4.8号上报，4.6号形成申报书，4.5号上午9点提交材料

最后框架：

1. 大规模低感知网络资源探测通道技术

* 大规模低感知网络探测技术(绕过、隐蔽、扩展性)
* 高可用抗反制高速探测技术(获取能力、覆盖范围、防追踪)
* 大规模网络探测通道管理技术（变换IP）
* 网络资源探测评价与分析技术(成本与代价、性能、覆盖度、隐蔽性评价)

大规模网络资源探测性能评价、大规模网络资源探测覆盖率评价、网络设备地址映射精度评价、特定网络信息探测与内容识别性能评价、网络空间资源探测成本与收益评价等。

1. 主被动大规模网络设备探测技术

* 基于通信关系和通信内容主流网络设备被动快速识别探测(被动分析)
* 多源分布式主流网络设备主动探测识别技术（主动获取）
* 核心网络设备拓扑结构分析技术（主被动结合，拓扑生成）

以下内容，仅供参考

1. 全球范围内多途径大规模网络资源探测技术

资源探测分为普查型探测和聚焦式探测两种，相对而言，前者具有轻量级、低负荷等特点，通常用于测量互联网拓扑结构、路径延迟、终端的系统指纹信息等，可通过降低冗余度的方式进一步提高探测性能，难点在于节点间连接关系的测全率；后者具有探测内容多样、载荷高、实时性要求高等特点，通常用于采集终端的详细设备指纹信息和安全漏洞，难点在于设备的可访问性、测量的性能与隐蔽性，可通过渗透技术、多源混淆测量技术等提高信息获取能力。

1. 主流网络设备的快速探测

快速探测的意义在于，能给出一个较小时间窗口内Internet设备的拓扑快照。ZMAP快速扫描工具，针对上述快速大规模测量而设计，使用随机化探测的技术，并且跳过协议栈直接生成以太栈，在扫描速度上能达到以太网理论上的极限，大大提高了扫描速度。此外ZMAP使用类SYN cookie技术，做到了不保存状态信息，不重传丢包，提高了扫描速度的同时降低了内存资源消耗。此外，ZMAP提供的模块接口，可以支持如TCP SYN scan、ICMP request scan，DNS scan等种单包探测，增加了扫描引擎的复用性和多态性。ZMAP面临的挑战是，其扫描策略是简单随机枚举，对于IPV6的测量，由于其地址空间过于庞大，枚举法不适用。此外，ZMAP的广泛使用，会给网络上的主机带来较大的负载，所以缺乏一种排除机制，选取适当的主机进行测量。

1. 主流网络设备的指纹识别

指纹识别的意义在于，除了测量网络设备的ip接口拓扑外，还提取设备上有关操作系统、提供的服务、防火墙类型等描述设备具体属性的设备指纹，对网络设备有更细节的掌握。NMAP工具，提供TCP SYN scan，Xmas scan等多种端口扫描技术的实现，结合社区维护的保存有主流的2200多个服务的namp-services数据库，进行服务探测。NMAP使用nmap-service-probes数据库，针对不同的服务，发送相应探测包，以进行进一步的服务版本探测，发现服务背后的协议类型，实现版本，版本号等，还有服务所反映的设备信息如主机名称、设备类型、操作系统信息等。对于在测量中发现的设备，使用TCP ISN采样、IPID采样、TCP选项支持，初始窗口大小检测等多种探测设备特征行为的方法，结合保存有2600多个主流OS指纹的nmap-os-db数据库，给出设备的操作系统零售商、操作系统类型、操作系统版本、还有设备本身的设备类型、在线时间、ip序列号的可预测性强弱等多种设备指纹信息。

1. 大规模低感知网络探测技术
2. 大规模网络拓扑探测（张宇）

大规模拓扑探测最早是从几个观测点出发进行的探测，例如法国UoS Pansiot等人进行的研究。专用大规模拓扑探测平台，CAIDA的Skitter利用web服务器，以及Skitter的后继Arc。一般意义的分布式测量平台还有，Planet Lab，iPlane，和UW的RocketFuel。全球有近千个Traceroute server，作为拓扑探测的窥镜(looking glass)，由于其测量点的分布覆盖范围广，能够保证较好的完全性。此外还有crowd sourcing测量，不再适用专用的测量平台，而是利用Internet大量的用户基础，通过在浏览器安装插件，让终端用户执行测量工作，如Scriptroute，Dimes，Bitprobe等。这种利他主义的方法，需要额外的设计权衡，和安全性考虑。

在大规模拓扑探测中，有两个科学问题：首先观察点的选取问题，有的观察点很难发现一些如AS间的p2p路径。相关研究使用了Targeted Probing技术，利用专家的领域知识，有根据的进行探测。其次，大规模traceroute测量平台要有合理的协作机制，如果不对冗余测量进行控制，和观察点拓扑距离较小的路由器将会有较大负载。针对该问题，通常在监控点内采用“远探针”手段，监控点间采用“协作监测”手段，去除冗余测量，做到高发现率的同时，降低负载。

1. 网络资源被动获取技术
2. 敏感音视频信息探测与分析
   1. 敏感音视频信息采集技术
   2. 敏感音视频内容分析技术
   3. 境内外网站有害信息探测与内容分析
   4. 基于线索的敏感信息内容获取（主动被动方式结合）

从海量信息中查找敏感内容，传统的被动抓取模式不能满足要求，因为搜索引擎的资源无法与整个互联网的信息抗衡，敏感信息获取的时效性也无法保证，因此需要按线索进行主动、聚焦抓取。

拟通过本体论结合主题映射的描述方式来建立线索库，在爬虫系统的运行过程中，由抓取结果反向推动线索库的自动更新；研究通用转换模型，将线索转换为爬虫能够接受的抓取参数，主动控制爬虫行为；针对爬虫系统盲目抓取的问题，研究对象变化规律模型，实现对最可能发生变化的对象进行抓取的资源调度技术；针对大型网站的深度连接难以获取的问题，研究多源分布式的深网爬取技术，有效规避爬虫陷阱，实现特定内容的高效获取。

* 1. 基于流量分析的移动设备定位技术

移动设备经常利用定位功能获取地理位置信息，并通过无线网络将位置信息发送给第三方，以获得基于位置的服务。由于地理位置信息会与包括IP在内的其他信息一同发送，因此，通过对基站流量的监测和分析，能够获取移动设备的地理位置信息。

在相关国际规范下，地理位置信息具备较为统一的数据格式，利用基于特征的流量识别技术，可以实现对含有位置信息的数据包的识别和抓取，从而获取地理位置信息。

此外，移动设备对位置信息的使用方式，与人的行为规律具有紧密联系，例如导航过程中的周期性位置信息发送，以及位置信息与服务请求信息的绑定性等。针对该特性，可以通过对位置信息在整体流量中规律的学习，提高位置信息的获取能力，从而进行更准确的设备定位。

创新点：

1. 基于大规模多通道的网络资源探测技术
2. 跨平台线索制导的敏感网络信息内容获取与研判
3. 全球范围网络设备与地理空间位置精确映射
4. 全球网络地图构建与可视化