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

Dns协议的运作过程和蕴含参数

Icmp协议的运作过程

Arp协议的运作过程

Ssdp协议的运作过程

在控制点接入网络设备的时候，

数据采集

Ubuntu系统下使用python的网络编程方法对于不同协议的协议内容发包，并采用tcpdump进行流量监听记录流量帧的信息。对于dns协议，预先选取200条网址做为域名请求，返回ip地址，在清除计算机上的dns缓存后，在socket库中使用获取地址信息的函数请求向路由器发送dns域名请求包，监听路由器的返回包，提取相关流量帧的特征。对于icmp协议，使用shell中的ping方法，以路由器在子网内的地址做为ping目标发送1500条ping请求，并监听路由器的返回信息，提取流量帧的特征。对于arp协议先获取路由器和监听主机的ip地址使用python中scapy库，向路由器发送2000条arp请求，监听路由器的返回包并提取相关的流量帧的特征。对于ssdp协议，采用被动收取的方法，在主机接入路由器后，监听upd的1900端口。

协议蕴含的参数

五个主要的分析

Ssdp单独分析

协议数据帧的实际分布特性

按照图以及几篇参考文献