第34卷 第22期 计 算 机 工 程 2008年11月
Vol.34 No.22 Computer Engineering November 2008
·网络与通信· 文章编号：1000—3428(2008)22—0140—03 文献标识码：A 中图分类号：TN925.93

无线局域网协议分析系统的设计与实现

吴亚军，胡爱群，宋宇波
(东南大学信息安全研究中心，南京 210096)

摘 要：现有的无线局域网协议分析系统多采用基于PC的单点模式，操作人员需在现场实施分析，存在分析范围小、灵活性差等问题。该文提出一种分布式协议分析系统构架，该系统通过无线局域网数据采集设备对多个无线局域网采集数据，该设备与协议分析平台间通过CDMA2000网络多路数据链路进行远程控制和数据上传。给出了无线局域网协议分析的方法和数据采集设备的设计与实现，经测试表明该设备可以有效采集无线局域网通信信息，该系统能够准确地分析无线局域网协议，在安全防护、网络监测等方面有较好的应用价值。
关键词：无线局域网；协议分析；CDMA2000网络

Design and Implementation of WLAN Protocol Analysis System

WU Ya-jun, HU Ai-qun, SONG Yu-bo
(Research Center of Information Security, Southeast University, Nanjing 210096)

【Abstract】 Existing Wireless Local Area Network(WLAN) protocol analysis systems use mostly PC-based single-point mode. These systems have to be operated by the administrators on the spot. It can bring about many defects such as small range, less flexibility and so on. This paper presents a distributed multi-point analysis architecture, in which not only one WLAN is analyzed by placing several data collecting devices at the same time. Data collecting devices can be controlled remotely by the administrator via CDMA2000 network. The methods of analyzing WLAN protocol, the design and implementation of the data collecting device are also described in this paper. Test results prove that this device can collect WLAN communication information effectively. This system can be applied in many circumstances such as security protection and network monitoring.
【Key words】 Wireless Local Area Network(WLAN); protocol analysis; CDMA2000 network

1 概述

无线局域网(Wireless Local Area Network, WLAN)是无线通信网络的一个重要组成部分，它采用ISM公用频段进行通信[1]。无线信号辐射使数据采集设备能够收集无线网络中的信息，这使管理者能够对无线局域网的运行状况进行分析，监视网络运行状况、检测未授权接入和恶意攻击等非法活动。

在单点分析系统中，数据采集模块和协议分析系统集成在一个平台上，工作人员必须携带无线局域网数据分析设备到现场操作，如国内一些公司开发的基于PC的无线局域网协议分析系统[2]，工作人员只对固定的无线局域网进行协议分析。还有国外Dr. Cyrus Peikari等提出的War Drive模式[3]，即将分析设备以车载方式到实地操作。这些方式，实时性差，无法同时对多个网络进行数据分析。

2 系统设计

无线局域网协议分析系统结构如图1所示。

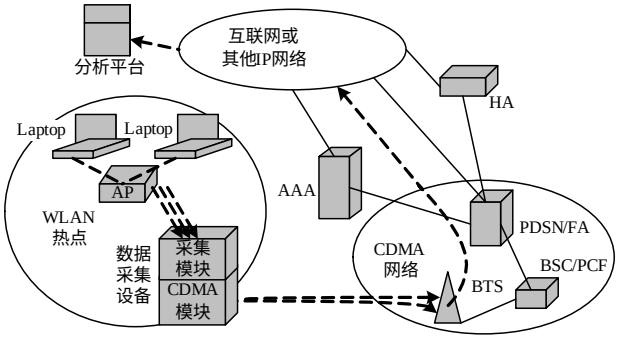

图1 无线局域网协议分析系统结构

图中热点地区覆盖WLAN，无线终端Laptop通过无线接入点(AP)接入WLAN。数据采集设备的采集模块具有802.11b/g无线局域网数据包捕获功能。同时数据采集设备能够通过认证凭借CDMA2000网络访问因特网，这使协议分析平台能够远程控制数据采集设备工作，同时数据采集设备将采集的数据由这个通道传输给分析平台，这有利于数据采集设备的分布式部署。

3 协议分析系统设计与实现

3.1 802.11MAC层协议的研究

无线局域网的帧有3种子类型：数据帧，控制帧，管理帧。每种帧有以下3个基本组成部分[4]：1个MAC帧头(MAC Header)；1个可变长度的帧体(Frame body)，对应不同子类型的帧类型；1个帧校验字段(FCS)。一般的MAC帧结构如图2所示。

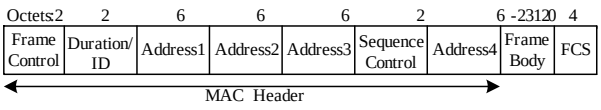

图2 MAC帧结构

基金项目：国家“863”计划基金资助项目(2006AA01Z268)；江苏省自然科学基金资助项目(BK2006108)；国家“242”计划基金资助项目(2005A14)
作者简介：吴亚军(1983－)，男，硕士，主研方向：信息安全；胡爱群，教授；宋宇波，博士
收稿日期：2008-01-06 **E-mail：**wel_1314@163.com

(1)帧控制字段(Frame Control)长度 2 Byte，如图 3 所示由以下子域组成，其中 Type 和 Subtype 可以用来区分帧的类型，即控制帧、数据帧和管理帧。

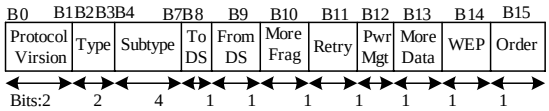

图 3　子类型结构

(2)地址字段(Address)用来指示基本服务集标识(BSSID)，源地址，目的地址，传输站地址，接收站地址。有些帧并不包含这么多地址。有些地址域在 MAC 头中指明了相对位置，而不依赖于图中的位置。

(3)顺序控制字段(Sequence Control)主要用于重组数据帧和去除重复帧。它分为 2 个部分，其中分段号长度为 4 bit，标识了一个 MSDU 的分段的编号，序列号长度为 12 bit，标识一个 MSDU 的序列号。

(4)帧体(Frame Body)的内容取决于不同的子类型，它的最大长度位 2 312 Byte。

(5)FCS 包含一个循环冗余(CRC)校验码。它用来保证帧在传输过程中没有被破坏。

控制帧用来实行区域清空操作、信道确认以及对收到的数据进行确认等功能。如当工作站需要传输比较大的数据帧时，需要利用 RTS 帧来获得媒体的控制权。CTS 帧用于对 RTS 帧的响应。ACK 帧被用来发出确认信息。当工作站从节点模式中唤醒时，会发出一个 PS-POLL 帧给 AP，来检查被缓存的数据帧。此外还有 CF-End 帧和 CF-End+CF-Ack 帧。

管理帧的主要功能是进行监督，主要用于工作站加入或离开无线网络，以及将联合从一个访问点移到另一个访问点。例如信标帧(Beacon)在一定的时间间隔发送处来，可以让工作站找到并识别一个网络，并提供一些工作站加入网络所需要的重要参数。探寻帧(Probe Request)被工作站用来寻找一个存在的 802.11 网络。此外还有探寻响应帧、关联请求及响应帧、重关联请求及响应帧、去关联帧和鉴权帧等。

3.2　协议分析系统设计

通过对无线局域网各种数据帧的分析，可以构建如图 4 所示的协议分析系统。

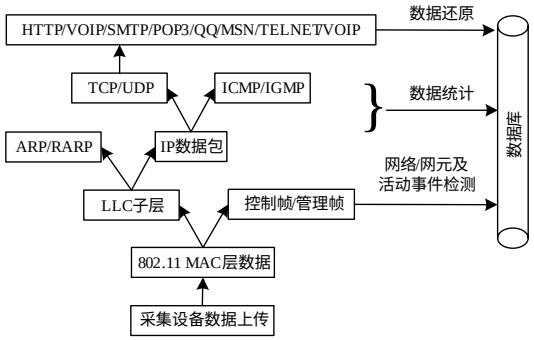

图 4　协议分析系统结构

协议分析平台主要完成网元及其活动事件检测、各种数据包的统计和应用层协议还原。无线局域网数据采集设备含有数据包过滤功能，它以 cap 的格式存储数据并传送到分析平台。协议分析系统以解封的形式逐层分析数据包：首先将 MAC 层的控制管理帧分离出来，监测网络/网元和活动事件；其次对于 MAC 层的数据帧，从 LLC 子层分离 ARP/RARP 数据包；接着从 LLC 的 IP 数据包中分离 ICMP/IGMP 数据包；最后从 IP 数据包的 TCP/UDP 包中对各种应用层数据包进行分类，由应用层协议分析模块对数据进行还原。另外对于中间分离出来的数据包作统计，并将统计信息、数据还原信息和网元及其活动信息存入数据库中以备查询。

4　数据采集设备设计与实现

一种提供无线传输功能的无线局域网数据采集设备至少包括嵌入式硬件平台、数据无线传输模块和无线局域网数据采集模块，其结构如图 5 所示。

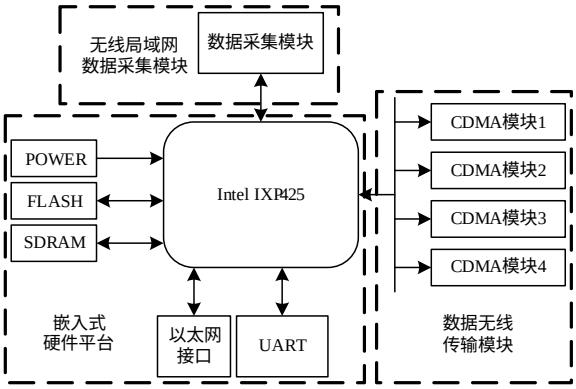

图 5　无线局域网数据采集设备硬件结构

嵌入式硬件平台主要包括：嵌入式微处理器 Intel IXP425，电源模块电路 POWER，以太网接口模块电路，串口接口模块电路 UART，随机存取模块电路 SDRAM 和闪存模块电路 FLASH。嵌入式硬件平台是系统功能的载体，同时提供了各种调试接口和功能扩展接口。

数据无线传输模块由一个串口扩展芯片 ST16C554D 连接 4 个 CDMA 网络通信芯片 CM800A 组成，四路传输提高了带宽。作为整个系统的后端，它的实现直接影响到系统在移动环境中通过无线方式接入互联网。

无线局域网数据采集模块由 Atheros 公司的基带处理器、数模/模数芯片 AR5212，结合双边带多模式射频芯片 AR2112 组成。作为整个系统的前端，这个低功耗高效率的无线局域网数据采集模块主要提供 802.11b/g 无线局域网数据采集功能。

5　功能及性能测试

(1)测试环境介绍

测试环境如图 6 所示。

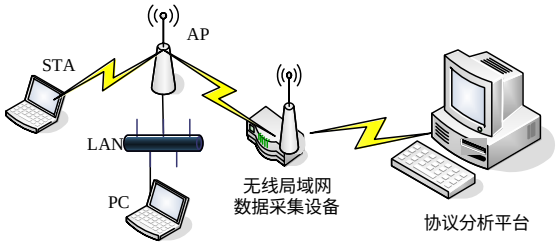

图 6　无线局域网协议分析系统测试环境

发送方 STA 通过 AP 接入 LAN 与 PC 通信，采取这种连接方式是为了避免在测试数据采集性能时重复截获相同的无线局域网数据包。无线局域网数据采集设备配合增益 7.5 dBi 的天线，在室内环境 50 m 左右的距离采集数据，并通过 CDMA 网络送到协议分析平台进行数据解析，连续测试时间为 72 h。

(2)无线局域网数据包采集测试

该数据采集设备对测试环境中的无线局域网进行数据包采集测试，以获得数据包相关信息，所得测试结果如图 7 所示。

No.	Time	Source	Destination	Protocol	Info	
41	3.298191	172.21.134.250	172.21.134.27	UDP	Src port: 1929	Des port: 5000
42	3.397439	172.21.134.250	172.21.134.27	UDP	Src port: 1929	Des port: 5000
43	3.496728	172.21.134.250	172.21.134.27	UDP	Src port: 1929	Des port: 5000
⋮		⋮	⋮	⋮	⋮	⋮

图 7　截获数据包分析图

为了有效地进行数据包采集测试，利用自行编写的服务器-客户端测试代码，从发送端(STA)向接收端(PC)发送负载长度为 500 的 UDP 数据包，并将采集设备设置成采集 UDP 数据包模式。由图 7 可知，IP 地址为 172.21.134.250 的 STA 从端口 1929 向目的 IP 地址为 172.21.134.27 的主机的 5000 端口发送了长度为 561 的 IEEE 802.11 数据(包括 UDP 头部和 500 Byte 负载)，与实验环境相符。

(3)数据包采集性能测试

在性能测试中，对 PC 的固定端口发送数据包，统计结果如图 8 所示。

Between first and last packet	36.389 s
Packets	418
Avg.packets/s	11.487
Avg.packet size	561 Byte
Bytes	234 498
Avg.Byte/s	6 444.217
Avg.Mb/s	0.052

(a)测试 1 结果

Between first and last packet	3.934 s
Packets	411
Avg.packets/s	104.468
Avg.packet size	561 Byte
Bytes	230 571
Avg.bytes/s	58 606.296
Avg.Mbit/s	0.469

(b)测试 2 结果

图 8　统计结果

在性能测试过程中，STA 分别以 0.100 ms 和 0.005 ms 的间隔向 PC 发送负载为 500 Byte 的 UDP 数据包 400 个。测试 1 中，数据包平均到达速率 11.487 p/s，平均包长 561 Byte、数据总长度 234 498 Byte，平均传输速率 52 Kb/s，数据采集设备实际采集到的数据包是 418 个，大于实际发包数，其原因是无线信道的不稳定性和误码的出现导致了 STA 和 AP 之间发生数据错误并重传，以致采集的数据包大于通信数据包。其中截获重传包数为 26，实际数据截获率 98%。测试 2 的数据平均传输率为 469 Kb/s，采集率为 100%。可见该采集设备有较好的性能，可以满足实用要求。

(4)无线局域网网元检测结果

协议分析平台对无线局域网的管理帧进行分析，所得网元列表如图 9 所示。

MAC 地址	目标类型	信道	加密	采集设备名
00:60:b3:16:55:9a	STA	6	OPE	Device-1
00:0c:41:0c:2a:8c	AP	6	OPE	Device-1

图 9　网络列表

图 9 显示了分析平台检测到的无线局域网设备列表，MAC 地址为 00:60:b3:16:55:9a 的 STA 就是被检测的站点，MAC 地址为 00:0c:41:0c:2a:8c 的 AP 就是被检测的接入点，可见该系统能有效采集和分析无线局域网的网元信息。

6　结束语

本文主要提出了一种将数据采集设备和协议分析平台相分离的分布式无线局域网协议分析系统，并讨论其原理和实现。与现有的系统相比，本系统采用基于嵌入式平台的数据采集设备，该设备可以通过 CDMA 网络传输数据，体积小，可长时间工作，便于灵活部署，工作人员可以远程使用协议分析平台对远程无线局域网进行协议分析。

参考文献

[1] 刘乃安. 无线局域网(WLAN)[M]. 西安: 西北电子科技大学出版社, 2004.

[2] 秦　鑫. 无线局域网网络协议分析与监测系统[D]. 北京: 北京邮电大学, 2006.

[3] Peikari C, Fogie S. Maximum Wireless Security[M]. 北京: 电子工业出版社, 2004.

[4] IEEE-Standard Board. IEEE Std. 802.11-1999 Wireless LAN Medium Access Control(MAC)and Physical Layer(PRY) Specification[S]. 1999.

(上接第 139 页)

利用 TCP 发送时，带宽节省 37.6%；利用 UDP 发送时，带宽节省 32.1%。造成这种差别的原因是 TCP 和 UDP 头部所占字节数不同。

5　结束语

本文提出的适合于 P2P MMOG 的包聚合机制是基于游戏交互阈值和聚合阈值的，能对游戏包进行聚合，降低了由数据包头部引起的开销，节省了带宽。以后的工作将进一步研究如何根据消息的发送频率以及消息类型进行消息聚合。

参考文献

[1] Kim J, Choi J. Traffic Characteristics of a Massively Multi-player Online Role Playing Game[C]//Proc. of the Int'l Conf. on Net Games. New York, USA: [s. n.], 2005.

[2] Chen Kuanta, Huang Chunying. An Empirical Evaluation of TCP Performance in Online Games[C]//Proc. of ACE 2006. Hollywood, CA, USA: [s. n.], 2006.

[3] Badia L, Fasolo E. Data Aggregation Algorithms for Sensor Networks with Geographic Information Awareness[C]//Proc. of WPMC06. San Diego, USA: [s. n.], 2006.

[4] Sangheon P, Choi J. Application Aware Data Aggregation in Wireless Sensor Networks[C]//Proc. of IEEE International Workshop on AWiN. [S. l.]: IEEE Press, 2005.