 随着无线技术和网络技术的发展，无线网络正成为市场热点，其中无线局域网（WLAN）正广泛应用于大学校园、各类展览会、公司内部乃至家用网络等场合。但是，由于无线网络的特殊性，攻击者无须物理连线就可以对其进行攻击，使WLAN的安全问题显得尤为突出。对于大部分公司来说，WLAN通常置于防火墙后，黑客一旦攻破防火墙就能以此为跳板，攻击其他内部网络，使防火墙形同虚设。与此同时，由于WLAN国家标准WAPI的无限期推迟，IEEE 802.11网络仍将为市场的主角，但因其安全认证机制存在极大安全隐患，无疑让WLAN的安全状况雪上加霜。因此，采用入侵检测系统（IDSintrusion detection system）来加强WLAN的安全性将是一种很好的选择。尽管入侵检测技术在有线网络中已得到认可，但由于无线网络的特殊性，将其应用于WLAN尚需进一步研究，本文通过分析WLAN的特点，提出可以分别用于有接入点模式WLAN和移动自组网模式WLAN的两种入侵检测模型架构。 上面简单描述了WLAN的技术发展及安全现状。本文主要介绍入侵检测技术及其应用于WLAN时的特殊要点，给出两种应用于不同架构WLAN的入侵检测模型及其实用价值。需要说明的是，本文研究的入侵检测主要针对采用射频传输的IEEE802.11a/b/g WLAN，对其他类型的WLAN同样具有参考意义。 1、WLAN概述 1.1 WLAN的分类及其国内外发展现状 对于WLAN，可以用不同的标准进行分类。根据采用的传

播媒质，可分为光WLAN和射频WLAN。光WLAN采用红外线传输，不受其他通信信号的干扰，不会被穿透墙壁偷听，而早发射器的功耗非常低；但其覆盖范围小，漫射方式覆盖16m，仅适用于室内环境，最大传输速率只有4 Mbit/s，通常不能令用户满意。由于光WLAN传送距离和传送速率方面的局限，现在几乎所有的WLAN都采用另一种传输信号射频载波。射频载波使用无线电波进行数据传输，IEEE 802.11采用2.4GHz频段发送数据，通常以两种方式进行信号扩展，一种是跳频扩频（FHSS）方式，另一种是直接序列扩频（DSSS）方式。最高带宽前者为3 Mbit/s，后者为11Mbit/s，几乎所有的WLAN厂商都采用DSSS作为网络的传输技术。 根据WLAN的布局设计，通常分为基础结构模式WLAN和移动自组网模式WLAN两种。前者亦称合接入点（AP）模式，后者可称无接入点模式。分别如图1和图2所示。 图1 基础结构模式WLAN 图2 移动自组网模式WLAN 1.2 WLAN中的安全问题 WLAN的流行主要是由于它为使用者带来方便，然而正是这种便利性引出了有线网络中不存在的安全问题。比如，攻击者无须物理连线就可以连接网络，而且任何人都可以利用设备窃听到射频载波传输的广播数据包。因此，着重考虑的安全问题主要有： a）针对IEEE 802.11网络采用的有线等效保密协议（WEP）存在的漏洞，进行破解攻击。 b）恶意的媒体访问控制（MAC）地址伪装，这种攻击在有线网中同样存在。 C）对于含AP模式，攻击者只要接入非授权的假冒AP，就可登录欺骗合法用户。 d）攻击者可能对AP进行泛洪攻击，使AP拒绝服务，这是一种后果严重的攻击方式。此外，对移动自组网模式内的某个节点进行攻击，让它不停地提供服

务或进行数据包转发，使其能源耗尽而不能继续工作，通常称为能源消耗攻击。 e）在移动自组网模式的局域网内，可能存在恶意节点，恶意节点的存在对网络性能的影响很大。