# 无线局域网中 WiFi 安全技术研究

高建华，鲁恩铭
( 湖南生物机电职业技术学院，湖南 长沙 410127)

摘 要 ：随着无线局域网技术的快速发展，WiFi 作为移动设备的无线联网技术应用越来越广泛。但无线局域网采用电磁波作为信息传播的载体，信息很容易被窃听或干扰，面临着严峻的网络安全问题。主要阐述了 WiFi 技术特点、WiFi 安全机制、WiFi 存在的问题及应用。

关键词 ：无线局域网 ；WiFi 安全机制 ；网络安全

## Research on WiFi Security Technology in WLAN

GAO Jian-hua,LU En-ming
*Hunan 410127 Hunan Biological and Electromechanical Polytechnic Changsha*

Abstract: with the rapid development of wireless LAN technology, WiFi as the application of wireless network technology and mobile devices more widely. Carrier but wireless LAN using the electromagnetic wave as the spread of information, the information is easily wiretapped or interference, facing serious problems of network security. This paper mainly expounds the problems and applications of WiFi technology, WiFi security mechanism, WiFi.

Key words: wireless local area network; WiFi security; network security



无线局域网（WLAN）因其灵活的移动能力和较高的数据速率被人们广泛地应用于各个领域。WiFi 技术作为 WLAN 技术家族中的重要成员，近年来发展迅速，已经应用到生活的各个方面。WiFi 技术是无线领域新兴的技术，它以其传输速度高、覆盖范围广的特点而日益受到人们关注，安全问题越来越受到重视。

## 1 WiFi 技术简介

### 1.1 WiFi 技术

WiFi 的英文全称是 Wireless Fidelity，中文名称为无线保真技术，它既是一种商业认证，也是一种无线联网技术。WiFi 与蓝牙技术一样同属于短距离无线技术，能将个人电脑、手持设备（如 PAD，手机）等终端以无线方式互相连接，所以俗称无线宽带。用户只要持有 WiFi 兼容的用户端装置，就可以在 WiFi 覆盖的区域内访问互联网，收发电子邮件。近年来，市场支持 UMA 等技术具备 WLAN 连接功能的智能手机越来越多，它们除了可以帮助 GSM/CDMA 移动通讯网通话外，还能在 WiFi 无线局域网覆盖的区域内，共享 PC 上网或 VoIP 通话。

### 1.2 WiFi 技术的特点

（1）无线电波覆盖范围广

基于蓝牙技术的电波覆盖范围非常小，半径大约只有 15m，而 WiFi 的半径可达 300m，适合办公室及单位楼层内部使用。

（2）组网简便

无线局域网的组建在硬件设备上的要求与有线相比，更加简洁方便，而且目前支持无线局域网的设备已经在市场上得到了广泛的普及，不同品牌的接入点

AP 以及客户网络接口之间在基本的服务层面上都是可以实现互操作的。WLAN 的规划可以随着用户的增加而逐步扩展，在初期根据用户的需要布置少量的点。当用户数量增加时，只需再增加几个 AP 设备，而不需要重新布线。而全球统一的 WiFi 标准使其与蜂窝载波技术不同，同一个 WiFi 用户可以在世界各个国家使用无线局域网服务。

（3）业务可集成性

由于 WiFi 技术在结构上与以太网完全一致，所以能够将 WLAN 集成到已有的宽带网络中，也能将已有的宽带业务应用到 WLAN 中。这样，就可以利用已有的宽带有线接入资源，迅速地部署 WLAN 网络，形成无缝覆盖。

（4）完全开放的频率使用段

无线局域网使用的 ISM 是全球开放的频率使用段，使得用户端无需任何许可就可以自由使用该频段上的服务。

## 2 WiFi 的安全机制

WiFi 安全性主要包括访问控制和加密两大部分，访问控制保证只有授权用户能访问敏感数据，加密保证只有正确的接收方才能理解数据。为了解决 WiFi 网络的安全问题，2003 年 WiFi 联盟推出了 WiFi 保护接入（Wi—Fi Protected Access，WPA）作为安全解决方案以满足日益增长的安全机制的市场需求。

### 2.1 WAP 技术

WAP 是无线应用协议（Wireless Application Protocol）的简称，是一种开放式的全球规范。有 WAP 和 WAP2 两个标准，是一种保护无线电脑网络（Wi—Fi）安全的系统。WAP 作为 IEEE802．11i 的一个子集，避开了 WEP 的众多弱点，可大大增强现有以及未来无线局域网系统数据保护的访问控制水平。WAP 可保证 WLAN 用户的数据受到保护，并且只有授权用户才可访问 WLAN 网络。

### 2.2 WiFi 网络安全策略

#### 2.2.1 加密方式

（1）TKIP 加密模式

WiFi 无线网络目前使用最广泛的加密模式是 WPA-PSK(TKIP) 和 WPA2-PSK(AES) 两种加密模式。TKIP 的含义为暂时密钥集成协议。TKIP 使用的仍然是 RC4 算法，但在原有的 WEP 密码认证引擎中添加了“信息包单加密功能”、“信息监测”、“具有序列功能的初始向量”和“密钥生成功能”等算法。

TKIP 是包裹在已有 WEP 密码外围的一层“外壳”，这种加密方式在尽可能使用 WEP 算法的同时消除了已知的 WEP 缺点。专门用于纠正 WEP 安全漏洞，实现无线传输数据的加密和完整性保护。但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 服务提供更加安全的保护。

（2）AES 加密模式

WPA2 放弃了 RC4 加密算法，使用 AES 算法进行加密，是比 TKIP 更加高级的加密技术。AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位（16 字节）分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换和替换输入数据。

#### 2.2.2 认证方式

WPA 要求用户必须提供某种形式的证据来证明它是合法用户，才能拥有对某些网络资源的访问

权，并且是强制性的。WPA 的认证分为两种 ：第一种采用 802.1x+EAP 的方式，用户提供认证所需的凭证，如用户名密码，通过特定的用户认证服务器来实现。另一种为 WPA 预共享密钥方式，要求在每个无线局域网节点（AP、STA 等）预先输入一个密钥，只要密钥吻合就可以获得无线局域网的访问权。

## 3 存在问题

WPA-PSK／WPA2-PSK（TKIP、AES）是目前主流的加密方式，但由于 TKIP 与 AES 子算法自身的问题。使得 WPA 也将面临着被彻底破解的威胁。目前使用的 IP 无线网络，存在一些不足，如带宽不高、覆盖半径小、切换时间长等，使得其不能很好地支持移动 VoIP 等实时性要求高的应用 ；并且无线网络系统对上层业务开发不开放，使得适合 IP 移动环境的业务难以开发。此前定位于家庭用户的 WLAN 产品在很多地方不能满足运营商在网络运营、维护上的要求。用户在使用无线网络时应该注意以下几点 ：

（1）对于自己搭建无线网络的用户，至少要进行一些最基本的安全配置，如隐藏 SSID，关闭 DHCP，设置 WEP 密钥，启用内部隔离等。

（2）如果安全要求再高一些，还可以启用非法 AP 监测，配置 MAC 过滤，启用 WPA／WPA2，建立 802．1x 端口认证。

（3）如果有更高的安全需求，那么可以选择的安全手段就更多，比如，使用定向天线，调整发射功率，把信号可能收敛在信任的范围之内 ；还可以将无线局域网视为 Internet 一样来防御，甚至在接口处部署入侵检测系统。

（4）如果您是企业用户，当您需要在热点区域使用无线网络时，如果认定网络不够安全，那么请尽量不要在此网络中提交或透露敏感信息，并尽量缩短在线的时间。

## 4 WiFi 的应用

由于 WiFi 的频段在世界范围内是无需任何电信运营执照的免费频段，因此，WLAN 无线设备提供了一个世界范围内可以使用的，费用低廉且数据带宽极高的无线空中接口。用户可以在 WiFi 覆盖区域内快速浏览网页，随时随地接听拨打电话。而其他一些基于 WLAN 的宽带数据应用，如流媒体、网络游戏等功能更是值得用户期待。WiFi 具有更大的覆盖范围和更高的传输速率，因此 WiFi 手机成为了目前移动通信业界的时尚潮流。现在 WiFi 的覆盖范围在国内越来越广泛了，宾馆，住宅区，飞机场之类的区域都有 WiFi 接口。在网络高速发展的时代，人们已经体验到了 WiFi 给我们带来的便利。我们坚信，WiFi 与 3G 的融合必定为我们开启一个全新的通信时代。

参考文献

[1] 盛仲飙 .WiFi 无线网络技术及安全性研究 [J]．电子设计工程，2012（16）:1-2.

[2] 凡星 , 刘培奇 . 无线局域网中 Wi-Fi 安全技术研究 [J]．电脑知识与技术，2012（7）:1-2.

[3] 王殊等 . 无线传感器网络的理论及应用 [M] . 北京：北京航空航天大学出版社，2007.

作者简介 :高建华（1970—）,女,湖南长沙人,系副主任,副教授，研究方向 :多媒体网络 ;鲁恩铭（1979—），男，湖南生物机电职业技术学院计算机信息技术系，讲师，研究方向 ：网络安全。

收稿日期 :2013-03-15