无线局域网 Sniff 技术研究

卜勇华　胡爱群　王兴建
（东南大学无线电系　东南大学信息安全研究中心　南京 210096）

Sniff Technology of Wireless LAN

BU Yong-Hua　HU Ai-Qun　WANG Xiang-Jian
(Research Center of Information Security, Southeast University, Nanjing, 210096 China)

Abstract　This paper researches the sniff technology of 802.11b wireless LAN. It describes the channel, topology, authentication and privacy of WLAN, points out the way to capture wireless data, then presents the analyse procedure of wireless frames. At last an actual frame is given.

Keywords　Wireless LAN(WLAN), IEEE802.11, Sniff

1. 引言

无线局域网(WLAN)为人们提供了一种便捷的网络接入方式，北京大运会上无线局域网的综合成功运用，使人们充分地认识到了无线局域网的高效和快捷。无线局域网可以和现有有线网实现无缝连接，本身更具有布局的简单性、灵活性，可以在移动中实现通信。美国 IDC 公布了全球有关无线 LAN LSI 市场的调查结果。调查表明，该市场在 2000 年～2005 年期间将以年平均 29%的增长率扩大。[1]

另一方面，无线局域网通过无线电波发送数据，无线节点间通过 CSMA/CA 机制共享一个频段，无线局域网就相当于一个大的 HUB 系统，在一个局部区域内的无线节点都能收到无线通信数据，因此无线局域网的监听比有线网络更为容易。而且由于处于 Sniff 机制下的无线节点无法发送数据，完全处于被动监听状态，对 Sniff 的探测也更为困难。

2. 802.11 WLAN 相关技术

1997 年，IEEE 确定 802.11 作为第一个国际认可的无线局域网标准。1999 年 9 月发布了 802.11b 标准。802.11b 标准描述了 OSI 模型的最底层(physical)以及一部分数据链路层(data link)协议。

WLAN 和我们熟悉的有线网如以太网的最大区别在于传送数据的介质不同。WLAN 信息的携带依赖于对无线电波的调制。802.11b 工作在 2.4GHz 频段。美国 2.4GHz 频段(2.40GHz 到 2.45GHz)的实现，分为 11 个可用的信道。为了限制干扰，实际使用小于信道带宽的一半。所有网络硬件设计为可以在任何一个信道上实现监听和发送，但为了直接通信，发送者和接收者必须在同一个信道上。对于 Sniff 来说，可以先进行信道扫描，确定存在通信的信道，然后固定在一个信道上进行监听。

在 IEEE802.11 中定义了几种常用的拓扑结构：基本服务组 BSS (Basic Service Set)；分布式系统服务 DSS (Distribution System Services)；扩展服务组 ESS (Extended Service Set)。

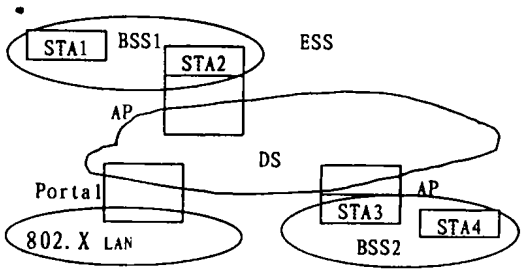

图 1　无线局域网拓扑图

基本服务组 BSS 是组成一个 802.11 局域网的最基本的单元。如图 1 中 BSS1 所示。一个基本服务组中可包含若干个站点 STA (Station)。在一个 BSS 中的站点之间可以直接通信。一个单独的 BSS 组成的网络(IBSS)是 IEEE802.11 中最基本的类型，它没有中枢链路基础结构，最少包含两台站点。一个基本服务组所能覆盖的区域受到环境和站点收发机特性

卜勇华　硕士，从事无线通信、网络安全的研究。胡爱群　博士，教授，博士生导师。王兴建　硕士，从事无线通信、网络安全的研究。

7　Tindell K W, Burns A, Wellings A J. Analysis of Hard Real-Time Control Applications. In: Proc. Real-Time Technology and Applications Symposium, May 1995. 240～249
8　Sprunt B, Sha L, Lehoczky J. Aperiodic task scheduling for hard real-time systems. The Journal of Real-Time Systems, 1989, 1: 27～60
9　Sha L, Rajkumar R, Lehoczky J P. Priority inheritance protocols: An approach to real-time synchronization. IEEE Transactions on computers, 1990, 39(9): 1175～1185
10　Han C C, Lin K J. Scheduling distance-constrained real-time tasks. In: Proc. IEEE Real-Time Systems Symposium, 1992. 300～308
11　Hsueh C, Lin K J, Fan N. Distributed pinwheel scheduling with end-to-end timing constraints. In: Proc. of IEEE Real-Time Systems Symposium, 1995. 171～181
12　Lin K-J, Herkert A. Jitter Control in Time-Triggered Systems. In: Proc. of the 29th IEEE annual Hawaii intl. conf. on system sciences, 1996
13　Strosnider J K, Lehoczky J P, Lui Sha. The deferrable server algorithm for enhanced aperiodic responsiveness in hard real-time environments, Computers, IEEE Transactions on, 1995, 41(1): 73～91
14　Mok A K. Fundamental design problems of distributed systems for hard real time environment: [Ph. D Thesis]. M. I. T., 1983
15　王志平，熊光泽，刘锦德. 1553B 实时网络流控问题研究. 计算机科学，1999, 26(7): 80～82

的限制。为了满足跨越 IBSS 范围限制的要求，我们可以把多个基本服务组通过分布式系统 DS (Distribution System) 连接起来。如图 1 中的 DS 所示。分布系统和基本服务组可以组成任意大小、复杂的无线网络，这样组成的网络称为扩展服务组(ESS)网络。如图 1 中 ESS 所示。

无线局域网通常有两种工作模式，Ad hoc 模式和 Infrastructure 模式。一般 IBSS 中的站点工作在 Ad hoc 模式下。在该模式下各站点之间两两直接通信，不需要第三者的介入。ESS 中站点工作在 Infrastructure 模式下。该模式需要 AP 的介入，任何通信都通过 AP 来转发。一个站点可以通过 AP 把数据发送给另一个站点，或者发送到 DS 中去。Ad hoc 模式及 Infrastructure 模式分别对数据截获没有影响，它们的区别体现在分析的结果中。

802.11bWLAN 的认证可以是开放式的或者是基于一个共享密钥知识。如果认证是开放式的，那么任何与标准兼容的设备都可以通过认证。如果认证是基于一个共享密钥的，那么要通过认证的设备必须证明它知道这个共享密钥。WEP (wired equivalent privacy)是 802.11b WLAN 协议中支持的可选数据加密技术。这种技术利用共享密钥以及作为初始化向量(IV)的一个伪随机数(PRN)来加密网络帧中的数据部分。802.11b WLAN 网络头部本身是不加密的，但是在 2001 年 8 月，有两位以色列魏兹曼研究所的专家与另一位思科公司的研究员在多伦多举行的密码会议上公布了他们破解 WEP 中的 RC4 加密技术，所以即使加密的数据也不是没有办法破解。

3. 无线局域网数据的截获

无线局域网如同一个广播系统，在 802.11b[2] WLAN 网络中，一个无线节点并不把数据帧直接发送给另一个节点，而是把目的地、接收工作站的地址放在帧的头部，然后把数据帧通过无线电信号发送。所有的无线网络节点平时处在监听模式，接收到一个数据帧后，利用 802.11[3] MAC 头的第一个地址来判断是不是应该处理这个帧。如果是，该节点就把该数据帧放入存储器，然后传递给协议栈下一层进行处理。如果消息接收准确，接收节点通常发送一个 ACK 进行确认。

通过这个过程我们可以发现，在进行物理地址的匹配判断之前，所有无线信号覆盖范围内的网络节点都能够从物理上接收到通信的数据帧。如果把这个判断的过程人为地去掉，就可以达到接收所有无线网络数据的目的。这个工作就是把网卡设成混杂模式(promiscuous mode)。有一点值得注意的是，和有线网络不同，处在混杂模式的无线节点是不能发送数据帧的。

现在生产无线网卡产品的公司已经很多，有 Symbol、Intermec、Cisco、Agere、Enterasys、3Com、Ericsson、Nokia 等。但很多对混杂模式支持不是太好，支持该模式的基本上都是基于 Intersil 公司 Prism2 芯片组的产品。其中 Cisco 公司的 Aironet PCM340 系列经过笔者试用是支持最好的。

4. WLAN 帧的剖析

这部分我们讨论各层 802.11 WLAN 帧头，以及帧中包含的网络数据协议的信息。典型的 802.11 帧把网络数据封装在物理层头里，里面是 MAC 层头及控制差错的 FCS 尾，如图 2 所示。所有版本的 802.11 都支持 802.2 标准的逻辑链路控制，即 LLC。物理导频、包开始分隔符和包结尾分隔符的字节一般是不截获的。

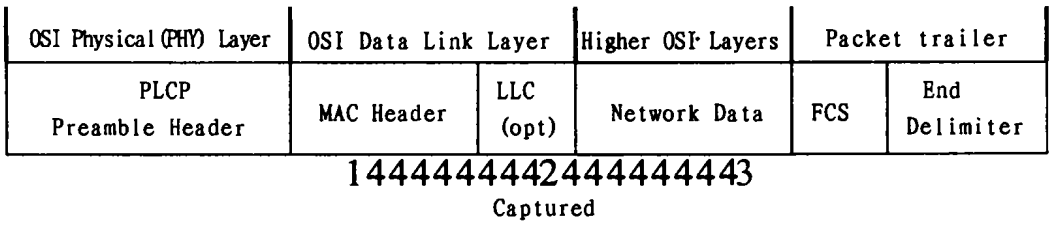

图 2　802.11b WLAN 帧结构

物理层头称为 PLCP(physical layer convergence protocol)，包括 PLCP 导频和 PLCP 头。PLCP 导频有两种形式：长形式和短形式。长形式导频以 16 字节的同步(一串逻辑 1)和 2 个字节的帧开始分隔符(SFD)开始。短形式只有 7 字节的同步(一串逻辑 0)和 2 个字节的 SFD。PLCP 头包含 4 个域：Signal、Service、Length 和 HEC(头差错校验)。Signal 域 1 字节长，定义了下面的 MAC 头和载荷传输的速率。可选的速率有 1,2,5.5,11Mbps。以 1Mbps 速率传送的帧可以不使用短形式导频。Service 域 1 字节长，包含有关传输的各种杂合信息。Bit7 是对 Length 的补充，说明那个域是否被包括。Bit3 定义了调制方式：0=CCK，1=PBCC。(CCK 是补码键控，PBCC 是帧二进制卷积编码。)Bit2 定义了发送工作站的发送频率和符号时钟是否从同一个振荡器而来，即是否锁定同步。该域的其它位保留给以后用。Length 域 2 字节长，定义了下面的 MAC 帧和帧载荷的长度。HEC 域是根据 PLCP 头本身计算出来的校验和。

802.11 MAC 头的具体格式取决于帧的类型：数据帧、网络管理帧或者控制帧。一个 802.11b WLAN 的数据帧如后面图 3 所示。管理帧和控制帧只有 4 个地址域中的 3 个。在帧体中根据特定的帧类型和子类型有固定或者可变长度的域也富含信息。

表 1　802.11MAC 头中的地址域

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	目的地址	源地址	BSS ID	N/A
0	1	目的地址	BSS ID	源地址	N/A
1	0	BSS ID	源地址	目的地址	N/A
1	1	接收者	发送者	目的地址	源地址

Frame Control 域 2 字节长，其内容分解在图 3 的下部，在下面进行解释。Duration ID 域 2 字节长，包含每个域的存在时间值。对于控制帧，该域还携带了发送工作站的关联标识(AID)。为了适应消息的中继可能性，和有线网不同，WLAN 有 4 个地址域而不是 2 个。什么域放哪个地址取决于帧是否通过分布式系统(DS)转发。Frame Control 域的 To DS 和

From DS 的取值决定了地址域的内容，如表 1 所示。Sequence Control 域 2 字节长，用来过滤重复的消息，例如因为前一个消息没有收到确认而重发的消息。

Frame Control 的位分解如下：开始的 2 个比特是协议版本，给出 802.11 的版本。Type 域(2 比特)和 Sub Type 域(4 比特)共同给出帧的类型和功能。To DS 和 From DS 域每个都是 1 比特，真设为 1，假设为 0，表明包是否发往还是从分布式系统接收来的。对于单个 BSS(基本服务集)中的消息，两个域都设为 0。如果当前帧还有分段，More Fragments 位就设为 1。

如果当前帧是以前帧的重传，Retry 位就设为 1。如果当前传送后，节点将进入节能模式，Power Management 位就设为 1；如果继续处于活动模式就设为 0。如果接入点有缓存的帧，等待传送给目的节点，More Data 位就设为 1。如果帧内容(载荷)用 WEP 算法加密了，WEP 位就设为 1。如果包必须严格按顺序处理，例如 IP 上的语音，Order 位就设为 1。

如同所有 IEEE802.x 家族局域网协议，802.11 使用 802.2 协议作为逻辑链路控制(LLC)层协议。802.2 头部，通常称为 LLC，包含有关帧协议类型的信息。802.2 头部是 3 字节或者 8 字节长。LLC 头的第一部分是 3 字节，含有 2 个 LSAP 值和 1 个 LSAP 命令。这些 LSAP 要么包含帧协议的信息，要么指向后面的可选 5 字节 SNAP 部分。如果指向 SNAP 部分，那么协议由这 5 字节的协议鉴别器或者 SNAP ID 来描述。

802.2 LLC 头的头 3 个字节如下：第 1 个字节是目的服务接入点(DSAP)，指定了目的协议。第 2 个字节是源服务接入点(SSAP)，指定了源协议，通常与 DSAP 的值相同。第 3 个字节是指明帧数据格式的控制字节。这个字节被绝大多数协议所忽略。如果 DSAP 和 SSAP 都设为 0xAA，该类型被解释为 IEEE 未定义的协议，而 LSAP 被称为子网访问协议 SNAP(SubNetwork Access Protocol)。

LLC 层以上就和有线网数据帧相同，这里不再论述。

5. 一个实际截获的 WLAN 帧

我们就在 802.11 WLAN 中实际截获的 HTTP 通信过程中的一帧数据作一个具体的分析。下面就是一个 HTTP 协议的 GET 命令帧，我们只取其 MAC 及 LLC 帧头。值得我们注意的一点是这里有个主机字节序及网络字节序的问题，就是两者对字节的存储顺序可能不同，具体细节请参看相关的网络书籍。

```
08 01 d5 00 00 04 25 02    00 31 00 04 25 01 00 63
00 d0 bc 4a ab 00 c0 68
aa aa 03 00 00 00 08 00 ……
```

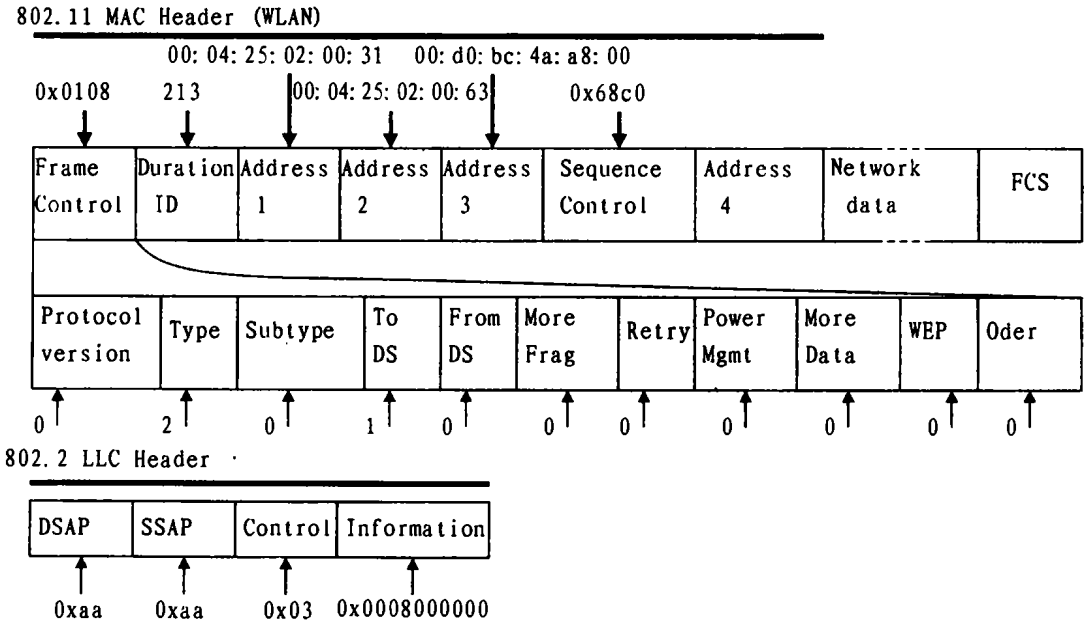

图 3 MAC、LLC 帧头及对应关系

按照我们前面的论述，有如图 3 所示的对应关系。这样，我们可以看出，在 MAC 层部分，该帧 802.11 协议的版本号是 0(默认值)，类型为数据帧，是从 WLAN 发送到分布式系统中去的，没有分段，不是重传，没有节能控制，没有缓存数据，没有加密，不要求按照严格的顺序进行处理。几个地址域分别表示了，网络标识为 00:04:25:02:00:31，源地址为 00:04:25:02:00:63，目的地址为 00:d0:bc:4a:a8:00。序列号为 1676。在 LLC 层部分，目的协议和源协议都为 0xaa，即为子网访问协议。Control 域显示为非标号的信息。Information 域显示为以太网封装(0x000000)，封装了 IP 协议(0x0800)。

参 考 文 献

1 Wireless LAN Management Forecast and Analysis, 2000-2005. http://www.idc.com, Document #: 25785, Publication Date: Oct. 2001

2 IEEE Std 802.11b-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band

3 ANSI/IEEE Std 802.11, 1999 Edition: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

4 ANSI/IEEE Std 802.2, 1998 Edition: Logical Link Control