 现在随着黑客技术的提高，无线局域网(WLANs)受到越来越多的威胁。配置无线基站(WAPs)的失误导致会话劫持以及拒绝服务攻击(DoS)都象瘟疫一般影响着无线局域网的安全。无线网络不但因为基于传统有线网络TCP/IP架构而受到攻击，还有可能受到基于电气和电子工程师协会 (IEEE) 发行802.11标准本身的安全问题而受到威胁。为了更好的检测和防御这些潜在的威胁，无线局域网也使用了一种入侵检测系统(IDS)来解决这个问题。以至于没有配置入侵检测系统的组织机构也开始考虑配置IDS的解决方案。这篇文章将为你讲述，为什么需要无线入侵检测系统，无线入侵检测系统的优缺点等问题。 来自无线局域网的安全 无线局域网容易受到各种各样的威胁。象802.11标准的加密方法和有线对等保密（Wired Equivalent Privacy）都很脆弱。在"Weaknesses in the Key Scheduling Algorithm of RC-4"文档里就说明了WEP key能在传输中通过暴力破解攻击。即使WEP加密被用于无线局域网中，黑客也能通过解密得到关键数据。 黑客通过欺骗（rogue）WAP得到关键数据。无线局域网的用户在不知情的情况下，以为自己通过很好的信号连入无线局域网，却不知已遭到黑客的监听了。随着低成本和易于配置造成了现在的无线局域网的流行，许多用户也可以在自己的传统局域网架设无线基站(WAPs)，随之而来的一些用户在网络上安装的后门程序，也造成了对黑客开放的不利环境。这正是没有配置入侵检测系统的组织机构开始考虑配

置IDS的解决方案的原因。或许架设无线基站的传统局域网用户也同样面临着遭到黑客的监听的威胁。 基于802.11标准的网络还有可能遭到拒绝服务攻击(DoS)的威胁，从而使得无线局域网难于工作。无线通讯由于受到一些物理上的威胁会造成信号衰减，这些威胁包括：树，建筑物，雷雨和山峰等破坏无线通讯的物体。象微波炉，无线电话也可能威胁基于802.11标准的无线网络。黑客通过无线基站发起的恶意的拒绝服务攻击(DoS)会造成系统重起。另外，黑客还能通过上文提到的欺骗WAP发送非法请求来干扰正常用户使用无线局域网。 另外一种威胁无线局域网的是ever-increasing pace。这种威胁确实存在，并可能导致大范围地破坏，这也正是让802.11标准越来越流行的原因。对于这种攻击，现在暂时还没有好的防御方法，但我们会在将来提出一个更好的解决方案。 入侵检测 入侵检测系统(IDS)通过分析网络中的传输数据来判断破坏系统和入侵事件。传统的入侵检测系统仅能检测和对破坏系统作出反应。如今，入侵检测系统已用于无线局域网，来监视分析用户的活动，判断入侵事件的类型，检测非法的网络行为，对异常的网络流量进行报警。无线入侵检测系统同传统的入侵检测系统类似。但无线入侵检测系统加入了一些无线局域网的检测和对破坏系统反应的特性。 无线入侵检测系统可以通过提供商来购买，为了发挥无线入侵检测系统的优良的性能，他们同时还提供无线入侵检测系统的解决方案。如今，在市面上的流行的无线入侵检测系统是Airdefense Rogue Watch 和Airdefense Guard。象一些无线入侵检测系统也得到了Linux 系统的支持。例如：自由软件开放源代码组织的Snort-Wireless 和WIDZ。 架构 无线入侵检测系统用于集中

式和分散式两种。集中式无线入侵检测系统通常用于连接单独的sensors，搜集数据并转发到存储和处理数据的中央系统中。分散式无线入侵检测系统通常包括多种设备来完成IDS的处理和报告功能。分散式无线入侵检测系统比较适合较小规模的无线局域网，因为它价格便宜和易于管理。当过多的sensors需要时有着数据处理sensors花费将被禁用。所以，多线程的处理和报告的sensors管理比集中式无线入侵检测系统花费更多的时间。 无线局域网通常被配置在一个相对大的场所。象这种情况，为了更好的接收信号，需要配置多个无线基站(WAPs)，在无线基站的位置上部署sensors，这样会提高信号的覆盖范围。由于这种物理架构，大多数的黑客行为将被检测到。另外的好处就是加强了同无线基站(WAPs)的距离，从而，能更好地定位黑客的详细地理位置。 物理回应 物理定位是无线入侵检测系统的一个重要的部分。针对802.11 的攻击经常在接近下很快地执行，因此对攻击的回应就是必然的了,象一些入侵检测系统的一些行为封锁非法的IP。就需要部署找出入侵者的IP,而且,一定要及时。不同于传统的局域网，黑客可以攻击的远程网络,无线局域网的入侵者就在本地。通过无线入侵检测系统就可以估算出入侵者的物理地址。通过802.11的sensor 数据分析找出受害者的,就可以更容易定位入侵者的地址。一旦确定攻击者的目标缩小，特别反映小组就拿出Kismet或Airopeek根据入侵检测系统提供的线索来迅速找出入侵者 策略执行 无线入侵检测系统不但能找出入侵者,它还能加强策略。通过使用强有力的策略,会使无线局域网更安全。 威胁检测 无线入侵检测系统不但能检测出攻击者的行为，还能检测到rogue WAPS，识别出未加密的802.11标准的数

据流量。为了更好的发现潜在的 WAP 目标，黑客通常使用扫描软件。Netstumbler 和Kismet这样的软件来。使用全球卫星定位系统（Global Positioning System ）来记录他们的地理位置。这些工具正因为许多网站对WAP的地理支持而变的流行起来。 比探测扫描更严重的是，无线入侵检测系统检测到的DoS攻击，DoS攻击在网络上非常普遍。DoS攻击都是因为建筑物阻挡造成信号衰减而发生的。黑客也喜欢对无线局域网进行DoS攻击。无线入侵检测系统能检测黑客的这种行为。象伪造合法用户进行泛洪攻击等。 除了上文的介绍，还有无线入侵检测系统还能检测到MAC地址欺骗。它是通过一种顺序分析，找出那些伪装WAP 的无线上网用户。 无线入侵检测系统的缺陷 虽然无线入侵检测系统有很多优点，但缺陷也是同时存在的。因为无线入侵检测系统毕竟是一门新技术。每个新技术在刚应用时都有一些bug，无线入侵检测系统或许也存在着这样的问题。随着无线入侵检测系统的飞速发展，关于这个问题也会慢慢解决。 结论 无线入侵检测系统未来将会成为无线局域网中的一个重要的部分。虽然无线入侵检测系统存在着一些缺陷，但总体上优大于劣。无线入侵检测系统能检测到的扫描，DoS攻击和其他的802.11的攻击，再加上强有力的安全策略，可以基本满足一个无线局域网的安全问题。随着无线局域网的快速发展，对无线局域网的攻击也越来越多，需要一个这样的系统也是非常必要的。 