 本文通过对Wi-Fi技术标准及其网络的分析，针对Wi-Fi网络所面临的网络安全问题进行了系统的探讨，并以此为基点从系统的角度提出了组建Wi-Fi网络时的一些安全策略。 一、Wi-Fi网络结构的安全性 (一)攻击方式 1.Wireless Dosattacks Dosattacks主要是通过洪水算法来阻塞网络，并导致网络合法用户无法使用该网络的服务。与有线网络相比，针对Wi-Fi网络的Dosattacks在网络的应用层和运输层的攻击没有什么特殊性，但由于无线通信介质的特殊属性使得Wi-Fi网络在数据链接层和物理层遭受的Dosattacks危害更为严重。常见的Wireless Dos attacks有以下几种方式。 (1)802.11b应用层攻击。攻击者通过向应用程序发送大量的合法请求来降低程序的服务效率，阻止其向其他合法用户提供服务。 (2)802.11b运输层攻击。在这一层，攻击者通过发送大量的链接请求来攻击主机的操作系统，降低其服务效率，常见的有SYN洪水攻击。 (3)802.11b网络层攻击。网络层的Dos攻击主要是针对效率较低的Wi-Fi网络，攻击者通过向网络发送大量的数据来攻击网络的脆弱结构，降低网络serverCPU的服务效率，常见的网络层Dos攻击是Pingflood攻击。但由于目前高速WLAN技术的成熟，这种攻击已经很少起作用了。 (4)802.11b数据链接层攻击。尽管WEP工作在该层，但鉴于WEP的脆弱性，甚至有些Wi-Fi网络不使用WEP，从而导致该层受到Dos攻击。另外不正确的使用DiversityAntennas也会使该层易受到Dos攻击。DiversityAntennas是一种用来避免多

径潮水效应的设备，它可以为Stations选择最强的信号来源以避免多径潮水效应，但同时这也将造成Wi-Fi网络易受到Dos攻击。只要攻击者将攻击设备的MAC地址改成Station的MAC地址，然后选择的Antenna的信号足够强，就会导致Station从其所在的Antenna上掉线。 (5)802.11b物理层攻击。鉴于Wi-Fi网络传播介质的特殊性，像有线网络的介质那样予以人为的保护是不可能的。由于Wi-Fi标准采用的是ISM公开的2.4GHz的波段，一旦攻击者利用工作在该波段的噪声设备发动足够强的噪音信号进行冲击，Wi-Fi网络的物理层将无法进行工作。 2.Illicituse 这种攻击主要有以下两种方式。 (1)盗用计费。非法使用AP的外部链接进入到Internet，盗用Wi-Fi网络的外部计费。 (2)隐蔽犯罪。为了隐藏身份，攻击者通过非法接入Wi-Fi网络AP，转而进入Internet采取攻击行为，从而使直接的责任落到了被寄生的AP身上，造成了Wi-Fi网络的麻烦。Illicituse风险对于有线LAN来说几乎不存在，但却会极大地危害到WLAN网络。这种攻击行为虽然无法造成Wi-Fi网络的系统问题，但攻击者可以通过这种方式非法使用Wi-Fi网络的外部链接，盗用Wi-Fi网络的外部计费，甚至掩盖其非法行为。 (二)网络维护方法 Wi-Fi网络的物理组网结构可分为两种：基础服务组和扩展服务组。 (1)基础服务组：网络由客户端(Stations)和接入点(APs)两部分组成，适宜小数据量网络的组建。如果仅仅是短期内进行连接组网，只需要有安装了Wi-FiCard的Stations即可实现端到端的Wi-Fi通信。 (2)扩展服务组：稳定的、完整的Wi-Fi网络由Stations、APs以及有线网络三部分组成，这种结构被称之为扩展服务组,通常是由BSS扩展而成的。 根据Wi-Fi网络的结构特点，针对上述有

关Wi-Fi网络本身的攻击方式，我们将从Stations安全、APs安全以及网络主干网安全三个方面对Wi-Fi网络可以采取的安全措施加以说明。 1.Stations安全 Stations安全涉及到整个Wi-Fi网络安全的核心。Stations中包含着大量的机密信息，如果攻击者攻破了Stations的安全措施，将给Wi-Fi网络带来巨大的损失。相关的安全措施主要有：(1)禁止Stations自己向外提供数据或者其他服务；(2)安装有效的杀毒软件，防止木马、蠕虫等病毒的侵入；(3)数据资源加密，评估自己的数据资源的重要级别，然后针对不同的安全等级对他们采取不同的加密措施和访问控制，这样既保证数据被合法用户采用，又可以保护数据不被恶意的攻击者窃取；(4)安装防火墙，防火墙可以是硬件也可以是软件，安装时应将防火墙放在网络入口处或需要保护的网段，保护网络的方式有，①数据包筛选：摒弃与规定不符的数据包。②代理服务：允许防火墙伪装成连接的终点，保护客户的IP地址。③状态检查：对比数据包的部分内容，对其进行筛选，比如IP地址、域名、协议、端口和内容等.(5)杜绝采取定期自动更新软件机制，这也是攻击者经常攻击的对象。 