北京信息科技大学

（楷体1号居中）

**毕业设计（论文）**

（楷体初号加粗居中）

**题 目：** 安卓中间人攻击的研究与实现

**学 院：** 计算机学院

**专 业：** 计算机科学与技术

**学生姓名：**计科1302 **班级/学号** 2013011172

**指导老师/督导老师：** 路旭强

**起止时间：**200 年 月 日 **至** 200 年 月 日

（以上宋体四号居中）

**摘 要**

（宋体、三号、加粗、居中）

随着网络信息技术的快速发展和普及，尤其是近年来无线接入技术和和移动终端技术的飞速发展，无线局域网已经成为人们工作和日常生活的必须。同时由于底层网络协议的不安全，导致主机对接受到的数据盲目信任，以至于让数据的传输不安全。中间人攻击（MITM）由于攻击方式简单，难于察觉等特点，成为危害无线局域网的主要方式。生活在局域网随处可见的环境下，了解一些网络数据传输原理和熟悉普遍的局域网攻击方式是很有必要的。

本文对ARP协议的内容、工作原理和协议漏洞有一定详细的介绍，并介绍了ARP欺骗攻击的原理和基本的防御方法。开发了一款运行在安卓系统上的应用，该应用实现了局域网ARP欺骗攻击和防御，主要功能有断网攻击、数据嗅探、HTTP数据劫持、和防御ARP欺骗攻击。通过该应用，普通用户可以体验ARP欺骗攻击的危害，加深对局域网安全的认识；安全研究人员可以学习ARP欺骗的原理和检测局域网是否安全。

（宋体、五号）

**关键词：**（3~8个词）中间人攻击； ARP欺骗； 局域网安全 ； 安卓；

数据劫持；

注：**关键词：**（宋体、五号、加粗） ；□□□□□□（宋体、五号）

**Abstract**

(Times New Roman、16磅、加粗、居中)

（Times New Roman 、12磅）

With the rapid development and popularization of network information technology, especially in recent years, the rapid development of wireless access technology and mobile terminal technology, wireless LAN has become a must for people to work and daily life. At the same time due to underlying network protocol insecurity,resulting in the host to blindly trust received data,so that the transmission of data is not safe. Man-in-the-middle attack (MITM) is the main way to harm wireless LANs because of the simple attack mode and difficult to detect. Living in the local area network can be seen everywhere in the environment, to understand some of the principles of network data transmission and familiar with the common LAN attack is necessary.

This article describes the contents of ARP protocol, working principle and protocol vulnerabilities, and introduces the principle of ARP spoofing attack and the basic defense method. Has developed an application running on the Android system, the application implements LAN ARP spoofing attack and defense, the main features are broken network attacks, data sniffing, HTTP data hijacking, and defense ARP spoofing attacks. Through this application, ordinary users can experience the dangers of ARP spoofing attacks, deepen the understanding of LAN security; security researchers can learn the principle of ARP spoofing and detect whether the LAN security.

**Keywords:** ( 3~8 words) □□□□□□;□□□□□□;□□□□□□;□□□□□□;□□□□□□;□□□□□□;□□□□□□

注：**Keywords:** 12磅加粗 ； □□□□□□ 12磅

**目 录**

（宋体、三号、加粗、居中）

**摘要** （中文） …………………………………………………………………………I

（英文） …………………………………………………………………………II

**第一章** □□□□□□□□□□□□□□□ ……………………………………

1.1 □□□□□□□□□□□□□□□□ ……………………………………

1.2 □□□□□□□□□□□□□□□□ ……………………………………

**第二章** □□□□□□□□□□□□□□□□ ……………………………………

2.1 □□□□□□□□□□□□□□□□ ……………………………………

2.2 □□□□□□□□□□□□□□□□ ……………………………………

∶

∶

**第X章** □□□□□□□□□□□□□□□□ …………………………………

**结束语** …………………………………

**参考文献** …………………………………

注：1 摘要、章、结束语、参考文献：（宋体、小四、加粗、居左）；

2 节：（宋体、五号）；

3 中文摘要、英文摘要、目录的页码依次编排用“Ⅰ、Ⅱ、Ⅲ …”罗马数字（宋体、小五号、居中、底部）。

**第一章 概述**（宋体、三号、加粗、居中）

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□（宋体、五号）

**1.1 □□□□□□□□□□□□□□**（宋体、小四、加粗）

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□（宋体、五号）

**1.2**  **□□□□□□□□□□□□□□**（宋体、小四、加粗）

**1.2.1 □□□□□□□□□□□□**（宋体、五号、加粗）

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□（宋体，五号）

**1.2.2 □□□□□□□□□□□□**（宋体、五号、加粗）

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□（宋体、五号）

（行距：最小值，18磅）

注：1论文正文的页码依次编排用“1、2、3 …”数字（宋体、小五号、居中、底部）