前言

由于无线路由得普及，各类网络的接入都通过无线路由器，因此从接入网络的用户来看，比较容易接入伪造的路由设备，从而将自己的网络流量暴露在不安全的网络环境之下，而对于设备的一些普通的验证方式，如mac地址、设备名称、（无线路由通道）等都容易伪造成同被伪造的路由一样的信息。所以，在客户机端对目标路由进行判断是否是伪造的路由设备不能光借助先前这些不安全并且较为容易仿造的信息，需要有新手段来检测路由设备的真伪，对于路由协议的流量包进行指纹比对和识别，以此来避免信息伪造的可能性，减少用户流量信息被窃取的情形。

研究的问题是

通过相关协议特征提取路由器的指纹特征，分析分类

研究方法

【被动收包+主动抓包】包抓取+分类器

相关路由器的协议分析

主要考虑路由器子网内的协议1.DNS 2.icmp 3.ssdp 4.arp