无线网络技术中的最新安全技术 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/259/2021_2022__E6_97_A0_E7_BA_BF_E7_BD_91_E7_c98_259415.htm 随着WLAN市场的蓬勃发展，其安全性问题日益突出，成为WLAN市场有序发展的主要瓶颈之一。国际标准组织对此曾提出了相关的技术建议，但引起了业界的争论。 我国在WLAN安全方面的研究进展比较迅速，日前，国家质检总局和国家标准化管理委员会联合发文，确定我国自主研发的WAPI技术为WLAN的强制性安全标准。 那么，要实现WLAN的安全性，到底有哪些技术手段呢？从定义来看，主要包括扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据；设置严密的用户口令及认证措施，防止非法用户入侵；设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容；采取网络隔离及网络认证措施等。 扩展频谱技术。扩展频谱技术在50年前第一次被军方公开介绍，它用来进行保密传输。从一开始它就设计成抗噪音、干扰、阻塞和未授权检测。扩展频储发送器用一个非常弱的功率信号在一个很宽的频率范围内发射出去，与窄带射频相反，它将所有的能量集中到一个单一的频点。扩展频谱的实现方式有多种，最常用的两种是直接序列和跳频序列。 用户认证和口令控制。即在无线网的站点上使用口令控制，当然未必局限于无线网。当前一些主要的网络操作系统和服务器均提供了包括口令管理在内的内建多级安全服务。口令应处于严格的控制之下并经常予以变更。由于WLAN的用户包括移动用户，而移动用户倾向于把他们的笔记本电脑移来移去，因此，严格的口令策略等于增加了

一个安全级别，它有助于确认网站是否正被合法的用户使用。 数据加密。假如用户数据要求极高的安全性，譬如说商用网或军用网上的数据，那么可能要采取一些特殊的措施。最后，也是最高级别的安全措施，就是在网络上整体使用加密产品。数据包中的数据在发送到局域网之前要用软件或硬件的方法进行加密。只有那些拥有正确密钥的站点才可以恢复、读取这些数据。如果需要全面的安全保障，加密是最好的方法。一些网络操作系统具有加密能力。基于每个用户或服务器、价位较低的第三方加密产品也可以胜任，有多种加密产品能够确保唯有授权用户可以进入网络、读取数据，而每个用户只须为此支付较低的费用。鉴于第三方加密软件开发商致力于加密事务，并可为用户提供最好的性能、质量、服务和技术支持，得到了WLAN供应商的积极支持。 WLAN还有些其它好的安全特性。首先，无线接入点会过滤那些对相关无线站点而言毫无用处的网络数据，这就意味着大部分有线网络数据根本不会以电波的形式发射出去。其次，无线网的节点和接入点有个与环境有关的转发范围限制，这个范围一般是几英尺。这使得窃听者必须处于节点或接入点的附近。最后，无线用户具有流动性，他们可能在一次上网时间内由一个接入点移动至另一个接入点，与之对应，他们进行网络通信所使用的跳频序列也会发生变化，这使得窃听几乎毫无可能。 总之，WLAN安全技术的发展，将极大促进无线网络的发展与应用，为安全的宽带无线网络通信时代的到来打下坚实的基础。 