# 802. 11 WLAN 通信安全的研究*

陈一天[1]，LAI NGAI MING[2]

(1. 广东科学技术职业学院，广东 广州 510640；2. 澳大利亚纽卡索大学 商业研究院，新南威尔士 卡莱根 NSW2308)

**摘　要**: 阐述了 802. 11 WLAN 目前使用的安全机制( SSID, MAC 地址过滤和 WEP 加密) 及其存在的漏洞和缺陷; 提出了一种新的信息安全措施——“捆绑认证”; 分析了 DSSS WLAN 的抗干扰性能; 导出 WLAN 在不同干扰情况时的处理增益。

**关键词**: WLAN; DSSS; 信息安全; 抗干扰; 处理增益

**中图法分类号**: TN925. 93; TP393. 08　　**文献标识码**: A　　**文章编号**: 1001-3695( 2006) 03-0123-03

# Communication Security of 802. 11 WLAN

CHEN Yi-tian[1], LAI NGAI MING[2]

*(1. Guangdong Vocational Institute of Science & Technology, Guangzhou 510640, China; 2. Newcastle Graduate School of Business, University of Newcastle, Callaghan NSW2308, Australia)*

**Abstract:** The security mechanisms of 802. 11 WLAN, including SSID, MAC filtration and WEP encoding, and their defects are discussed. A new security measure for 802. 11 WLAN named "binding authentication" is presented. The anti-interference functionality of DSSS WLAN is studied and its processing gain under various interferences is derived.

**Key words:** WLAN; DSSS; Security; Anti-interference; Processing Gain

## 1　引言

无线局域网( WLAN) 与有线网络相比较有许多相类似的地方, 但由于 WLAN 的特点( 如使用无线电波传输介质) , 使它的通信安全问题比有线网络复杂。对于向公众开放的 WLAN, 更为复杂。WLAN 的通信安全包括通信的信息安全( Security) , 以及通信的安全可靠。

在通信的信息安全方面, 由于 IEEE 802. 11 使用 SSID, MAC 地址过滤和 WEP 加密的安全机制存在严重的漏洞和缺陷, 必须采用新的安全措施, 或者在原有安全机制的基础之上进行改进和补充, 才能确保通信的信息安全。本文在下面提出的“捆绑认证”就属于后者。

802. 11 规定可以采用直接序列扩频( DSSS) 或跳频扩频( FHSS) 。DSSS 或 FHSS 不能视为安全措施的主要部分, 因为这两种技术原本都只是通信技术, 不能提供足够的抗恶意攻击的能力[1]。虽然如此, 由于 WLAN 信号在空间传输时可能会遭受各种干扰, 导致系统性能下降, 从而影响到通信的安全可靠。因此, 在 WLAN 的通信的安全可靠方面, 有必要提高其抗干扰能力。WLAN 采用 DSSS 比采用 FHSS, 不仅能提高传输速率, 也能提高抗干扰性能。

收稿日期: 2005-01-03; 修返日期: 2005-04-22

基金项目: 广东省科技计划资助项目( 2003C40406, 2004B40401002) ; 珠海市科技计划资助项目( PC20041103)

## 2　“捆绑认证”保障 WLAN 通信的信息安全

### 2.1　802.11 WLAN 现有安全机制的漏洞[1~4]

802. 11 提供了三种方式来规定运行在 WLAN 上的数据的安全性, 即服务群标识符( SSID) 的使用; 对 MAC 地址列表基站的验证; 有线等价保密 ( WEP) 加密的使用。文献[1 ~4] 介绍了这些安全机制存在的安全漏洞。

(1) 802. 11 的认证形同虚设。802. 11 默认的是开放系统认证, 这等于没有认证。共享密钥认证存在重大漏洞, 用以下的攻击方法可以通过认证: 当 AP 向请求者 STA 发送应答帧时, 把其中包含的质询信息记为 $P$, 把请求者 STA 响应的加密信息记为 $C = P$　PRKC, 攻击者记下 $P$ 和 $C$, 并做 $P$　$C =$ PRKC( $K$) 。以后攻击者便可以要求认证, 并用获得的 PRKC ( $K$) 成功通过认证。

(2) SSID 几乎不能保证安全。SSID 是一个可选项, 许多产品默认允许任何 SSID 都可以登录 AP。802. 11 允许 SSID 由 AP 通过信标帧定期以明文形式广播( 当然也允许关闭广播) 。SSID 是一个 BSS 中所有 STA 共享的秘密, STA 越多, 泄密的可能性就越大。有的产品允许 STA 发 Probe 帧, 向 AP 询问 SSID, 即使以上方法都不行, 攻击者还是可以窃听到合法用户登录时出示的未经加密的 SSID。

(3) MAC 地址过滤只能提供最简单的访问控制。攻击者可以通过无线网络的信息流来侦听有效的 MAC 地址, 并通过配置 WLAN 网卡也使用同样的 MAC 地址进行访问。

(4) WEP 算法存在巨大的安全漏洞。WEP 加密用来提供访问控制、数据加密和完整性检验等。但它是可选功能,大多数产品默认为关闭,因此把用户数据完全暴露在攻击者面前;WEP 对 RC4 的使用方式不正确,易受 IV Weakness 攻击而被完全恢复秘密密钥 SK;802.11 没有规定 WEP 中秘密密钥 SK 如产生和分发;SK 一旦产生,用户很少更新,且 SK 为所有用户共享,泄露的可能性很大;IV 空间太小;WEP 中的 CRC32 算法原本是通信中用于检查随机误码的,并不具备抗恶意攻击所需的消息认证功能。因此,802.11WLAN 的认证存在严重的安全隐患。

### 2.2 “捆绑认证”

随着攻击者技术的不断提高,上述安全机制存在的漏洞会使入侵更容易、威胁更大。因此,为了保证 WLAN 通信的信息安全,必须采取多项安全保障措施,并互相配合使用。目前,这方面的研究在国内外已有不少报导。本文提出了一种新的安全防范补充措施:“MAC、静态 IP 与用户口令的捆绑认证”(简称“捆绑认证”)。它基于上述原有的安全机制,并能大大提高网络的安全性能。其方法是:

(1) 按照 802.11 建立基本的 MAC 地址过滤表。首先把网络中所有网络适配器的 MAC 硬件地址,即固化地址(Burned-in)收集起来,建立一张 MAC 地址明细表,注明每个 MAC 地址所在的 AP 位置。然后通过设备厂商所提供的管理软件,在每一个 AP 的安全设置项中,建立合法用户的可信 MAC 地址表。该表组成了 802.11 所要求的 MAC 地址过滤器,可以实现 MAC 地址过滤。

(2) 设立无线静态 IP 地址。WLAN 利用了与以太网或令牌环访问方法相同的 TCP/IP 栈,其无线部分属于访问结构中的物理层和数据链路层。由于 TCP/IP 栈位于该结构的顶端,并且允许无缝集成到有线局域网中。也就是说,无线的 IP 地址与有线的 IP 地址在一定程度上等效,有线网络采用静态 IP 地址的安全策略在 WLAN 中仍然有用。因此,WLAN 完全可以效仿有线局域网的做法,为所有合法用户建立一张 IP 地址表进行过滤。对 WLAN 不同的是,在该表中要注明每个 IP 地址所在的 AP 的位置以及为每个 IP 指定其登录口令。

(3) MAC 地址、静态 IP 地址、用户口令的捆绑认证。首先在服务器中编写一个用户登录认证程序。然后将上述建立的 MAC 地址过滤表、静态 IP 地址和用户口令表在程序中分别建立对应的关联关系,将表中的 MAC, IP, 口令与所在的 AP 的地址关联起来。

当移动用户请求登录时,必须通过下面三个过程:

(1) 用户首先要通过它所在的 AP 的 SSID 认证、MAC 地址过滤、WEP 认证。

(2) 进入服务器的认证程序。服务器的认证程序先将请求者的口令, IP, MAC 读入寄存器,然后对 IP, MAC 所在 AP 与其所在的 AP 地址进行比较,如果比较结果为“真”时,进入下一个认证步骤。

(3) 只有当口令, IP, MAC 三者与关联表间相互一致时,方可登录。

### 2.3 “捆绑认证”的应用实例

“清新无线网”在已有的 SSID, MAC 地址过滤、WEP 加密安全机制基础之上,应用了“捆绑认证”。该网基于 802.11b,工作在 ISM2.4GHz 频段,采用 DSSS,传输速率为 1, 2, 5.5, 11Mbps(速率自动调节),点对点远程传输距离达 20km。下面介绍该网应用“捆绑认证”的具体做法:

(1) 分配 IP 地址与建立 IP 表。在该网中按 C 类地址对各子网进行地址分配,然后对所有用户(包括有线用户和无线漫游用户)指定了静态的 IP 和登录口令,并将该 IP、登录口令一一对应建立成一个用户 IP 及登录口令表。

(2) 建立 MAC 过滤表。对该网的所有用户,在登记用户时,读取其 MAC 地址,建立用户的 MAC 地址表,并将该地址写入所在的 AP 中,激活 AP 的 MAC 地址过滤器,启用 AP 的 MAC 地址过滤功能。

(3) 编写用户资料表“User”。根据以上(1)、(2),以及用户所在单位、网络中的权限建立用户资料表,该表中各个用户的各项数据资料相互绑定,并将该表分别存储在对应的子网服务器、主域服务器中,以供登录程序 COM 调用。

(4) 用户登录捆绑认证程序说明。在 VB 中建立一个 ActiveX 调用数据库连接和存储过程,该模块的项目名可命名为 Mycomm,类名为 Users。当用户登录时,认证程序读取登录请求者当前的 MAC, IP,以及用户口令,然后从服务器中取出其用户资料进行比较认证。当通过认证时方可登录。否则,拒绝登录,同时将该用户的当前登录资料记录到可疑用户监测数据库中,当该数据出现三次时,系统向管理员报警。

## 3 DSSS 保障 WLAN 通信的安全可靠[5]

电磁干扰会导致系统性能的下降,提高抗干扰能力是 WLAN 通信安全可靠的重要保障措施之一。WLAN 由于采用了 DSSS,因而提高了抗干扰性能。

### 3.1 DSSS 的 WLAN 的抗干扰性能

在高斯白噪声干扰的条件下,系统的信道容量 $C$(或称极限传输速率)由 Shannon 公式给出:

$$C = B\log_2(1 + S/N)$$

式中, $B$ 为信号带宽; $S$ 为信号平均功率; $N$ 为噪声功率。

由 Shannon 公式可以看出:

(1) 通过增加系统的信号带宽 $B$,或增加信噪比 $S/N$,可以增加信道容量 $C$,即提高了系统的信息传输速率。$C$ 与 $B$ 是正比关系, $B$ 与 $S/N$ 是对数关系,因此,为了可以增加信道容量,增加信噪比 $B$ 比增加 $S/N$ 更有效。

(2) 在给定的信道容量 $C$,即传输速率不变的条件下,频带宽度 $B$ 和信噪比 $S/N$ 可以互换,即可以通过增加信号的功率,降低对系统带宽的要求;或者通过增加带宽 $B$,降低系统对信噪比 $S/N$ 的要求,这表明宽带系统可以在较低的信噪比情况下传输信息,有较好的抗干扰性。

设白噪声的功率谱密度为 $n_0$,则噪声功率为 $N = n_0 B$,代入上式,得信道容量为

$$C = B\log_2\left(1 + \frac{S}{n_0 B}\right)$$

由上式可以看出,系统的 $B$, $n_0$, $S$ 一定时,信道容量 $C$ 就确定了。

DSSS 将要发送的信息用伪随机(PN)序列扩展到一个很

宽的频带上。在接收端,用与发送端扩展用的相同的伪随机序列对接收到的扩频信号进行相关处理,恢复出原来的信息。干扰信号由于与伪随机序列不相关,在接收端被扩展,使落入信号频带内的干扰信号功率大大降低,从而提高了系统输出的信噪(干扰)比。因此,在强干扰情况下(甚至信号被噪声淹没的情况下),仍然可以保持可靠的通信。

扩频系统的传输信号在扩频和解扩的处理过程中,提高了抗干扰性能,这种扩频处理得到的好处称为处理增益。对于 DSSS,处理增益定义为射频带宽($B_c$)与信息带宽($B_a$)的比值,或为伪随机码速率($R_c$)与信息速率($R_a$)的比值,也即 DSSS 的扩频倍数,即

$$G_P = \frac{B_c}{B_a} = \frac{R_c}{R_a}$$

上式是在一定条件下的近似。对于不同形式的干扰信号,基本符合上式的关系,但系统的处理增益有所不同。文献[5]给出各种表达式如下:

对噪声的系统处理增益为 $G_{P_n} = \frac{S_o/N_o}{S_i/N_i}$

对干扰的系统处理增益为 $G_{P_j} = \frac{S_o/J_o}{S_i/J_i}$

在实际中遇到的干扰主要有白噪声干扰或宽带噪声干扰、部分频带噪声干扰、单频及窄带干扰、脉冲干扰等。在实际应用中,应根据干扰情况的不同,确定 DSSS 的 WLAN 的处理增益和其他参数,使之达到可靠通信的目的。

### 3.2　加性白噪声干扰

WLAN 的信号在传输过程中,必然会受到噪声干扰,这种干扰一般为加性高斯白噪声(AWGN)或带限白噪声。设噪声的单边功率谱密度为 $n_0$,经混频后为一带限白噪声,带宽为扩频信号带宽 $B_c$,谱密度仍为 $n_0$,故相关器输入噪声功率为

$$N_i = n_0 B_c$$

相关器输出噪声功率为

$$N_o = \frac{1}{2\pi w_\alpha} G_{n'_I}(\omega)\,\mathrm{d}\omega$$

式中,$G_{n'_I}(\omega)$ 为相关解扩器输出端噪声的功率谱密度,$W_a = 2\pi B_a$。考虑到 $B_a << B_c$,只考虑 $f_I$ 附近的噪声功率,则 $G_{n'_I}(\omega)$ 近似为 $Kn_0$,其中 $K$ 为一与调制方式有关的常数。所以

$$N_o = \frac{1}{2\pi} K n_0 W_a = K n_0 B_a$$

由于解扩前后信息能量不变,因此白噪声干扰时的处理增益为

$$G_{P_n} = \frac{S_o/N_o}{S_i/N_i} = \frac{N_i}{N_o} = \frac{B_c}{KB_a} = \frac{G_P}{K}$$

由上式可知,对白噪声干扰的处理增益为 $G_P/K$。对 PSK 调制,$K = 0.903$;对 MSK 调制,$K = 0.995$。因此,在采用 PSK 调制或 MSK 调制时,白噪声干扰时的处理增益比 $G_P$ 稍大。

### 3.3　窄带干扰与单频干扰

设窄带干扰的中心频率为 $f_J$,带宽为 $B_J$,且 $f_J = f_I$,$B_J = B_a$。输入相关器的干扰功率为 $N_J$,功率谱密度为 $G_J(\omega)$,那么,解扩后干扰的输出功率为

$$N_{J_o} = \frac{1}{2\pi w_\alpha} G_J(\omega) \times G_C(\omega)\,\mathrm{d}\omega$$

由于 $G_J(\omega)$ 的带宽为 $B_a$,$G_C(\omega)$ 的带宽(主瓣带宽)为 $B_c$,而 $B_a << B_c$,因此 $G_J(\omega)$ 与 $G_C(\omega)$ 卷积后的带宽为 $B_c + B_a \approx B_c$,可以认为是将干扰的功率重新分配到 $B_c$ 频带上,且基本上是均匀的。对干扰而言,干扰功率在解扩后基本不变,则解扩后干扰的功率谱密度必然降低,与其扩展的频带的倍数成反比。所以

$$N_{J_o} = B_a \frac{1}{B_c} N_J$$

由上式得出抗窄带干扰的能力为

$$G_{P_J} = \frac{N_J}{N_{J_o}} = \frac{B_c}{B_a} = G_P$$

由上式可知,抗窄带干扰的能力可用处理增益 $G_P$ 来表示。由于单频干扰可以看成是窄带干扰的实例,因此,抗单频干扰的能力同样可用 $G_p$ 来表示。

### 3.4　正弦脉冲干扰

应用以上类似的方法,分析 DSSS 的 WLAN 抗正弦脉冲调制波干扰的性能。设 $f_J$ 为正弦脉冲调制波的中心频率。相关解扩器的输出信干比为

$$\frac{S_o}{N_{J_o}} = \frac{B_c}{B_a}\,\frac{S}{N_m} = \frac{B_c}{B_a}\,\frac{S_i D_m}{N_J}$$

式中,$N_m$ 为干扰峰值功率;$D_m$ 为占空比;$N_J$ 为干扰脉冲的平均功率。抗正弦脉冲干扰的能力为

$$G_{P_J} = \frac{S_o/N_{J_o}}{S_i/N_j} = \frac{B_c}{B_a} D_m = G_P D_m$$

由上式可知,$G_{P_J}$ 与 $G_P$ 成正比,其比例系数为占空比($D_m$)。

## 4　结束语

本文提出的“捆绑认证”是 802.11WLAN 在现有安全机制基础上补充的安全防范措施,已经在“清新无线网”中成功应用。其优点是简单、有效和可靠。

一个高的处理增益能增强信号的抗干扰能力。FCC 所允许的最小线性处理增益是 10,WLAN 大部分的商业产品低于 20 运行。IEEE 802.11 工作组已经设定它的最小处理增益是 11[6]。DSSS 的 WLAN 的抗干扰性能强,这些商业产品可以在一定程度上克服各种干扰,能保证通信的安全可靠。

**参考文献:**


[1] 曹秀英,耿嘉,沈平. 无线网络安全系统[M]. 北京: 电子工业出版社, 2004. 35-37.

[2] [美] Christian Barnes, *et al*. 无线网络安全防护[M]. 北京: 机械工业出版社, 2003. 165-172.

[3] 金纯,郑武,陈林星. 无线网络安全——技术与策略[M]. 北京: 电子工业出版社, 2004. 65-66.

[4] 刘乃安,李晓辉,张联峰, 等. 无线局域网(WLAN)——原理、技术与应用[M]. 西安: 西安电子科技大学出版社, 2004. 395-405.

[5] 曾兴雯,刘乃安,孙献璞. 扩展频谱通信及其多址技术[M]. 西安: 西安电子科技大学出版社, 2004. 97-103.

[6] [美] Jim Geier. 无线局域网[M]. 北京: 人民邮电出版社, 2001. 31.


**作者简介:**


陈一天(1943-),男,广东南海人,副教授,主要研究方向为计算机网络、通信工程;LAI NGAI MING(1963-),男,新加坡籍,高工,硕士研究生,主要研究方向为商业及计算机应用。