doi:10.11959/j.issn.1000-436x.2016247

基于 BP 神经网络的 Wi-Fi 安全评价模型的研究

康海燕[1]，闫涵[1]，黄浩然[2]，孙璇[1]
（1. 北京信息科技大学信息安全系，北京 100192；2. 北京北大方正电子有限公司，北京 100085）

摘 要：提出了基于 BP 神经网络的 Wi-Fi 安全评价模型。首先，分析了大量 Wi-Fi 热点，选取与无线热点安全相关的信息源；其次，构造 BP 神经网络模型，并对权值进行调整，形成了有较高可信度的 Wi-Fi 安全性评估体系；最后，在 Android 平台上，设计了基于 BP 神经网络的 Wi-Fi 安全模型。实验证明，该安全评价模型能够对用户周边无线热点进行扫描及安全性评估，并提供不安全无线热点断开连接功能。

关键词：Wi-Fi；智能保护盾；Android；Wi-Fi 安全评价
中图分类号：TP312 **文献标识码**：A

Wi-Fi security evaluation model based on BP neural network

KANG Hai-yan[1], YAN Han[1], HUANG Hao-ran[2], SUN Xuan[1]
(1. Department of Information Security, Beijing Information Science and Technology University, Beijing 100192, China;
2. Beijing Founder Electronics Co. Ltd., Beijing 100085, China)

Abstract: A Wi-Fi security evaluation model was proposed based on BP neural network. Firstly a large number of Wi-Fi hotspots was analyzed, safety information sources about wireless hotspots were selected. Secondly, a model of BP neural network was constructed, the weights were adjusted, and the evaluation system for Wi-Fi safety was formed, which was higher credibility. Finally, on the Android flatform the application based on above theory was designed. A lot of experiments show the model is able to scan and evaluate the wireless hotspot around user. It can also provide the disconnect function on unsafe wireless hotspot.

Key words: Wi-Fi, intelligent protection shield, Android, Wi-Fi security evaluation

1 引言

如今越来越多的人使用手机、笔记本等移动终端通过 Wi-Fi 无线热点上网。然而，现有网络安全协议远没有达到人们期望的安全水平，用户在自己丝毫没有察觉的前提下，被别人窥探到网络浏览过程中录入的私人信息以及个人上网习惯，个人隐私将会受到极大的威胁，造成隐私泄露、个人财产的损失。如 2015 年的 3·15 晚会上，央视曝光了免费 Wi-Fi 的安全问题，并在晚会现场向民众演示了黑客通过 Wi-Fi 网络轻易截取用户的账号、密码等信息的全过程。正如《融 360：金融防骗手册》中提示的，因随意使用公共 Wi-Fi 而被黑客盗取个人信息已成为信用卡诈骗的新手段。据相关介绍，有部分不法分子专门在商场、咖啡厅等各公共场所使用黑客软件搭建免费的不明 Wi-Fi 连接，一旦用户在网页上进行登录，黑客将掌握用户的全部银行卡信息，轻而易举地进行盗刷。总之，这些安全漏洞如果被攻击者利用，就可以通过网络监听、密码攻击、会话劫持、脚本注入及后门植入等方式，窃取所有连接该 Wi-Fi 网络的用户信息。

因此，研发一套能够对非法无线热点进行识别及拦截的评价系统（Wi-Fi 保护盾）将会大大减小用户连接无线热点的安全风险。本文的主要贡献为

收稿日期：2016-09-28
基金项目：高水平人才交叉培养“实培计划”（科研）基金资助项目（No.5111623601）；国家自然科学基金资助项目（No.61370139）；北京市社会科学基金资助项目（No.15JGB099）
Foundation Items: High Level Talents Cross Training “Tranining Plan”(Rearch) Project (No.5111623601), The National Natural Science Foundation of China (No.61370139), Beijing Social Science Found (No.15JGB099)

以人工智能领域 BP 神经网络模型为基础，建立 Wi-Fi 评价体系，实现了实时检测和拦截的智能评价系统。

2　相关工作

早期的无线网络（ALOHA）在美国的夏威夷大学诞生，接着，国外一些设备商（如 Cisco、Lucent）也加入其中开始用于商用。为了 WLAN 的健康发展，1997 年国际电子电气工程师协会（IEEE）制定了 802.11 标准，随后分别发布了 802.11b、802.11a 和 802.11g 标准，标志着国外在该领域的研究日益成熟[1]。国内较早对 WLAN 进行研究的单位是西安电子科技大学、北京邮电大学、东南大学等。我国于 2003 年 5 月公布了自己具有自主知识产权的 WLAN 安全标准 WPAI，该标准通过了 IEEE 的认证和授权，这个标准代表了我国在 WLAN 安全领域取得的成就[2]。

Wi-Fi 又称无线宽带，是 IEEE 802.11b 的别称，是一种短程无线传输技术。Wi-Fi 的突出优势有 3 个，1) 无线电波的覆盖范围广，覆盖半径可达 100 m，而蓝牙只有 15 m；2) 传输速度快，可以达到 54 Mbit/s；3) 厂商进入的门槛低，不需网络布线接入。缺点是数据安全性能比蓝牙差，传输质量也有待改进[3]。

近几年内，无线访问节点（AP，access point），又称“热点”的数量飞速增加，Wi-Fi 已成为目前无线接入的主流标准，其安全性是决定无线局域网能否获得市场接受、用户信任的关键因素[4,5]。Wi-Fi 安全性主要包括加密和访问控制两大方面[6]。加密机制保证只有正确的接收者方能访问数据；访问控制机制保证只有被授权者方能访问敏感数据。为了解决 Wi-Fi 的安全问题，Wi-Fi 联盟于 2003 年推出 Wi-Fi 保护接入（WPA，Wi-Fi protected access）作为安全解决方案。目前，WPA2-PSK（AES）和 WPAPSK（TKIP）是 Wi-Fi 无线网络使用最广泛的 2 种加密模式。但是因为 WPA2-PSK（AES）和 WPAPSK（TKIP）的子算法的问题[7]，让 WPA 面临着被破解的危险。本文针对该问题设计了 Wi-Fi 安全评价模型。

3　BP 神经网络模型

1) 人工神经网络工作原理

人工神经网络工作原理[8]，通常是模拟人的神经网络结构和功能，先遵照预定的学习规则进行训练和学习，再进行准确、快速地识别和判断。

2) BP 神经网络模型工作原理

BP（back propagation）神经网络[9]，通常由信息的正向传播和误差的反向传播 2 个过程组成。其中包含输入层、隐含层和输出层。输入层各神经元负责接收来自外界的输入信息，并将其处理结果输出给隐含层（中间层）神经元；隐含层是 BP 神经网络模型的内部信息处理层，负责信息的变换处理，根据实际需求，隐含层可以规划为多隐含层或单隐含层过程，最后一个隐含层负责将隐含层处理结果传递給输出层各神经元；再经过输出层进一步处理后，实现一次学习的信息正向传播过程，最后，由输出层负责向外界传递处理结果。

处理结果输出与期望结果输出相差较大（超出阈值）时，启动误差的反向传播过程。误差首先按误差梯度下降的方式修正各层权值，通过输出层、隐含层和输入层逐层反传。信息的正向传播和误差的反向传播过程的不断循环，使各层权重逐步调整，一直到输出的误差可以接收，趋于合理。这个过程是 BP 神经网络训练学习的过程。

4　基于 BP 神经网络的 Wi-Fi 安全评价模型

为了测定扫描到的 Wi-Fi 热点是否安全，前提是有一套相对可靠的无线热点安全评估体系做保障[10,11]。因此，通过对大量 Wi-Fi 热点的分析并选用 BP 人工神经网络模型对初始权值进行调整，建立相对可靠的 Wi-Fi 安全评估体系。

4.1　Wi-Fi 安全评价指标体系的建立

1) 评价指标（参数）集的建立

评价 Wi-Fi 无线热点的安全性指标的选取关系到能否发挥评价的作用和功能。表 1[12]列出了 Google 官方文档中对于 android.net.wifi 包 ScanResult 类中扫描信息的说明。

2) 各评价指标（参数）的取值和标准化

本文中根据被评价 Wi-Fi 无线热点的具体情况取值，因各个指标反映 Wi-Fi 无线热点状况的不同方面，其衡量单位不同，各个指标的取值很难直接互相比较。所以，为了解决 BP 神经网络训练的收敛问题和直接比较各个指标的问题，首先对各指标进行标准化（统一化）处理，然后进行比较，标准化处理方法包括定量指标和定性指标的处理。

定量评价指标的标准化处理：由于各个指标反

映 Wi-Fi 无线热点状况的不同方面，需对其进行标准化处理，本文中设取值在 0~1 之间，处理步骤如下。

① 正向型参数标准化处理：$F_j=\dfrac{X_j-X_{j\min}}{X_{j\max}-X_{j\min}}$；

② 逆向型参数标准化处理：$F_j=1-(X_j-X_{j\min})\cdot(X_{j\max}-X_{j\min})$。

其中，j 是评价指标的数目，F_j 是标值为 X_j 的标准化值，$X_{j\max}$ 是预先确定的第 j 项指标的最大值，$X_{j\min}$ 是预先确定的第 j 项指标的最小值。

定性评价指标的标准化处理：为保持与定量指标之间的可比性，对于定性指标，采用专家打分法并将其统一化处理。

3) Wi-Fi 热点评价结果评语集的构建

按照 Wi-Fi 热点评价指标的选取特点和安全评价特性，本文将评价结果评语集设为 4 个等级（危险（很不安全），不安全，基本安全，安全），评语集等级解释如表 2 所示。

4.2 基于 BP 神经网络的 Wi-Fi 安全评价模型设计

4.2.1 模型构建

根据 BP 反向传播网络，如图 1 所示，Wi-Fi 安全评价模型包括输入层、隐含层、输出层。各层的构建如下。

1) 构建输入层。参照 BP 神经网络模型工作原理的设计规则，Wi-Fi 安全评价指标的个数和输入层神经元节点的个数相对应。本文的评价指标由 6 个二级指标构成，并且根据二级指标采集数据，同时，结合实际情况删除 timestamp、BSSID、SSID 指标评价模型的输入层，共有 3 个输入神经元节点 capabilities、frequency、level。

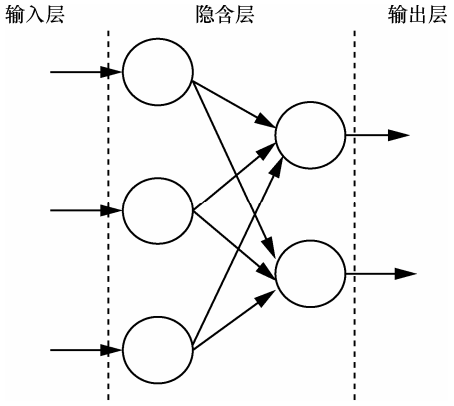


图 1 BP 反向传播示意

2) 构建隐含层。依据 Robert Hecht-Nielsen[13] 的理论，在闭区间的任何一个连续函数均能使用隐含层的 BP 神经网络来模拟。通常情况下，一个 3 层的 BP 网络能够实现任意的 M~N 维的映射处理。在实践中，大部分 BP 神经网络采用单隐含层，因此，本文采用了单隐含层的 BP 神经网络结构。

在构建 BP 神经网络时，网络隐含层节点数选择太多，使训练学习时间效率降低，学习效果未必最佳；节点数选择太少，网络的容错性和非线性映射性能变差。目前，常见隐含层节点数确定的经验公式有 $h=N+0.618(N-O)$或 $h=\ln N(N$ 表示输入节点个数，h 表示隐含层节点数，O 表示输出节点个数)，

表 1 Wi-Fi 无线热点检测信息描述

序号	类型	属性名	属性解释
1	字符型（public string）	接入点地址（BSSID）	接入点地址
2	字符型（public string）	Wi-Fi 名称（SSID）	网络名称
3	字符型（public string）	加密（capabilities）	接入点支持的身份验证、密钥管理和加密方案
4	整型（public int）	信号频率（frequency）	用户接入网络的信道频率（MHz）
5	整型（public int）	信号强度（level）	被测信号强度（dBm）
6	长整型（public long）	时间戳（timestamp）	同步时间戳（ms）

表 2 评语集等级说明

等级	说明
安全	Wi-Fi 网络具有较强的安全保障能力，应用安全
基本安全	Wi-Fi 网络具有一定的安全保障能力，应用基本安全
不安全	Wi-Fi 网络安全保障能力有限，应用存在安全隐患
危险（很不安全）	Wi-Fi 网络安全保障能力较差，应用存在安全形势严峻

本文使用 $h=\ln N$ 决定隐含层节点个数为 $h=1.584\ 9\approx 2$。

3) 构建输出层。本文的输出是对于目标 Wi-Fi 热点的安全评价结论，参照表 2 的设定，本文 BP 神经网络设计的输出层节点个数设置为 2。其中，输出结果(1,1)表示安全，(1,−1)表示基本安全，(−1,1)表示不安全，(−1,−1)表示危险。

根据每次测试样本实际输出值与期望值的误差，对于整个神经网络模型进行反向调整权值，直至测试样本实际输出值与期望值在合理范围内。

Wi-Fi 安全评价模型算法流程，如图 2 所示。假设循环次数为 30 就可以对权值进行较好的调整，学习率 *learn_rate*=0.1；激励函数 *stimulant_func*() 设定为若输出值大于等于 0，则返回 1；否则返回 −1；*t* 为控制变量。

4.2.2 评价体系的训练及学习

本文 BP 神经网络算法的自学习原则是信号强度越强、信号频率越高、加密措施越完善则安全系数越高。表 3 为训练 Wi-Fi 安全评估模型的 6 组训练样本，其中，前 4 组为刻意选取的不同安全等级的无线网络，本文采集到网络的基本属性（信号频率、强度、加密类型以及不同的输入节点等），下面是对表 3 取值的说明。

1) 信号频率的取值范围是 2 400~2 500 GHz，频率大小与安全性成正比，频率越大越安全。本文将频率分为 4 段：2 400~2 425 GHz 为很不安全，2 425~2 450 GHz 为不安全，2 450~2 475 GHz 为基本安全，2 475~2 500 GHz 为安全。

2) 信号强度的取值范围是−100~−50 dBm，强度大小与安全性成正比，强度越强越安全，其中，强度为 50 dBm 时最安全，强度为−100 dBm 时最不安全。本文将强度分为 4 段：−100~−87.5 dBm 为很不安全，−87.5~−75 dBm 为不安全，−75~−62.5 dBm 为基本安全，−62.5~−50 dBm 为安全。

3) 加密方式有 4 种，其中，ESS 代表加密方式为空，很不安全，WEP 为不安全，WPA 为基本安全，WPA2 为安全。

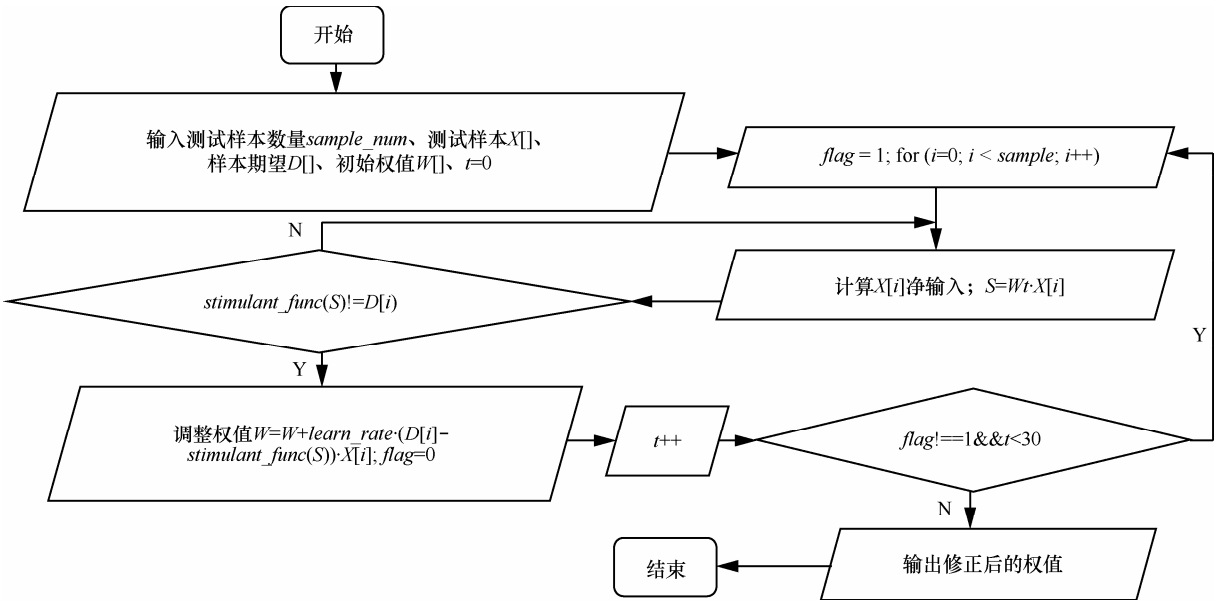


图 2　BP 神经网络算法流程

表 3　　Wi-Fi 安全评估模型训练样本

组别	频率/GHz	强度/dBm	加密类型	输入节点 1（权值）	输入节点 2（权值）	输入节点 3（权值）	期望输出
1	2 480	−55	WPA2	0.8	0.9	1	安全（1, 1）
2	2 467	−70	WPA	0.67	0.6	0.67	基本安全（1, −1）
3	2 438	−80	WEP	0.38	0.4	0.33	不安全（−1, 1）
4	2 412	−90	ESS	0.12	0.2	0	危险（−1, −1）
5	2 497	−76	WEP	0.97	0.48	0.33	安全（1, 1）
6	2 419	−62	WPA	0.19	0.76	0.67	基本安全（1, −1）

确定选择的属性及其特性后，为其赋予较为合适的权值，通过 BP 神经网络模型进行自学习，得出期望值。期望值分为 4 个等级，其中，（1, 1）为安全;（1, −1）为基本安全;（−1,1）为不安全;（−1, −1）为危险。最后，随机选取了 2 个无线网络进行测试，得到相应的网络期望值以及安全评级，验证了本文算法的可行性。

如表 3 所示，所有输入节点数据均进行标准化处理。测试中，通过以下 6 组安全等级不同的数据。使初始权值进行一个自学习过程，自动修改权值，最终使权值调整为一组相对可靠的数据。

① 信号频率安全、强度安全、加密方式安全的无线热点网络。

② 信号频率基本安全、强度基本安全、加密方式基本安全的无线热点网络。

③ 信号频率不安全、强度不安全、加密方式不安全的无线热点网络。

④ 信号频率很不安全、强度很不安全、加密方式很不安全的无线热点网络。

⑤ 信号频率安全、强度不安全、加密方式不安全的无线热点网络。

⑥ 频率很不安全、强度安全、加密方式基本安全的无线热点网络。

调整后的权值结合图 1 可表示为

(A,B,C,D,E,F)=(0.065 093, −0.042 88, 0.160 573, 0.103 907, −0.093 208, 0.065 143)

5 Wi-Fi 安全评价模型的实现

根据以上 Wi-Fi 安全评估体系的建立，在 Android 平台上，实现了基于 BP 神经网络的 Wi-Fi 安全评价模型（即 Wi-Fi 保护盾）。首先检测系统是否开启无线功能，开启无线后进入主界面，主要包括 2 个功能模块，“查看已连接的 Wi-Fi 网络信息”以及“扫描 Wi-Fi 网络热点”。“查看已连接的 Wi-Fi 网络信息”模块用于实现网络基本信息以及网络安全信息的查看，内容有网络 ID、SSID、接入点地址、物理地址、信号强度、连接速度、是否隐藏 SSID、加密方式、请求者状态等。“扫描 Wi-Fi 网络热点”模块用于扫描周边 Wi-Fi 网络热点并进行热点属性的罗列，内容有 Wi-Fi 名称、信号频率、信号强度、是否加密等。通过扫描到的属性结合 Wi-Fi 安全评估体系测评出扫描到的每一个无线热点的安全性。评价分为 4 个等级，包括安全、基本安全、不安全、危险，使用户直观地了解到自己所连接到的网络的安全性从而做出继续连接、选择其他无线网络的判断，具体实现如下。

1) 主界面

主界面由 2 个按钮（“查看已连接的 Wi-Fi 网络信息”和“扫描 Wi-Fi 网络热点”）组成，进入主界面后，首先检测本机是否开启 Wi-Fi 功能，如果没有开启，显示对话框询问用户是否开启 Wi-Fi 功能。

当单击“查看已连接的 Wi-Fi 网络信息”按钮时，显示当前已经连接的 Wi-Fi 网络信息，其中包括当前 Wi-Fi 的网络连接 ID 值、当前 Wi-Fi 的名称等，以对话框形式显示出来；当点击“扫描 Wi-Fi 网络热点”按钮时，显示扫描到的 Wi-Fi 网络热点。

2) 适配器

首先自定义适配器 my array adapter，继承 array adapter 适配器；然后对 my array adapter 适配器进行构造，定义一个 ScanResult 类型（主要用来描述已经检测出的接入点，包括接入点的地址、接入点的名称、身份认证、频率、信号强度等信息）的链表。用 LayoutInflater 来找 res/layout/下的 xml 布局文件，加载 ListView 列表项布局，通过 textview、findviewbyid 和 settext 对 Wi-Fi 热点名称、频率、信号强度和加密情况进行查询并将查询信息存入刚才定义的 ScanResult 类型的列表中。

3) Wi-Fi 热点信息查询界面

这个模块是为了 Wi-Fi 热点扫描，调用安卓的 API 进行工作，并且将扫描的热点以列表的形式展示出来，定义了触发事件，并且定义了单击事件，扫描得到结果的类型为 ScanResult，并以链表的方式存储，通过单击从而触发上述定义的事件，调用 gendialog 方法，生成一个对话框，显示出相应 Wi-Fi 热点对应的信息，Wi-Fi 名称、Wi-Fi 的接入点地址、Wi-Fi 的信号强度、Wi-Fi 的信号频率，Wi-Fi 的加密方式以及安全等级。其中，安全等级的确定，系统将采集到的网络属性进行加权计算，结合 BP 神经网络模型计算出的权值进行了网络安全性评估。

4) permission 设定

允许权限包括修改网络状态、修改 Wi-Fi 状态、允许应用访问网络上的信息等。

6 实验与分析

实验环境：Android 系统手机一部、网络共享软

表 4　　Wi-Fi 热点网络安全性评估结果

测试地点	Wi-Fi 名称	信号强度/ dBm	信号频率/GHz	加密	安全系数	准确性	准确率
图书馆	Hhr	−33	2.4	是	安全	√	83.3%
	TP-LINK_601	−45	2.4	是	安全	√	
	System Attack	−67	2.4	是	危险	×	
	Saierhao	−84	2.4	是	基本安全	√	
	TP-Link_7FF76	−88	2.4	是	基本安全	√	
	53637389	−85	2.4	是	基本安全	√	
实验楼	Hhr	−23	2.4	是	安全	√	80%
	teacher li lab	−60	2.4	是	基本安全	√	
	Bistu	−79	2.4	是	基本安全	√	
	CMCC-AUTO	−76	2.4	是	不安全	×	
	CMCC	−76	2.4	是	基本安全	√	

件（connectify）和评价系统（Wi-Fi 保护盾）。Wi-Fi 保护盾是运行在 Android2.3 以上环境中的 apk。

功能测试。在 Andriod 平台搭建 Wi-Fi 扫描应用软件，通过 connectify 软件开启无线热点，手机开启 Wi-Fi 保护盾后进行网络信息查看，本系统的用户操作界面清晰友好、功能明确，用户易于使用。

性能测试。选取了北京信息科技大学图书馆及实验楼进行了测评，测评结果如表 4 所示。

测试结果分析：1) 评价系统的准确率在 80% 以上，能够成功准确地扫描到用户周边的无线热点网络并给出无线网络的基本信息，随着训练样本数量的增加和评价指标的丰富（如用户满意度应被列入评价指标）将会更加准确；2) 检测出 Wi-Fi 网络的危险、不安全、基本安全、安全的等级，同时提供打开关闭无线网络的连接功能，能够满足用户对网络安全性评价的需要。

7　结束语

现今，用户对移动设备的依赖性越来越强，但在绝大多数用户普遍缺乏安全观念的背景下，用户应对央视曝光的免费 Wi-Fi 的安全问题提起足够的重视。针对目前 Wi-Fi 存在的安全隐患，提出了基于 BP 神经网络的 Wi-Fi 安全评价模型。提出了 Wi-Fi 保护盾的概念，设计了 Wi-Fi 安全评价体系、并在 Android 平台上研发了评价系统。实验证明该模型能够给出无线热点的安全性评价，能够比较准确地给出无线网络的安全评级，同时提供打开、关闭无线网络的连接按钮，方便用户在了解网络安全性后对网络进行断开、连接的操作。用户可以发现覆盖和连接问题，找到非授权或恶意的接入点，查看超负荷的网络和信道，以及检测干扰和验证安全设置，使用该模型，将使用户繁重而复杂的工作变得更高效、安全、轻松，确保用户的网络安全运行。

参考文献：

[1] 陈剑, 李贺武, 张晓岩, 等. IEEE 802.11n 中速率、模式及信道的联合自适应算法[J]. 软件学报, 2015, 26(1): 98-108.
CHEN J, LI H W, ZHANG X Y, et al. Joint adaptation algorithm of rate, mode and channel for IEEE 802.11n[J]. Journal of Software, 2015, 26(1): 98-108.

[2] 孙全富. 无线局域网数据加密和接入认证机制安全性研究[D]. 新疆大学, 2013.
SUN Q F. Research on data encryption and access authentication mechanism in wireless local area network security[D]. Xinjiang University, 2013.

[3] 叶彩红. 基于 IEEE802.11b 无线网络控制系统的建模与控制[D]. 燕山大学. 2010.
YE C H. Modeling and control for wireless networked control systems based on IEEE 802.11b[D]. Yanshan University, 2010.

[4] 周勇林. Wi-Fi 网络安全问题与防护建议[J]. 通信管理与技术, 2016, 03:19-20.
ZHOU Y L. Wi-Fi network security issues and protection recommendations[J]. Communication Management and Technology, 2016, 03:19-20.

[5] 任勇金. 浅谈 Wi-Fi 技术及其发展前景[J]. 信息通信, 2012, 5: 87
REN Y J. Talking about the Wi-Fi technology and its development prospects[J]. Information Communication, 2012, 5: 87.

[6] 盛仲飙. Wi-Fi 无线网络技术及安全性研究[J].电子设计工程, 2012, 20(16): 1-3.
SHENG Z B. Wi-Fi wireless network technology and security research of[J]. Electronic Design Engineering, 2012, 20 (16): 1-3.

[7] 高建华, 鲁恩铭. 无线局域网中 Wi-Fi 安全技术研究[J]. 计算机安全, 2013(4): 37-39.

GAO J H, LU E M. Research on Wi-Fi security technology in WLAN[J]. Computer Security 2013(4): 37-39.

[8] 王涛, 张丽莎, 高岩. 基于 BP 神经网络的改进型新奇检测技术诊断大跨度拱桥异常状态[J]. 北京理工大学学报, 2016, 36(2): 157-162.
WANG T, ZHANG L S, GAO Y. Abnormality identification of large-span arch bridge based on BP neural improved novelty detection technique[J]. Journal of Beijing Institute of Technology, 2016, 36 (2): 157-162

[9] 吕红芳, 顾幸生. 基于蚁群神经网络的两级信息融合算法[J]. 上海交通大学学报, 2016, 50(8): 1323-1330.
LV H F, GU X S. A two level information fusion algorithm based on ant colony neural network[J]. Journal of Shanghai Jiao Tong University, 2016, 50(8): 1323-1330.

[10] 陶跃, 田迎华. 多级可拓评价方法在网络安全评价中的应用[J]. 吉林大学学报(信息科学版), 2013, 31(1): 95-100.
TAO Y, TIAN Y H. Application of multilevel extension assessment method in network security evaluation[J]. Journal of Jilin University (Information Science Edition), 2013, 31(1): 95-100.

[11] 黄亮, 冯登国, 连一峰, 等. 一种基于多属性决策的 DDoS 防护措施遴选方法[J]. 软件学报, 2015, 7: 1742-1756.
HUANG L, FENG D G, LIAN Y F, et al. Method of DDoS countermeasure selection based on multi-attribute decision making[J]. Journal of Software, 2015, 7: 1742-1756.

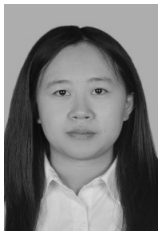
[12] Android.net.Wi-Fi 包 ScanResult 类中 Wi-Fi 无线热点信息[EB/OL]. http://developer.android.com.
Android.net.Wi-Fi package ScanResult class Wi-Fi wireless hotspot information[EB/OL]. http://developer.android.com.

[13] Robert Hecht-Nielsen. Theory of the back propagation neural network[C]//The International Joint Conference on Neural Networks. 1989: 593-605.

[14] 李健宏, 李广振. 网络安全综合评价方法的应用研究[J]. 计算机仿真, 2011, 28(7): 165-168.
LI J H, LI G Z. Application study on evaluation method of network security[J]. Computer Simulation, 2011, 28(7): 165-168.

作者简介：

康海燕（1971-），男，河北石家庄人，博士，北京信息科技大学教授、硕士生导师，主要研究方向为网络安全和隐私保护。



闫涵（1994-），女，北京人，主要研究方向为信息安全。

黄浩然（1992-），女，北京人，北京北大方正电子有限公司工程师，主要研究方向为个人信息安全隐私保护。

孙璇（1985-），女，山东淄博人，博士，北京信息科技大学讲师，主要研究方向为无线网络安全。