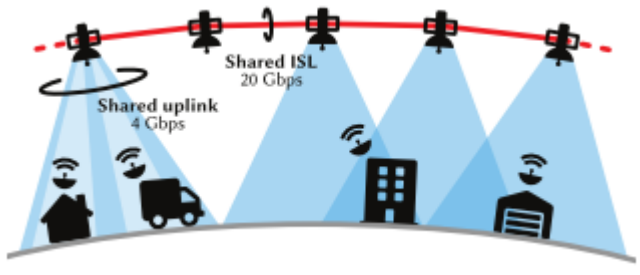
2025-02-27汇报

文献阅读

USENIX=>2021=>ICARUS=>近地轨道卫星网络攻击

- **攻击场景**——针对低地球轨道LED卫星网络(2000公里以下)特性，提出一种新的拒绝服务DoS攻击方法，即ICARUS



全球可访问性	**可以在不同地点发起攻击，增加了攻击的灵活性和难以追踪性**
低延迟目标	通常采用最短路径路由，使得攻击者更容易预测和利用路由
路径结构公开	LEO卫星的位置和网络结构公开，可根据信息规划攻击流量
高带宽链路	星际链路ISL具有较高带宽，但相对较少，可集中攻击这些链路造成网络拥堵

- **攻击原理**——利用LEO网络的全球可访问性和低延迟目标，确定合适的目标链路，选择合适的流量分配策略，通过控制僵尸网络中的主机(由受感染的启用卫星的主机进行)，集中向薄弱环节注入流量，造成目标链路的拥堵

- **流量分配策略**——注入流量的同时，尽量降低攻击成本，并减少对单个卫星上行链路的带宽占用，降低被检测的风险

单链路攻击	**选择攻击单个链路，如上行链路、下行链路或ISL，通过在这些链路上产生大量流量来造成拥堵**
多链路攻击	选择同时攻击多个链路，以阻断大区域之间的通信，更广泛地影响网络

攻击流程

- **链路与路径发现**——使用已知的卫星间拓扑创建连接图，运行`Dijkstra算法`计算每个bot与通信可达卫星的最优路径
- **路径过滤**——只保留在期望攻击方向上的目标路径
- **可行攻击流计算**——决定流量分配：1.目标链路刚好高于容量；2.其他链路不拥塞，确保攻击流量能够顺利到达目标链路，避免攻击流量"自我拥塞"
- **减小最大攻击流量maxUp**——迭代优化，每次降低流量执行可行性检查，直到找到最小值
- **降低可探测性**——将攻击流量分布在众多上行链路进行攻击

概率ICARUS

路径不确定性——多链路情况下存在**负载均衡、均匀随机路由**的情况，攻击者无法提前知道他们的攻击流量将采取哪条特定路径，因此以概率ICARUS方式执行攻击流量分配，即**高概率淹没目标链路**，同时避免攻击流量之间的自拥塞，降低maxUp

评估实验设置

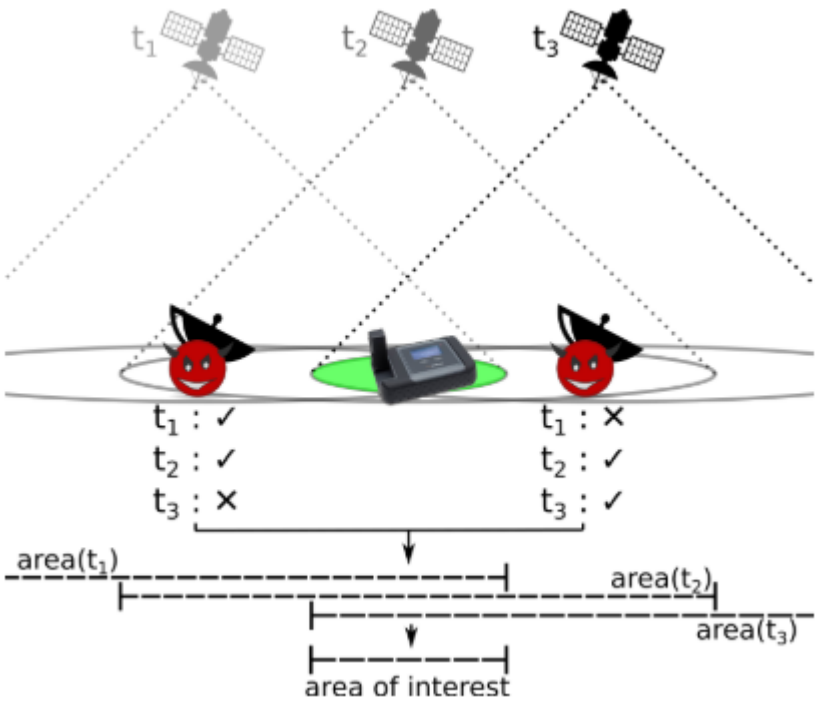
模拟场景——对SpaceX星链壳I星座进行LSN框架(约5000行Python代码，支持任意星座)模拟，总共1584颗卫星，并将各卫星地理位置离散到三角形平铺的测地线网格，每个三角形代表10万平方公里面积，进行三种良性流量场景测试(空流量、区域GDP流量、人口流量)

改进思路

- **路径识别优化**——ICARUS对路径的发现与过滤方法过于过于传统，可以根据**历史流量数据(流量大小、时间戳、源卫星、目标卫星等)**以及**路由数据(不同时间段内的路由选择策略和路径变化)**训练模型，预测卫星网络中的流量模式和路径变化，更快速精准的找到目标路径，制定相应攻击策略
- **优化攻击策略**——优先攻击原有流量较高的目标链路，对目标链路通信距离较近的僵尸主机群进行攻击流量分配与快速响应
- **考虑虏拓扑动态性**——利用实时卫星网络拓扑数据，动态更新路径发现算法，确保攻击路径始终最优；也可利用卫星在区域之间移动过程中负载变化进行针对攻击

USENIX=>2024=>RECORD=>近地轨道卫星接收区域确定攻击(偏信号)

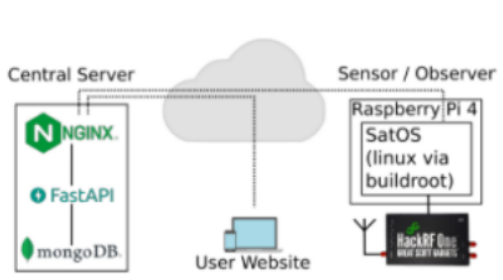
- **LEO卫星系特性**——绕地球运行时的相对角速度高，从地面观察会随时间移动。在这一定移动时间段内，接收器才能接收到来自这颗卫星的信号
- **攻击思路**——根据卫星靠近和远离目标时，不同卫星波束的接收转换事件确定卫星用户的位置。即：被动地利用观察到目标设备的下行链路通信，估计其位置
- **攻击影响**——铱星公司在全球拥有190万用户，只要攻击者可以将铱嗅探器放置在卫星波束的范围内(可以在其他国家)，任何人都可以跟踪目标人的家庭基地



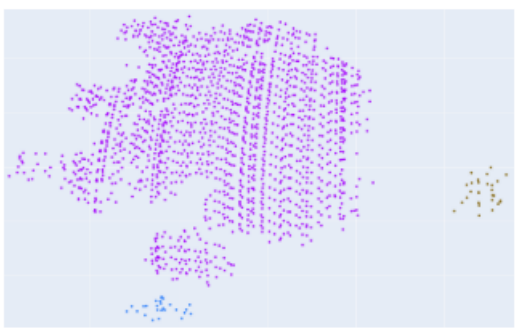
- **RECORD攻击**——两个观察者随着时间推移接收下行链路消息，并结合估计终端的位置区域，将目标卫星用户所在的区域缩小到比卫星波束大小低几个数量级的程度(如观察2.3小时将用户位置缩小到半径11公里以内，原卫星波束大小4700公里，增加观察时间区域可进一步缩小)

RECORD攻击实现

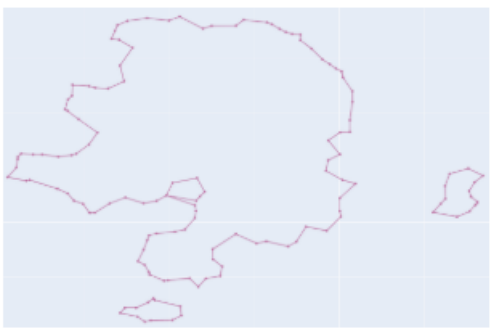
- **实验设置**——`中央服务器`提供网站控制和管理系统；`观察者`核心树莓派4，连接HackRF One(含有铱天线、GPS、LTE屏蔽)；三个观测服务器



- **天线波束建模**——收集铱状态消息(包含发送该信息的卫星和波束天线的编号)，计算出各卫星天线的发送角度，对于不同波瓣，使用`scikit-learn`库的基于密度的空间聚类算法`DB-SCAN`，对每个天线的测量值划分为天线每个瓣的簇，并只保留外部数据点，最终创建高效轻量的最大天线占地面积模型，可以投射到地球表面



(a) Clustered measurements.



(b) Optimized borders.

(c) Projection onto Earth surface.

- **记录受害者流量**——受害者随机访问网站产生攻击所需流量，观测服务器收集流量数据，使用工具`gr-iridium`与`iridium-toolkit`记录与解析数据包，识别目标设备的下行链路消息：利用连接设置，铱星中**GSM身份验证**过程存在**静态TMSI限制**，允许攻击者在连接建立期间识别设备。一旦完成连接，即可得到目标设备的消息列表
- **估计目标位置**——利用对铱星协议知识，以及目标设备可利用的铭文状态消息，提取事件列表，并根据天线模型计算每个事件的`接收区域RoI`。即：通过合并多个天线的覆盖范围，来计算各事件`接收区域RoI`，并且`接收区域RoI`会随着时间的推移进一步缩小，最终集中在所有事件的重叠部分

(a) Single antenna footprints.

(b) Union of the footprints.

局限性——(1)目标设备在观察期间不会移动太远；(2)如何区分干扰，即：由于障碍物/噪声或由于在天线波束之外而无法接收的消息

改进思路

- **针对移动性**——引入实时动态跟踪算法，以预测和补偿目标设备的移动；
- **针对干扰信号**——(1)通过训练模型识别不同干扰源的特征，对接收到的信号进行分类，区分有效信号和干扰信号；(2)采用自适应滤波和频谱分析，识别和过滤掉干扰信号
- **优化天线模型**——在攻击过程中实时更新天线参数，以反映环境变化对天线性能的影响
- **优化解析技术**——通过改进算法，优化数据包解析工具，提高解析速度和准确性
- 可进行**实验复现**来讨论如何**优化攻击**、以及对该攻击的**阻断防御**——(**虚拟位置生成**——设备通信中引入虚拟位置信息、**延迟发送**——随机延迟下行链路消息的发送时间、**动态TMSI分配**——避免使用静态TMSI，改为动态分配和定期更新)