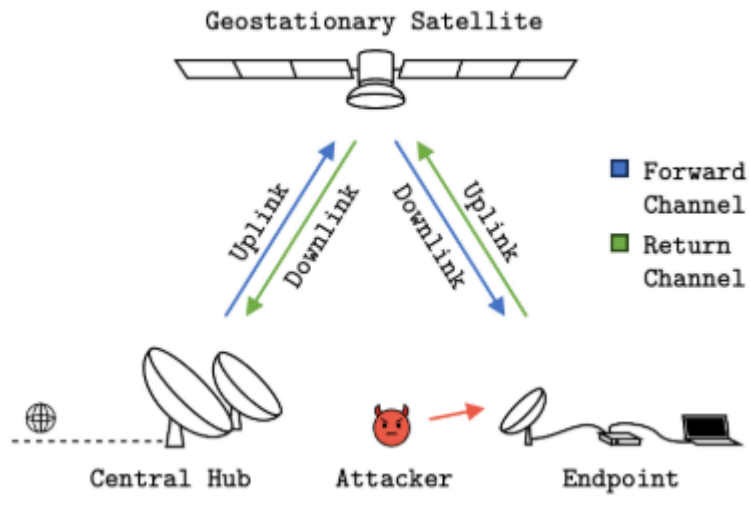


卫星通信协议栈典型代表=>CCSDS DVB-S2

特性	CCSDS	DVB-S2	Starlink[协议栈高度定制化]
适用场景	科学和政府航天/空间任务，强调可靠性和适应性，普通用户无法直接接收	商业广播和宽带通信，强调频谱效率和高数据速率	全球高速互联网接入
是否支持星间链路	包含支持星间链路的协议栈及射频特性	不支持，需定制化扩展	支持，基于IP的定制化动态路由，软件定义网络SDN
物理层	S/X/Ka波段，低阶调制	QPSK/8PSK/16APSK/32APSK，适应不同的信噪比环境	Ka/Ku波段，高阶调制

DVB-S2协议栈的卫星通信系统=>VSAT[VSAT_USENIX_2024] [海上VSAT_SP_2020]

- **中央集线器**——卫星与地面通信系统的中继器，配有大型蝶形天线(`天线系统`)，用于向卫星收发信号
- **卫星**——互通中央集线器与端点的数据，不执行任何数据处理/路由/身份验证，可定位在静止轨道GEO，中轨道MEO与低轨道LEO
- **端点**——与卫星通信，将接收的数据传达到接收方(下行链路)，或通过卫星传输数据至中央集线器(上行链路)



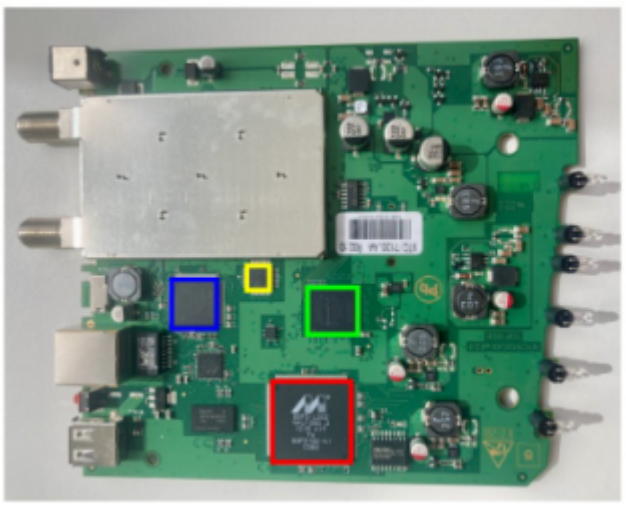
终端系统VSAT=>双向数据传输

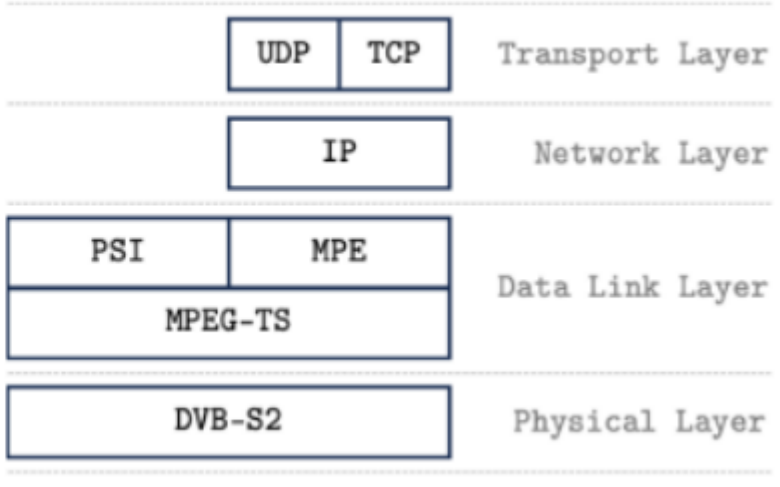
- **室外单元ODU** `射频前端` ——高增益碟形天线(向地球同步卫星发送和接收信号)、收发器
- **室内单元IDU**——室外机与用户网络之间的接口，包括**调制解调器** `固件` (调制输出信号进行传出、解调输入信号进行接收)、**网络接口** `网络协议` (以太网、WiFi等，连接用户本地网络)

DVB-S2协议栈的调制解调器与天线等硬件介绍

1. 调制解调器：Newtec MDM2200[Newtec MDM2200] [VSAT_USENIX_2024]

- **硬件架构**：
  - **信号处理模块**：包括FPGA、解调器、DAC等，负责将接收到的射频信号转换为数字信号。
  - **微控制器**：运行Linux操作系统，负责控制调制解调器的各项功能，如信号处理、配置更新等。
  - **网络接口**：支持以太网和WiFi，用于连接用户的本地网络。





协议栈：

- **物理层**：采用DVB-S2标准，支持多种调制方式(如QPSK、8PSK)和前向纠错(FEC)
- **数据链路层**：使用传输流(MPEG-TS)和多协议封装(MPE)进行数据封装和解封装；可能使用更新的**通用流封装(GSE)协议[海上VSAT_SP_2020]**
- **网络层**：支持IP over CCSDS，允许通过卫星链路传输IP数据包
- **传输层**：支持TCP和UDP协议，用于端到端的数据传输
- **应用层**：支持HTTP、FTP等应用层协议，用于具体的业务应用

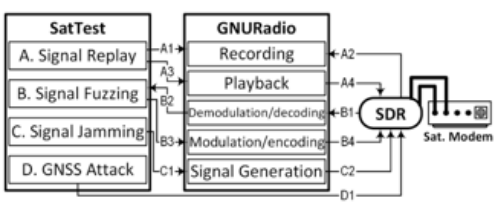
2. 蝶形天线

- **类型**：高增益定向天线，通常直径为0.75米到1米，支持C、Ku、Ka波段。
- **功能**：用于发射和接收卫星信号，确保与卫星之间的通信链路。
- **安装要求**：天线需要精确校准，确保指向卫星的方位角和仰角正确。

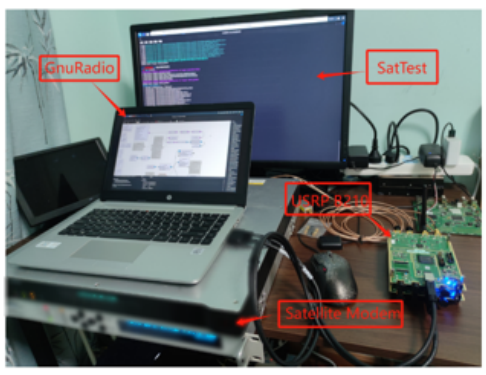
3. 接收/发射信号=>无线电设备 USRP B210=>大规模实验=>2500$ USRP B200=>小型研究=>1500$

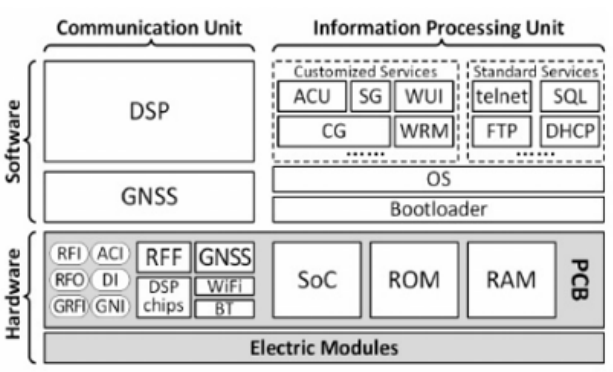
USRP B210 [Satellite Modems_CCS_2024]

- **卫星通信接口安全分析与测试工具**：AirSecAnalyzer
  - **SDR硬件**：USRP B210 与正在测试的卫星调制解调器通信，可将GNU Radio生成的**低频基带信号**转换为**射频信号**
  - **中间件GNU Radio**：作为软件数据生成工具SatTest与SDR之间的接口，接收SDR数据解调后传至SatTest；同时通过TCP接收测试数据调制后传至SDR
  - **SatTest**：四个典型测试：信号重放、信号模糊、信号干扰、GNSS攻击



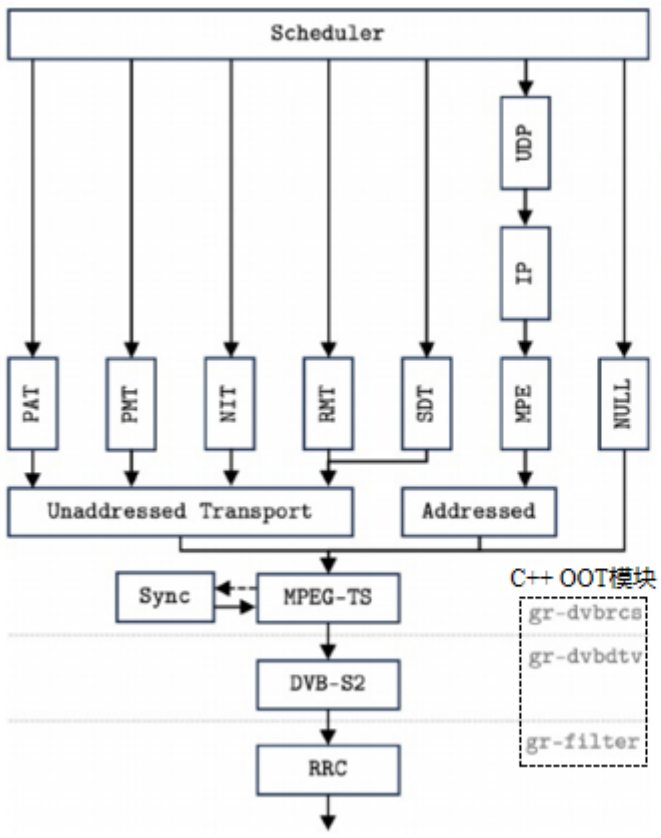
Make and Model	Net.	Deploy	Applications
Comtech *C1*	p2p	SA	mil, bc, aero
Comtech *C2, C3*	p2p	SA	mil bc aero, mari
UHP *U1, U2*	star/mesh	SA	mil bc
Intellian *Int*	star	int	mari, land
iDirect *i1, i2, i3*	star	SA	ent mil aero

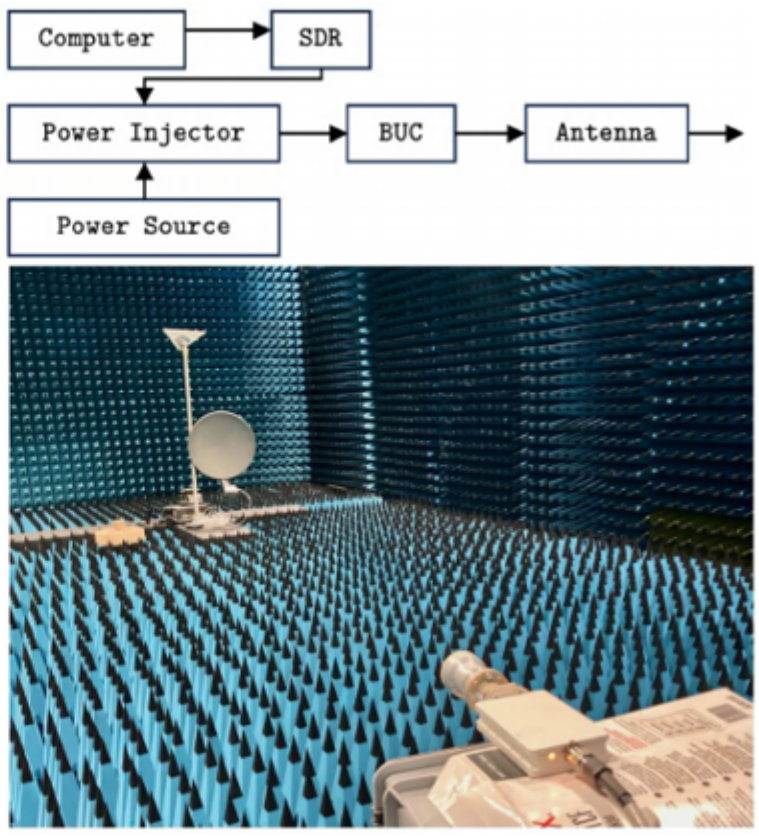




USRP B200/B200mini [VSAT_USENIX_2024]

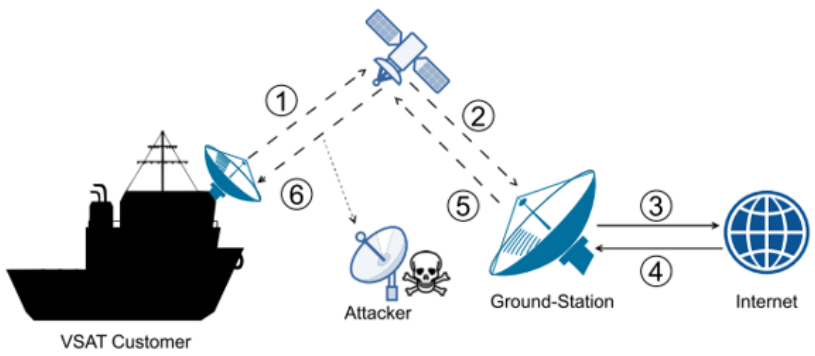
- **基于USRP B200的信号注入发射器**：复制真实的中央集线器传输
  - **gr-dvbrcs**：UDP、IP、DVB-RCS、MPE和MPEG-TS层，生成用于初始化调制解调器和发送攻击数据包的比特流
  - **gr-dvbdtv**：调制比特流，在开源框架**GNU Radio模块**中实现
  - **gr-filter**：信号处理，滤波以减少信号中码间干扰，提高信号质量



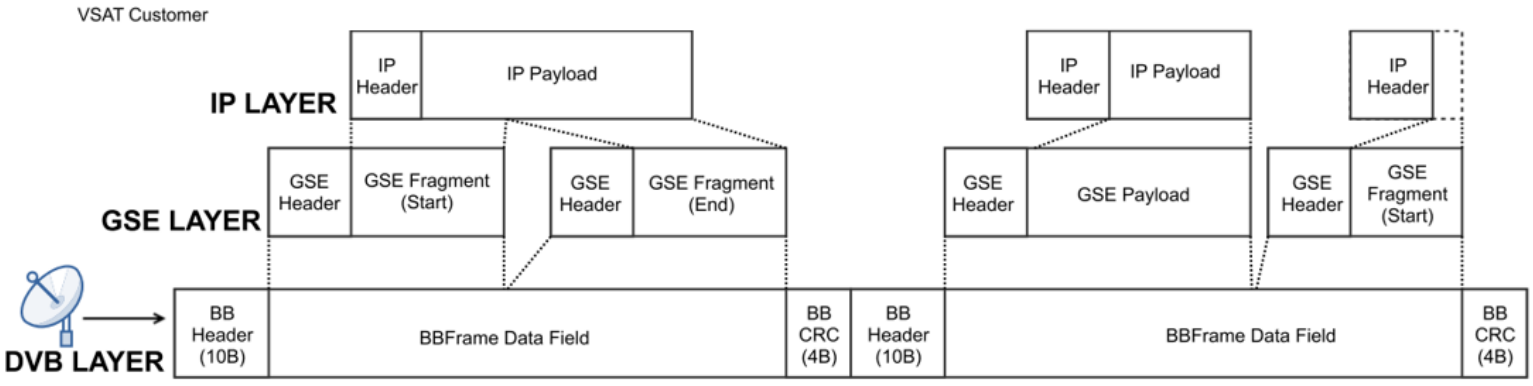


4.其他接入信号方式[海上VSAT_SP_2020]

- **设备组成**：考虑到专业设备造假昂贵，且不会直接出售给消费者(企业对接、通常以每月数千美元的年度合同形式)。使用标准的家庭电视卫星天线和廉价的业余卫星调制解调器，总价不过400$，虽存在定位不准确、无法保持可接受的吞吐量率，但仍能拦截、解调部分海上VSAT信号流，且可能包含敏感数据
- **数据提取和信号解释**：与以往VSAT的**MPE协议**不同，海上VSAT倾向更复杂的传输模式`16-32APSK调制`以及更新的**通用流封装协议GSE**，且无公开可用的软件用于接收与解调，因此开发了[GSExtract]，允许从原始GSE连续流中恢复任意IP数据包，实施被动攻击

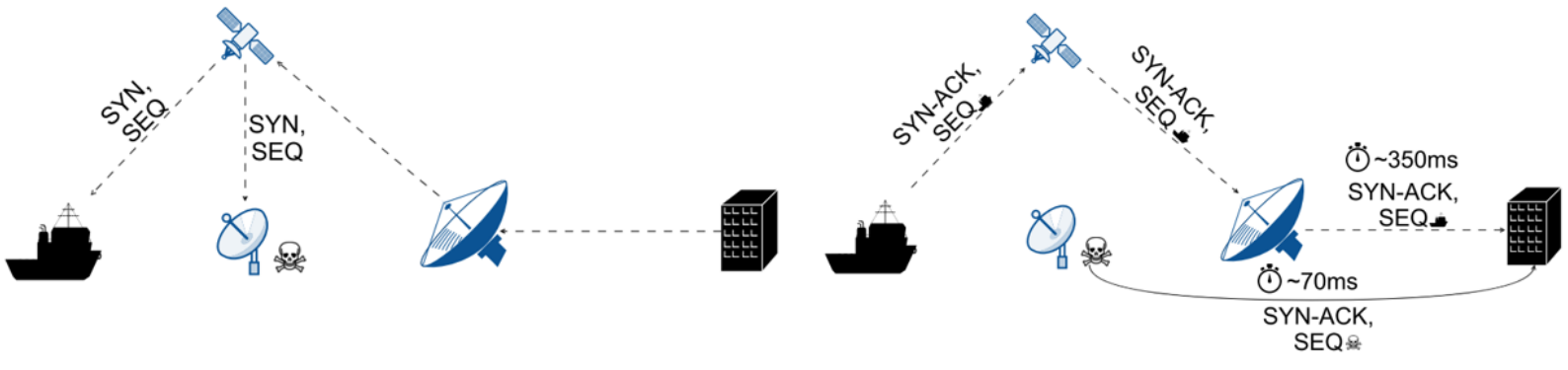


Item	Approximate Cost
TBS-6903 DVB-S2X PCI Card	$300
Selfsat H30D Satellite Dish	$88
3-meter Coaxial Cable	$5
Total	$393



数据链路层协议	通用流封装GSE	多协议封装MPE
封装粒度	通常封装单个或少量的IP数据包，每个GSE帧可以包含一个或多个IP数据包	通常封装大量的IP数据包，形成一个大的MPE段，每个MPE段可以包含多个IP数据包
效率	更适合于小数据包传输，减少了封装开销，提高了传输效率	更适合于大数据量传输，但可能引入更多的封装开销
应用场景	适用于实时数据传输、文件传输、以及需要高可靠性和低延迟的应用场景	适用于非实时数据传输、大规模数据分发等应用场景

- **主动攻击**：由于信号高度定向，需要攻击者位于目标附近，且需要使用**昂贵而复杂的无线电设备**等条件限制，主动攻击历来少受关注，但卫星网络独特的物理特性`光速延迟`，为TCP会话劫持提供了理想条件
- **TCP劫持过程**：
  - 从地面后台发送的**TCP-SYN包**和**相关序列号**同时到达合法接收方和窃听方
  - 攻击者用接收到的序列号生成**SYN-ACK响应**，并通过低延迟有线互联网连接传输。由于**光速延迟**，攻击者的响应几乎可以保证先到达。



无线电设备与调制解调器接入卫星方式比较

- **无线电设备**：适合研究和原型开发，具有高灵活性和低成本优势**[VSAT_USENIX_2024]**
- **调制解调器**：适合商业部署，具有高性能和易用性优势**[海上VSAT_SP_2020]**
- **搭配使用**：通过共用天线系统和计算机实现数据交换和协同处理，结合两者的优势进行卫星通信研究和实验**[Satellite Modems_CCS_2024]**

1. 区别

维度	USRP B200/B200mini	Newtec MDM2200
设备类型	软件定义无线电（SDR）	专用调制解调器
灵活性	高（支持多种协议和调制方式）	低（内置固定协议）
成本	低	高
开发友好性	高（适合研究和原型开发）	低（适合商业部署）
性能	中等（受限于硬件和软件）	高（专为卫星通信优化）
易用性	低（需要编程和配置）	高（提供图形化界面）

2. 共同点

- **天线系统**：都需要抛物面天线、LNA和滤波器
- **信号处理**：都需要解调和处理卫星信号
- **应用场景**：都可用于卫星通信研究和实验

3. USRP B210/B200/B200mini详细分析比较

参数	USRP B210	USRP B200	USRP B200mini
通道数	双通道（全双工）	单通道（半双工）	单通道（半双工）
应用场景	**复杂信号处理**：如星间链路仿真、动态路由测试	**单链路通信**：如卫星遥测、DVB-S2信号接收	**简单实验**：如频谱监测、信号重放攻击测试
尺寸	较大（适合固定实验环境）	中等（便携性较好）	小型（便携性最佳）
供电	USB 或外部电源	USB 或外部电源	USB 供电
价格	较高	中等	较低

4. 例=>USRP B210/B200/B200mini/RTL-SDR 配置与连接

- **设备清单**：
  - **USRP B210/B200/B200mini**：软件定义无线电（SDR）硬件
  - **天线**：根据卫星频段选择（如：抛物面天线用于Ku波段，螺旋天线用于L波段）
  - **低噪声放大器（LNA）**：提升接收信号的信噪比（如：Nooelec's SAMbird+GOES）
  - **同轴电缆与适配器**：低损耗电缆（如：LMR-400）和对应接口（SMA/N型）
  - **计算机**：安装Ubuntu或支持UHD驱动的系统


- **连接步骤**：
  - **天线 → LNA → USRP B210/B200/B200mini/RTL SDR → 计算机**：通过同轴电缆按顺序连接天线、LNA，并接入USRP的RX端口，最后使用USB 3.0线缆连接USRP与计算机
  - **供电**：若使用高增益天线或LNA，需外接电源（如USB供电不足时使用独立电源）
- **确定目标卫星参数**：

    - **频率**：如亚洲7号卫星的Ku波段下行频率为12.5 GHz
    - **极化方式**：水平（H）或垂直（V），需与天线匹配
    - **符号率与调制方式**：如DVB-S2 QPSK，符号率30 MSym/s
- **使用GNU Radio接收信号**：验证硬件连接

```
sudo uhd_images_downloader  # 下载FPGA镜像

sudo apt install gnuradio # 安装GNU Radio

uhd_find_devices  # 检测USRP是否被识别
uhd_fft -f 12.5e9 -s 10e6  # 查看12.5 GHz频段频谱（替换为你的卫星频率）
```

- **验证信号接收**：
    - **频谱特征**：
        - 在频谱仪中观察是否存在明显的信号峰（带宽与符号率匹配）
        - 例：DVB-S2信号的带宽为符号率的1.2倍（30 MSym/s → 36 MHz带宽）
    - **星座图**：
        - 若信号为QPSK，星座图应显示4个聚集点；若解调正确，点越集中，信噪比越高
