Wi-Fi 无线网络技术及安全性

随着互联网的迅速发展及普及，特别是各种便携式通信设备以及各种家用电器设备的迅速增加，人们在无线通信领域对短距离通信业务提出了更高的要求。

于是，许多短距离无线通信技术开始应运而生，以 802.11b 协议为基础的的 WIFI 技术便是其中的热点。被认为是无线宽带发展的新方向。

WIFI 是 IEEE 定义的一个无线网络通信的工业标准(IEEE 802.11)。也可以看作是 3G 技术的一种补充。WIFI 技术与蓝牙技术一样，同属于在办公室和家庭中使用的无线局域网通信技术。

WIFI 是一种短程无线传输技术，能够在数百英尺范围内支持互联网接入无线电信号。它的最大优点是传输速度较高，在信号较弱或有干扰的情况下，带宽可调整，有效地保障了网络的稳定性和可靠性。但是随着无线局域网应用领域的不断拓展，其安全问题也越来越受到重视。

1 WIFI 技术简介

1.1 WIFI 技术

WIFI(WireleSS Fidelity)俗称无线宽带，又叫 802.11b 标准，是 IEEE 定义的一个无线网络通信的工业标准。IEEE802.11b 标准是在 IEE E802.11 的基础上发展起来的，工作在 2.4 Hz 频段，最高传输率能够达到 11 Mbps。该技术是一种可以将个人电脑，手持设备等终端以无线方式互相连接的一种技术。目的是改善基于 IEEE802.1 标准的无限网络产品之间的互通性。

WIFI 局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

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 15 m，而 Wi—Fi 的半径可达 300 m，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。WIAN 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 WIAN 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。

1.2 WIFI 总体拓扑结构

WIFI 网络结构如图 1 所示。由 AP 和无线网卡组成。AP 一般称为网络桥接器或接入点，它是当作传统的有线局域网络与无线局域网络之间的桥梁，因此任何一台装有无线网卡的 PC 均可透过 AP 去分享有线局域网络甚至广域网络的资源，其工作原理相当于一个内置无线发射器的 HUB 或者是路由，而无线网卡则是负责接收由 AP 所发射信号的 CLJENT 端设备。

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 WPA 技术

WPA 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 WPA 和 WPA2 两个标准，是一种保护无线电脑网络(Wi—Fi)安全的系统。WPA 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。WPA 可保证 WIAN 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 4 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。主要体现在以下几点：

①静态 WEP 的密钥为手工配置，且一个服务区内的所有用户都共享同一把密钥。而 TKIP 的密钥为动态协商生成，每个传输的数据包都有一个与众不同的密钥。

②TKIP 将密钥的长度由 WEP 的 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，提高了 WEP 加密的安全性。

③TKIP 支持 MIC 认证(Message Integrity Cheek，信息完整性校验)和防止重放攻击功能。

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(permutations)和替换(substitutions)输入数据。

2.2.2 认证方式

WPA 给用户提供了一个完整的认证机制，AP 根据用户的认证结果决定是否允许其介入无线网络中；认证成功后可以根据多种方式动态地改变每个接入用户的加密密钥。对用户在无线中传输的数据报进行 MIC 编码，确保用户数据不会被其他用户更改。

WPA 有 2 种认证模式：

1)是使用 802.1x 协议进行认证，即就是 802.1x+=EPA 方式(工业级的，安全要求高的地方用。需要认证服务器)；

2)是预先共享密钥 PSK 模式(家庭用的，用在安全要求低的地方。不需要服务器)。AP 和客户端分享密钥的过程叫做 4 次握手，过程如图 2 所示。

1)客户端 SrrA 与无线接入点 AP 关联；

2)STA 需要向 AP 发送认证消息，在被授权以前，即使 STA 与 AP 始终关联，TSA 也不能够访问网络，只能继续向 AP 发送认证消息，经由远程认证拨号用户服务 AP 将认证消息发送给后端服务器来认证；

3)客户端 STA 利用 EAP 协议，通过 AP 的非受控端口向认证服务器提交身份凭证，认证服务器负责对 STA 进行身份验证；

4)如果 STA 未通过认证，客户端一直被阻止访问网络；如果认证成功，则认证服务器通知 AP 向该 STA 打开受控端口；

5)身份认证服务器利用 TKIP 协议自动将主配对密钥分发给 AP 和客户端 STA，主配对密钥基于每用户、每个 802.1x 的认证进程是惟一的；

6)STA 与 AP 再利用主配对密钥动态生成基于每数据包惟一的数据加密密钥；

7)利用该密钥对 STA 与 AP 之间的数据流进行加密。

这样就好象在两者之间建立了一条加密隧道，保证了空中数据传输的高安全性。

2.3 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。

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，千万不要忘记建立完善的安全管理制度并分发至员工。当您需要在热点区域使用无线网络时，您需要能够您所在网络的安全程度，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。

3 结论

随着无线局域网应用领域的不断拓展，安全问题越来越受到重视。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。

文中较详细地分析了 WIFI 网络的技术特点，对 WIFI 网络的安全性做了一定程度的探讨，给出了相应的结论。只有加强人为安全方面的控制技术的改进，才可更好加强 WIFI 安全性。