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

观察一段时间内的路由器和主机间收发的数据包，可以发现其网络协议主要为ICMP\ARP\SSDP\ARP

[wiki]

1. DNS协议是一
2. Icmp（Internet Control Message Protocal）是用来返回错误信息和分析路由的。很多常用的工具基于icmp消息，本文的实验中使用的ping来获得数据包在主机和测试路由器之间收发状况，其运作原理是向目标主机传出一个ICMP id字段中为“echo request”的类别代码，并接收id字段中为“echo reply”的类别代码。
3. Arp(Address Resolution Protocol) 是用来透过目标设备的IP地址。查询目标设备的MAC地址，以保证通信的顺利进行。本文的实验中使用向