加密协议拒绝无线网络遭遇非法攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/430/2021_2022__E5_8A_A0_E5_AF_86_E5_8D_8F_E8_c101_430315.htm 由于无线上网设备的价格正逐步“ 大众化 ”，无线上网设备的技术正逐步“ 成熟化 ”，越来越多的单位甚至是家庭都采用无线技术进行组网。在尽情享受无线网络给我们带来方便的同时，无线上网的安全现象也正被越来越多的用户所重视，那么如何才能让自己的无线网络拒绝遭遇非法攻击呢?本文下面就从无线网络的加密协议出发，来为各位朋友推荐一套非常可行的办法，帮助本地无线网络拒绝遭遇非法攻击! 走近无线加密协议 在使用无线加密协议保护本地无线网络远离非法攻击之前，我们不妨走近无线加密协议，撩开它的神秘面纱。大家知道，数据文件利用无线网络通道进行传输时与普通邮寄有点相同，倘若我们没有对数据文件进行加密就直接让其在无线网络中传输的话，那么本地无线网络周围的无线工作站都有可能将那些没有采取加密保护措施的数据文件截取下来，那么本地向外发送的数据文件就会将隐私信息泄露出去.倘若我们不希望这些数据文件对外泄露隐私信息时，那么我们在将目标数据文件传输出去之前就应该对它们先进行加密或采取其他安全保护措施，确保那些不知道解密方法的工作站用户无法访问具体的数据内容。 目前，在使用IEEE802.11b/g通信标准的无线网络中，为了提高网络的安全抵抗能力，普通用户广泛使用的无线网络加密协议主要包括WEP加密协议和WPA加密协议两种，其中WEP协议也称有线等效加密协议，这种无线通信协议常常是那些急于生产销售无线设备的厂家在比较

短的时间内拼凑而成的非正规无线加密通信标准，从目前来看这种无线网络加密协议还有相当多的安全漏洞存在，使用该加密协议的无线数据信息很容易遭到攻击.WPA协议也被称为Wi-Fi保护访问协议，这种加密协议一般是用来改进或替换有明显安全漏洞的WEP加密协议的，这种加密协议可以采用两种技术完成数据信息的加密传输目的，一种技术是临时密钥完整性技术，在该技术支持下WPA加密协议使用128位密钥，同时对每一个数据包来说单击一次鼠标操作就能达到改变密钥的目的，该加密技术可以兼容目前的无线硬件设备以及WEP加密协议.另外一种技术就是可扩展认证技术，WPA加密协议在这种技术支持下能为无线用户提供更多安全、灵活的网络访问功能，同时这种协议要比WEP协议更安全、更高级。 启用WEP协议进行普通加密 在无线网络中传输一些保密性要求不高的数据信息时，我们常常会选用WEP协议，这种协议基本被普通的家庭用户广泛使用。启用WEP协议保护本地无线网络的操作非常简单，现在本文就以DI-624 A型号的D-LINK无线路由器为例，来向各位详细介绍一下启用WEP协议的操作步骤： 首先从客户机中运行IE浏览器程序，并在浏览窗口中输入无线路由器设备默认的后台管理地址，之后正确输入管理员帐号名称以及密码，进入到该设备的后台管理页面，单击该页面中的“ 首页 ”选项卡，并在对应选项设置页面的左侧显示区域单击“ 无线网络 ”项目，在对应该项目的右侧列表区域，找到“ 安全方式 ”设置选项，并用鼠标单击该设置项旁边的下拉按钮，从弹出的下拉列表中我们可以看到DI-624 A型号的D-LINK无线路由器同时支持“ WEP ”加密协议和“ WPA ”加密协议. 选中最常用的“ WEP ”加密

协议，之后选择好合适的身份验证方式，一般无线路由器都为用户提供了共享密钥、自动选择以及开放系统这三个验证方式，为了有效保护无线网络传输信息的安全，我们应该在这里选用“ 共享密钥 ”验证方式。接着在“ WEP密码 ”文本框中正确输入合适的无线网络访问密码，再单击对应设置页面中的“ 执行 ”按钮，以便保存好上面的设置操作，最后将无线路由器设备重新启动一下，如此一来我们就在无线路由器中成功地本地无线网络进行了无线加密。 在无线路由器设备中启用了WEP密码协议后，我们还必须对无线网络的工作站进行正确地设置，才能保证它们顺利地访问到无线网络中的内容。在对普通工作站配置无线上网参数时，我们可以依次单击“ 开始 ”/“ 设置 ”/“ 网络连接 ”命令，在弹出的网络连接列表窗口中，用鼠标右键单击无线网卡设备对应的网络连接图标，从弹出的快捷菜单中执行“ 属性 ”命令，打开无线网络连接属性设置窗口.单击该窗口中的“ 无线网络配置 ”选项卡，在对应的选项设置页面中找到“ 首选网络 ”设置项，并从中找到目标无线网络节点，再单击对应页面中的“ 属性 ”按钮.之后进入到“ 关联 ”选项设置页面，选中该页面“ 网络验证 ”设置项处的“ 共享式 ”选项，最后单击“ 确定 ”按钮完成工作站无线上网参数的设置操作。 日后，本地无线网络中的无线工作站要访问无线网络时，只要双击对应工作站中的无线网卡设备，在随后出现的登录连接对话框中，正确输入之前设置好的加密密码，再单击登录对话框中的“ 确定 ”按钮，如此一来无线网络的访问与传输操作就安全了。即使本地无线网络附近的普通工作站截获到我们通过无线通道传输的数据信息，如果猜不中密码的话他们同样无法看

到其中的内容。 尽管WEP协议能够确保普通家庭用户进行无线访问的安全，可是该加密协议也有明显的缺憾，因为该协议的密钥固定，采用的算法强度不是很高，初始向量只有24位，一些非法用户可以借助AirSnort等专业工具就能轻松进行破解，所以对于保密性要求非常高的单位用户以及个人用户来说，使用WEP协议往往有一定的安全风险，此时他们不妨选用更加安全的WPA加密协议，来保护重要隐私信息的无线网络传输。 