2011 年 5 月　　西 安 邮 电 学 院 学 报　　May 2011
第 16 卷 第 3 期　　JOURNAL OF XI'AN UNIVERSITY OF POSTS AND TELECOMMUNICATIONS　　Vol. 16 No. 3

# 基于 Linux 的无线网络监听技术

刘　敏，朱志祥

（西安邮电学院 通信技术研究所，陕西 西安　710061）

**摘要**：为了改善目前无线网络数据监听技术中存在的严重丢包现象，在 Linux 环境下提出一种基于 Libpcap 异步机制的监听新方法，可通过进行 IEEE 802.11 协议的数据包捕获和过滤模块设计，利用 Libpcap 机制的 BPF 过滤器和包转发功能，实现无线网络数据包的有效监听。与普通监听技术相比，基于新方法而设计的体系结构丢包少、效率高，能有效提高网络数据监听效率。

**关键词**：无线网络；网络监听；数据过滤；数据捕获

**中图分类号**：TP302.1　　**文献标识码**：A　　**文章编号**：1007-3264(2011)03-0065-04

在无线局域网中通过无线捕包技术，可以截获无线网络[1]传输的数据帧，对捕获的数据帧进行分析和解码，可以实时监视网络的状态、数据的流动及网络上传输的信息，但现有的无线网络监听方法在对数据包进行捕获时存在着严重的丢包现象，特别是当网络传输速率增大时丢包率显著增加，总是无法将整个数据包较完整的捕获，针对目前现有技术存在的问题，本文对数据包监听原理做了分析和研究，提出一种 Linux 环境下的监听方法[2]基于 Libpcap 异步机制的有效监听方法。该方法可以改善现有的无线网络监听技术的不足，有效减小无线局域网高传输速率下的数据包捕获丢包率。

## 1　无线局域网监听原理

一个无线网卡主要包括网卡（Network Interface Card，NIC）单元、扩频通信机和天线 3 个组成功能块。NIC 单元属于数据链路层，由它负责建立主机与物理层之间的连接。扩频通信机与物理层建立了对应关系，实现无线电信号的接收与发射。当计算机要接收信息时，扩频通信机通过网络天线接收信息，并对该信息进行处理，判断是否要发给 NIC 单元，如是则将信息帧上交给 NIC 单元，否则丢弃掉。如果扩频通信机发现接收到的信号有错，则通过天线发送给对方一个出错信息，通知发送端重新发送此信息帧。当计算机要发送信息时，主机先将待发送的信息传给 NIC 单元，由 NIC 单元首先监测信道是否空闲，若空便立即发送，否则暂不发送，并继续监测。由此看出，无线局域网（Wireless Local Area Network，WLAN）的工作方式与由 IEEE802.3 定义的有线网的载体监听多路访问/冲突检测（Carrier Sense Multiple Access/Collision Detect，CSMA/CD）工作方式很相似。

无线局域网 WLAN 由无线网卡、无线接入点（Access Point，AP）、计算机和有关设备组成，拓扑结构如图 1 所示。WLAN 中的工作站（Station，STA）是指能够发送和接收无线网络数据的计算机设备，如配置无线网卡的个人电脑（Personal Computer，PC）或笔记本电脑。接入点 AP 类似于有线局域网中的集线器，是一种特殊的无线工作站，其作用是接收无线信号并发送到有线网络，它可以通过标准以太网电缆与传统的有线网络相连，作为无线网络和有线网络的连接点。

由于无线网络的电磁辐射难以精确地控制在某个范围之内，所以在数据发射机覆盖范围内的几乎

**收稿日期**：2011-01-30

**基金项目**：国家科技重大专项基金资助项目（2009ZX03004-003-04）

**作者简介**：刘敏（1986-），女，硕士研究生，研究方向：无线网络安全，E-mail：minminbl04@sina.com；朱志祥（1959-），男，教授，博士，研究方向：信息安全。

任何一个无线网络用户都能够获取这些数据。从这个意义上说，无线接入点 AP 可以看作一个无线集线器，无线局域网可以看作一个广播式以太网，无线局域网数据监听的实现正是基于这一原理。

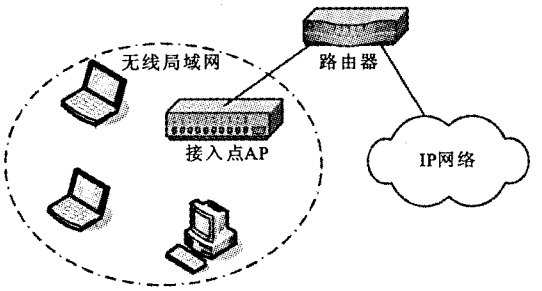


图 1 无线网络拓扑结构

## 2 无线网络监听系统的设计与实现

### 2.1 无线网络监听体系结构

在无线网络中，无线设备之间传输的数据都是采用广播方式进行传播的，但要截获所需要的无线网络数据包，需要使监听设备尽量满足以下条件：

(1)使监听设备接近信息的源发送点；

(2)内置网卡停止发送数据；

(3)在捕包时尽量减少监听设备 CPU 的其他开销；

(4)选择特定的信道进行监听。

监听的体系结构如图 2 所示。

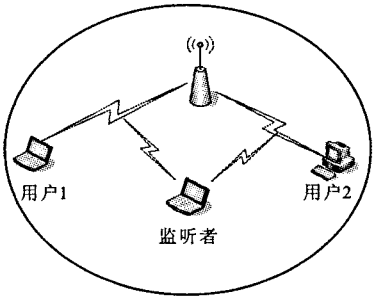


图 2 网络监听体系结构

### 2.2 数据包的捕获概述

Linux 网络流量分析系统首先依赖于一套捕捉网络数据包的函数库。这套函数库工作在网络分析系统模块的最底层。作用是从网卡取得数据包或者根据过滤规则取出数据包的子集，再转交给上层分析模块。从协议上说，这套函数库将一个数据包从链路层接收，至少将其还原至传输层以上，以供上层分析。

现有的大部分 Linux 捕包系统都是基于 Libpcap[3,4]这套函数库或者是在它基础上做一些针对性的改进。Libpcap 是一个基于包过滤器(Berkeley Packet Filter，BPF)的开放源码的捕包函数库。Libpcap 函数不仅拥有高效的 BPF 过滤器，还具有灵活的包转发功能，利用它可以较容易地开发网络监听程序。它提供了一系列函数接口，为上层应用程序捕捉，记录和分析数据包提供了有力支持。它包括包捕捉模块和包转发模块两部分。包捕获模块完成从网络驱动程序拷贝数据到根据过滤条件选择是否丢弃数据包的功能。Libpcap 的工作流程：

(1)利用 Pcap_lockupdev ()找到可用的网络设备；

(2)利用 pcap_live_open()初始化网络设备，并返回一个 pcap_t 结构的指针；

(3)再利用 pcap_compile()和 pcap_serfilt()设置过滤器；

(4)最后调用 pcap_loop()函数不断获取数据包，放入缓存中供应用程序处理。包转发模块利用 pcap_sendpacket()完成向网络中发送数据包，且无需调用系统应用编程接口(the Application Programming Interface，API)。

Libpcap 工作流程如图 3 所示。

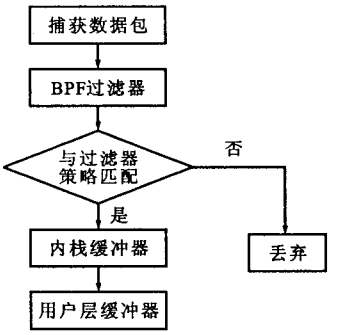


图 3 Libpcap 工作流程

### 2.3 数据包捕获和过滤模块的设计

在传统的有线局域网中，用户可以将网卡设置为混杂模式(promiscuous mode)来关闭有线网卡的过滤机制，从而获得网卡接收到的所有数据包。然而，在无线网络中抓包无线网卡必须被设置在监听模式下。若不设置在监听模式下则无法正常的显示无线网络数据包，网卡或网卡中的驱动会自动将其转换成有线网络数据包的形式。采用监听模式工作的无线网卡可以使主机不接入周围的任何一个基站子系统 (Base Station Subsystem，BSS)，从而使无线网卡能够捕获其覆盖范围内的所有传输数据。另外，采用监听模式工作的无线网卡不能向外发送数据帧，这意味着无线网卡只能完全“被动”的获得网

络信息,因此也就不会被其他无线网络探测工具发现,从而增加了攻击的隐蔽性。无线网络抓包包括数据包的捕获和过滤两大主要模块,以下是两个模块的实现。

2.3.1　数据包捕获模块

先将网卡设置为监听模式,进入监听状态。如果监听到 802.11 数据包则调用回调函数,将其拷贝到内存,为下一步数据包的处理做准备。

处理流程:

(1)根据初始化模块获取的网卡信息选择一块适合用来捕获数据包的网卡;

(2)创建捕获数据包所需要的数据结构(其中包含设备的信息和设置选项)并设置其中的选项,如果失败则转至(7);

(3)开始启动监听,如果失败则转至(7);

(4)设置需要监听的频道;

(5)捕获到数据包触发调用回调函数,将数据包拷贝至内存中等待处理;

(6)暂停监听,再重新启动;

(7)结束监听,销毁创建的数据结构,关闭网卡,释放其他资源。

2.3.2　数据包过滤模块

按照 IEEE 802.11 协议的格式解析数据包,识别出数据包类型[5](数据帧、控制帧和管理帧)。如果数据包类型为数据帧,则准备用于破解密钥;如果数据包类型是控制帧,直接丢弃;如果数据包类型是管理帧,继续判断其子类型,如果是信标帧,则用于网络发现,否则丢弃。

处理流程:

(1)对保存在内存中的数据包做完整性检测,发现错误则丢弃;

(2)获取当前时间,计算数据包的长度,将这些信息和数据包一起保存并交给数据包分析功能的函数;

(3)根据数据包起始 2 个字节的值判断它为哪种数据类型;

(4)根据数据包的类型进一步处理,如果是数据帧,则准备用于破解,然后转至(6),如果是控制帧,直接转至(6),如果是管理帧,进入下一步;

(5)如果是管理帧,判断其子类型是否为信标帧[6](beacon 帧)。如果是则将其基本服务集标识符 (Basic Service Set Identifier,BSSID)字段同已经发现的 WLAN 集合中的各个 WLAN 的 BSSID 字段相比较,未发现相同的则表明新发现一个 WLAN,将此 beacon 帧的相关信息存入已发现的 WLAN 集合,并将此 WLAN 的信息显示在工具的 WLAN 信息窗口中。如果比较中发现相同的 BSSID,表明此 beacon 帧属于已发现的 WLAN,则不做处理。

(6)完成一个数据包的处理后等待回调函数递交下一个数据包。

## 3　测试结果

模拟测试环境:1 个 D-Link AP,3 个 TP-WN821 客户端(STA),1 个抓包系统。

通过命令:sudo iwconfig wlan0 rate ＊M 来控制客户端的发包速率。

实验测试结果:

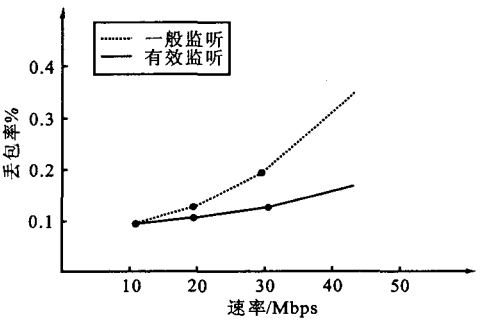


**图 4　一般监听与有效监听对比**

从图 4 可以看出,在较低网络速率下,两种监听方法的丢包率差别并不明显,都是在 0.1%左右,但是随着网络传输速率的增加,两种方法所对应的丢包率的差别开始扩大,在 40Mbps 速率下,一般监听方法的丢包率超过了 0.3%,而 Libpcap 异步机制监听方法的丢包率仍然在 0.2%以内。随着网络传输数据速率增大,普通监听方法丢包率会急剧增加,而 Libpcap 异步机制监听方法的丢包率增加缓慢,要明显小于普通监听方法。针对目前网络技术的不断改进,数据传输速率的不断增大,Libpcap 异步机制监听方法更适合于现有网络监听。

使用常用的监听方法很容易造成丢包现象,而 Libpcap 异步机制监听方法监听能尽可能的捕获完整的数据包的原因是:

一般监听是基于某个网卡驱动的数据捕获接口[7,8],单独封装相应的数据捕获模块,兼容性不好,而且效率较低。Libpcap 异步机制监听方法监听是采用跨平台的 libpcap 开发库,利用其高效的 BPF 过滤器和灵活的包转发功能,实现无线网络数据包的有效监听。

## 4 总结

通过测试结果可以看出一般监听方法在网络传输数据量增大时丢包率急剧增加，而 Linux 环境下基于 Libpcap 异步机制的监听方法的丢包率不会出现该情况，在较高的网络速率下的丢包率维持在 0.2%以下，有效改善了一般监听方法的监听效率，相比较一般监听方法，Libpcap 异步机制监听方法更适合于现有高速率网络。随着现有的网络技术不断改进，数据传输速率在未来的几年内会不断增大，各种监听方法在更高数据传输速率的改善丢包率的效率和性能，能否有新的监听方法的将丢包率降到更低的水平等，将是下一步需要继续研究的方向。

### 参 考 文 献

[1] 孙冀. 无线局域网概述[J]. 今日科苑，2007，(24)：189-189.

[2] 刘赞. Linux 内核下数据包捕获与分析[J]. 中国水运，2008，8(5)：56-57.

[3] 刘泓，张常泉. 常见的包捕获机制研究[J]. 现代商贸工业，2010，(1)：306-307.

[4] 李革新. 网络数据包捕获工具的开发与实现[J]. 计算机工程与设计，2007，28(8)：1834-1836.

[5] 马建峰. 无线局域网安全-方法与技术[M]. 北京：机械工业出版社，2005.

[6] 乔恩·爱德尼，威廉·阿尔保. 无线局域网安全实务[M]. 北京：人民邮电出版社，2006.

[7] 刘冠梅，张琴. 网络数据包捕获技术研究[J]. 现代商贸工业，2010，(1)：271.

[8] 王帅领. 网络数据包捕获技术研究[J]. 经营管理者，2010，(4)：285-286.

## An monitoring technique of wireless network based on Linux

LIU Min, ZHU Zhi-xiang

(Communication Technology Institute, Xi'an University of Posts and Telecommunications, Xi'an 710061, China)

**Abstract**: In order to overcome the packet-loss problem in wireless network monitoring technology, a new method based on Libpcap asynchronous mechanism in Linux is proposed, which can be carry out by properly designing the packet-capturing and packet-filtering modules with IEEE802.11 protocol, and making the best use of the Libpcap BPF filters and packet-forwarding mechanism. Compared with the ordinary monitor, a system based on the new method works effectively, and lose little packet.

**Key words**: wireless network; network monitoring; data monitoring; data capture

[责任编辑：祝 剑]