(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106330935 A
(43)申请公布日 2017.01.11

(21)申请号 201610782822.9

(22)申请日 2016.08.30

(71)申请人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 化存卿 翁祈桢 李维欣 姜赵晖 杨琨

(74)专利代理机构 上海旭诚知识产权代理有限公司 31220
代理人 郑立

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/08(2009.01)
H04W 12/12(2009.01)

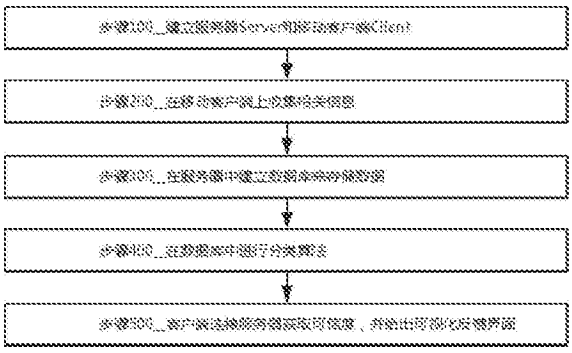
权利要求书1页 说明书8页 附图5页

(54)发明名称

一种钓鱼Wi-Fi的检测方法

(57)摘要

本发明公开一种钓鱼Wi-Fi的检测方法，涉及无线通讯安全领域，包括：使用服务器和移动客户端架构：移动客户端收集并上传用户周围Wi-Fi的Traceroute信息、地理位置信息，以及其他Wi-Fi连接属性信息至服务器；服务器使用数据库整合大量反馈信息，通过结合路由表和参数比对算法，以及数据挖掘的分类算法，给出Wi-Fi可信度评估，并基于客户端当前位置，利用地图给出相应可视化反馈界面，以供用户规避连接钓鱼Wi-Fi的风险。



CN 106330935 A

1.一种钓鱼Wi-Fi的检测方法,其特征在于,包括以下步骤:

步骤100、建立服务器和移动客户端,所述移动客户端被配置为采集AP的特征信息;所述服务器被配置为分析所述特征信息和Wi-Fi连接属性值,根据分类算法和比对算法对AP划分信用级别;

步骤200:在所述移动客户端被配置为通过调用Wi-Fi Manager的系统API来获取基本的Wi-Fi信息,使用Traceroute命令获取路由路径信息,和所述服务器进行数据传输;

步骤300:在所述服务器中建立数据库来存储数据;

步骤400:在所述数据库中运行分类算法,所述分类算法被配置为通过结合机器学习和基于规则的方法实现目标AP的可信度评估;

步骤500:所述移动客户端连接所述服务器获取可信度,并给出可视化反馈界面。

2.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤100中,所述特征信息包括SSID、MAC地址、信道、加密方式、用户接入、位置信息和Traceroute值。

3.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,所述在步骤100中,所述分类算法和比对算法包括数据库维护授权AP的列表、AP的用户接入历史记录、位置信息历史记录和Traceroute历史记录。

4.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤200中,所述基本的Wi-Fi信息包括路由器物理地址、SSID、加密方式、信号强度,MAC地址、接入设备经度、接入设备维度、数据获取时间戳。

5.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤200中,使用Traceroute命令获取路由路径信息的具体方法为在Android上使用Busy Box来模拟Linux系统。

6.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤300中,所述数据库包括用户列表、授权AP列表、AP特征表、用户接入表和AP信用级别表。

7.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤400中,所述机器学习被配置为将基本Wi-Fi连接信息作为输入项,将可信度评估作为输出项,其他视为暂时无法判断,结合神经网络的反向传播算法得出基础可信度参考值。

8.如权利要求7所述的钓鱼Wi-Fi的检测方法,其特征在于,将所述基础可信度参考值中标记为安全的Wi-Fi选出,根据基于规则的方法进行第二次判断。

9.如权利要求8所述的钓鱼Wi-Fi的检测方法,其特征在于,所述基于规则的方法包括冒名顶替、飘忽不定和路由异常的判断,其中所述路由异常的判断又由路径不变性检测、路径可探测性检测、外网连通性检测的结果结合之后给出;一旦目标Wi-Fi符合这些规则,则判定为危险。

10.如权利要求1所述的钓鱼Wi-Fi的检测方法,其特征在于,在步骤500中,进一步包括所述客户端向所述服务器申请周围Wi-Fi的可信度评估返回值;所述客户端将根据可信度评估返回值给当前Wi-Fi列表中的Wi-Fi打上标记;所述客户端利用地图SDK的位置信息将周围的Wi-Fi信息用图标标记在地图界面上;如果用户点击了具体的Wi-Fi,则会使用弹窗显示该Wi-Fi的具体信息,包括基本Wi-Fi连接属性和可信度评估,供用户来判断是否连接该Wi-Fi。

一种钓鱼Wi-Fi的检测方法

技术领域

[0001] 本发明涉及无线通讯安全领域，尤其涉及一种钓鱼Wi-Fi的检测方法。

背景技术

[0002] 随着智能手机，平板电脑等移动终端的普及，目前在很多的公共场所均有Wi-Fi覆盖，尤其是在机场，酒店，商场，咖啡厅等场所。越来越多的人会在这些公共场所选择连上免费Wi-Fi上网。在这些免费Wi-Fi的背后，其实暗藏被“钓鱼”的风险。恶意Wi-Fi会窃取用户的个人信息，轻则隐私信息泄露、遭遇恶意诈骗，重则网银账户密码会被盗取。此外，即使不窃取个人信息，用户也有遭遇中间人攻击的危险，譬如访问黑客伪造的网络地址，收看到黑客投放的广告为黑客带去非法利益。

[0003] 目前学术界提出了有监测网络活动的Wi-Fi网络混合式恶意AP保护框架，包含了分布式检测模块和中央检测模块；工业界也实现了企业级的无线入侵检测系统(WIDS)/无线入侵防御系统(WIPS)的Wi-Fi网络和无线安全解决方案:AirTight Management，提供给客户自动化的侦测、分类、定位、阻挡等功能。但前者要求在系统中布置特定的无线数据帧收集器和抢占引擎，后者则更为强调中央控制管理员对于恶意威胁对象的截断和对普通客户端的强力控制，两者更为适用于企业内部，而非目前公共Wi-Fi更为普遍出现的公共场所，因此针对这个场景，需要在基于前者的思想上，进行特殊的系统组件和交互信息设计。

[0004] 现有技术中，如北京奇虎科技有限公司的公开号为CN104955028A的申请公开一种钓鱼Wi-Fi识别方法，所述方法包括：接收并保存第一设备上传的信任Wi-Fi的连接属性信息；接收第二设备在连接未知Wi-Fi后、检测并上传的所述未知Wi-Fi的连接属性信息；判断所述未知Wi-Fi的连接属性信息与所述信任Wi-Fi的连接属性信息是否符合预设的匹配关系，若是，则确定所述未知Wi-Fi为钓鱼Wi-Fi。这个现有技术的缺点是要求预先有一个可信的第一设备来设置路由信息，对于路由表经常变化的区域、以及缺少可信认证的区域，实际效果不好。

[0005] 再如，中国科学院信息工程研究所的公开号为CN104580152A的申请公开了一种防护Wi-Fi钓鱼的保护方法：检测与终端连接的无线接入点AP的AP参数，并根据所述AP参数判断所述AP是否在预设的白名单中；若所述AP不在所述白名单中，则将所述白名单中第一个AP的AP参数修改为与终端连接的所述AP的AP参数，使得终端与所述AP断开连接；恢复所述第一个AP的AP参数，并重新关联所述终端至新的AP，直至所述AP为所述白名单中的AP。这个现有技术的缺点是依赖于预先设置可信AP，包括分配密码并将其加入白名单，不适合缺少可信认证的区域，以及无线热点分布情况经常更新变化的区域。

[0006] 再如哈尔滨工业大学的申请号为CN201510902314.5的申请公开了一种移动终端钓鱼Wi-Fi的检测与抵御方法，包括给予C/S架构的检测和防御钓鱼Wi-Fi方法的基本原理，各个模块之间的交互及数据流向、基于C/S架构的检测和防御钓鱼Wi-Fi系统客户端的具体工作流程以及各个模块之间的调用关系和数据库的构建过程以及本地知识库与云端知识库的交互方式。这个现有技术的缺点是仅仅针对Krama攻击所伪造的虚假响应包(Probe

Response)进行防御,对于具有主观欺骗性的钓鱼Wi-Fi,以及利用其他攻击原理的钓鱼Wi-Fi没有很好的应对措施。

发明内容

[0007] 有鉴于现有技术的上述缺陷,本发明所要解决的技术问题是如何对具有主观欺骗性的钓鱼Wi-Fi主动进行侦测和防御。

[0008] 为实现上述目的,本发明提供了一种钓鱼Wi-Fi的检测方法,包括以下步骤:

[0009] 步骤100、建立服务器和移动客户端,所述移动客户端被配置为采集AP的特征信息;所述服务器被配置为分析所述特征信息和Wi-Fi连接属性值,根据分类算法和比对算法对AP划分信用级别;

[0010] 步骤200:在所述移动客户端被配置为通过调用Wi-Fi Manager的系统API来获取基本的Wi-Fi信息,使用Traceroute命令获取路由路径信息,和所述服务器进行数据传输;

[0011] 步骤300:在所述服务器中建立数据库来存储数据;

[0012] 步骤400:在所述数据库中运行分类算法,所述分类算法被配置为通过结合机器学习和基于规则的方法实现目标AP的可信度评估;

[0013] 步骤500:所述移动客户端连接所述服务器获取可信度,并给出可视化反馈界面。

[0014] 进一步地,在步骤100中,所述特征信息包括SSID、MAC地址、信道、加密方式、用户接入、位置信息和Traceroute值。

[0015] 进一步地,所述在步骤100中,所述分类算法和比对算法包括数据库维护授权AP的列表、AP的用户接入历史记录、位置信息历史记录和Traceroute历史记录。

[0016] 进一步地,在步骤200中,所述基本的Wi-Fi信息包括路由器物理地址、SSID、加密方式、信号强度,MAC地址、接入设备经度、接入设备维度、数据获取时间戳。

[0017] 进一步地,在步骤200中,使用Traceroute命令获取路由路径信息的具体方法为在Android上使用Busy Box来模拟Linux系统。

[0018] 进一步地,在步骤300中,所述数据库包括用户列表、授权AP列表、AP特征表、用户接入表和AP信用级别表。

[0019] 进一步地,在步骤400中,所述机器学习被配置为将基本Wi-Fi连接信息作为输入项,将可信度评估作为输出项,其他视为暂时无法判断,结合神经网络的反向传播算法得出基础可信度参考值。

[0020] 进一步地,将所述基础可信度参考值中标记为安全的Wi-Fi选出,根据基于规则的方法进行第二次判断。

[0021] 进一步地,所述基于规则的方法包括冒名顶替、飘忽不定和路由异常的判断,其中所述路由异常的判断又由路径不变性检测、路径可探测性检测、外网连通性检测的结果结合之后给出;一旦目标Wi-Fi符合这些规则,则判定为危险。

[0022] 进一步地,在步骤500中,进一步包括所述客户端向所述服务器申请周围Wi-Fi的可信度评估返回值;所述客户端将根据可信度评估返回值给当前Wi-Fi列表中的Wi-Fi打上标记;所述客户端利用地图SDK的位置信息将周围的Wi-Fi信息用图标标记在地图界面上;如果用户点击了具体的Wi-Fi,则会使用弹窗显示该Wi-Fi的具体信息,包括基本Wi-Fi连接属性和可信度评估,供用户来判断是否连接该Wi-Fi。

[0023] 本发明可以应用在有众多Wi-Fi网络互相覆盖的公共场合中。在该场景下，用户可以通过手机移动端，查看周围的众多Wi-Fi。此时移动客户端会自动扫描周围Wi-Fi，将其数据上传至服务器，服务器结合本次数据以及之前的历史数据，通过机器学习和基于规则的判断，给出当前用户所看到的各个Wi-Fi的可信度评估，包括安全/可以/未知。客户端再从服务器中下载相关内容，不仅在列表界面进行标签提示，还可以通过地图界面来进行可视化的展示和选择操作，从而对当前环境下Wi-Fi的安全性能有一个直观的了解，知道应当警惕哪一些安全性可疑的Wi-Fi，连接安全可靠的Wi-Fi；甚至在有必要时，可以通过地图所给出的附近Wi-Fi的情况，步行前往可靠Wi-Fi的所在区域进行无线网络的接入。

[0024] 如图8所示，在公司使用无线网络也可能存在安全隐患。本发明也可以应用在使用无线网络进行网络覆盖的公司环境中。在该场景下，员工不仅可以通过上述功能，选择连接进入公司的合法AP，并且每一个员工的每一台移动设备，都可以成为公司的恶意AP检测器。一旦部署在公司的服务器发现有任何一名员工的移动设备上报了一个可疑的AP，即可立即通过其路径信息和基本Wi-Fi连接属性得知该AP的物理地址，加密方式等信息，并且通过员工手机的GPS以及相关信号强度，可以直接定位到可疑AP所在的具体位置，从而对恶意AP第一时间采取相应的处置，避免公司经受更大的经济损失、信息泄露和安全隐患。

[0025] 本发明提出的钓鱼Wi-Fi检测方法包括以下流程和具体操作，如图1所示：

[0026] 步骤100：建立服务器Server和移动客户端Client；

[0027] 步骤200：在移动客户端上收集相关信息；

[0028] 步骤300：在服务器中建立数据库来存储数据；

[0029] 步骤400：在数据库中运行分类算法；

[0030] 步骤500：客户端连接服务器获取可信度，并给出可视化反馈界面。

[0031] 其中，

[0032] 如图2所示，步骤100：建立服务器Server和移动客户端Client

[0033] 采用传统的Client/Server架构，移动客户端负责采集AP的特征信息(SSID，MAC地址，信道，加密方式，用户接入，位置信息，Traceroute等值)，服务器负责分析获得的AP的特征信息，通过数据库维护授权AP的列表，AP的用户接入历史记录，位置信息历史记录，Traceroute历史记录，再分析各种Wi-Fi连接属性值，做比对算法和分类算法，最终将AP划分为三个信用级别(Credit Level)：可信的(Trusted)、未知的(Unknown)、危险的(Risky)。

[0034] 服务器可以使用轻量级的Python Web框架web.py来实现，并且配以数据库来支持。服务器可以使用Url handler来处理用户的url请求，每个url都有对应的类来处理，通过正则表达式来匹配Url中的内容，并作为参数传递到对应的Get方法中。

[0035] 移动客户端的功能要求能够实现和服务器的及时通信，能够收集周围AP的特征信息，如SSID，MAC地址，Encryption，RSSI，TraceRoute，位置信息等，并且搭载在移动端平台上(比如Android)。

[0036] 服务器和移动客户端之间的交互，由于数据量较少(纯文本不包含多媒体数据)，可以使用Http协议来实现通信和传递数据。

[0037] 通过编写相关函数，使得服务器可以将客户端所发送的数据，按照一定格式存放入数据库。

[0038] 如图3所示，步骤200：在移动客户端上收集相关信息

[0039] 该系统的移动客户端，是基于Android平台进行开发；通过调用Wi-FiManager的系统API来获取基本的Wi-Fi信息；对于路由路径信息，则使用Traceroute命令；最后借由HttpClient模块，来和服务器进行简单的数据传输。

[0040] Android平台上，目前采用的最低兼容版本为Android 4.0，最高兼容版本为Android6.0，比较符合市面上一般手机的配置范围。使用Android Studio或Eclipse进行开发。

[0041] 对于基础的Wi-Fi连接信息，通过Wi-Fimanager即可实现。获取的信息包括但不限于：BSSID路由器物理地址，SSID路由器名称，Security加密方式，Signals信号强度，Mac Address接入设备物理地址，Longitude接入设备经度，Latitude接入设备维度，TimeString数据获取时间戳等。

[0042] 值得一提的是，对于路径路由信息的收集和利用，是本申请的一个重要创新点。Traceroute命令用于追踪数据包在网络上的传输时的全部路径，在Android上可以使用Busy Box来模拟Linux系统，从而实现该功能。

[0043] 在移动端上实现了Traceroute信息的收集之后，可以通过规则设定以及比对合法等方式来应用。具体判断步骤可以参见步骤400，数据库中进行分类算法。

[0044] 由于服务器和客户端交互的数据量较少(纯文字内容)，因此使用轻量级的HttpClient模块即可实现数据的上传和下载功能。

[0045] 如图4所示，步骤300：在服务器中建立数据库来存储数据

[0046] 使用MySQL数据库，与服务器建立连接，创建五个表(table)：

[0047] 1)用户列表(Users)：用户名(主键)，密码，Cookie；

[0048] 2)授权AP列表(AuthorizedAPs)：AP的MAC地址(主键)，SSID，位置，生产商；

[0049] 3)AP特征(APsFeatures)：AP的MAC地址(主键)，SSID，相邻AP，AP位置，信号强度，加密方式；

[0050] 4)用户接入(UserAccess)：客户端IP(主键)，AP的MAC地址，连接开始时间，连接结束时间；

[0051] 5)AP信用级别(APsCredit)：AP的MAC地址(主键)，SSID历史，位置历史，RouteTrace历史，加密方式历史，RTT评估，信用级别；

[0052] 如图5所示，步骤400：在数据库中运行分类算法

[0053] 该系统采用了分类算法，通过结合机器学习和基于规则的方法，来实现目标AP的可信度评估。首先需要导出数据的内容，使之以csv格式的文件进行保存。

[0054] 机器学习方法：将基本Wi-Fi连接信息，包括：BSSID路由器物理地址，SSID路由器名称，Security加密方式，Signals信号强度，Mac Address接入设备物理地址，Longitude接入设备经度，Latitude接入设备维度，TimeString数据获取时间戳等，作为输入项，将可信度评估Trust?作为输出项，Yes意为安全，No意为危险，其他视为暂时无法判断。通过神经网络的方式，结合Back Propagation算法，最终得出基础可信度参考值。

[0055] 随后将基础可信度参考值中，标记为安全的Wi-Fi选出，根据基于规则的方法进行第二次判断。如图6所示，通过经验总结出了三条规则：Imposter(冒名顶替)，Mobility(飘忽不定)，以及Traceroute Abnormality(路由异常)。其中路由异常又由三种检测的结果结合之后给出：Path Invariance(路径不变性检测)，Path Detectability(路径可探测性检

测),External Network Connectivity(外网连通性检测)。一旦目标Wi-Fi符合这些规则,则也可以判定为“危险”。

[0056] 冒名顶替:意思是在同一个位置所上报的AP数据中,如果有两个AP,其显示名称相同,但路由器的地址不同,则其中有可能会出现一个恶意AP冒用了一个合法AP的名字,从而起到欺骗的作用。由于我们认为,合法AP一般会长期地驻于某地,对于其路由器地址的上报次数会远远大于恶意AP,因此规则设定为,将路由器地址在数据库中出现的次数,远远少于另一个路由器地址的出现次数的那个路由,标记为“危险”。

[0057] 飘忽不定:意思是指同一个路由器地址的AP,如果它的地理位置经常在发生变化;或者在数据库中,出现两条及以上的,地理位置相距甚远的记录,那可以认为该AP是一个移动的人为搭建的AP,并非合法固定的AP,存在一定的风险。

[0058] 路径异常:由三种检测的结果结合之后给出:Path Invariance(路径不变性检测),Path Detectability(路径可探测性检测),External Network Connectivity(外网连通性检测)。

[0059] 路径不变性检测:指的是在同一个地点,通过固定合法路由连通外网,其经过的路径一般是固定的。然而如果连上某一个AP之后,路由表出现了重大的变化,或者在以往路由表的基础上增加了某一跳或某几跳,则可以认为该AP起到了一个流量过滤的作用,将部分网络流量从正常路由中截取出来,进行分析,并重新导向了一个旧有的结点。

[0060] 路径可探测性检测:恶意AP有时为了防止探测,会关闭对traceroute包的的回应,因而会出现大量或部分条目为“***”,以此来表示数据包超时而无法探测;合法固定AP则不太会有这种情况。

[0061] 外网连通性检测:若一个路由不设密码,且不经过认证界面(例如SJTU-WEB、McDonalds Wi-Fi、花生Wi-Fi等)就能自由连接上外网,则其为恶意AP的可能性较大。这一条规则是根据日常的经验所得出的。

[0062] 该系统通过这种机器学习和规则判断的方式,来实现对用户最大程度上的保护。最后将可信度记录回数据库,以供后续客户端向服务器申请查看时使用。

[0063] 如图7所示,步骤500:客户端连接服务器获取可信度,并给出可视化反馈界面

[0064] 首先客户端通过HttpClient,向服务器申请周围Wi-Fi的可信度评估返回值。

[0065] 随后客户端将根据Trust?的值(Yes或No或空缺),来给当前Wi-Fi列表中的Wi-Fi打上标记:安全/可疑/未知。

[0066] 同时客户端也利用百度地图SDK,向服务器申请周围位置区域的Wi-Fi信息,通过经度纬度等位置信息,将周围的Wi-Fi信息用图标标记在地图界面上,以供用户查看周围可使用的Wi-Fi。

[0067] 如果用户点击了具体的Wi-Fi,则会使用弹窗显示该Wi-Fi的具体信息,包括基本Wi-Fi连接属性和可信度评估,供用户来判断是否连接该Wi-Fi。

[0068] 本发明公开的一种钓鱼Wi-Fi检测方法,特别是涉及一种采用服务器和移动客户端进行交互,并约定传输并分析特定信息的方法。本发明技术方案带来的有益效果如下:

[0069] 1.不依赖于路由器生产厂家。不同于国内各大手机管家,对于钓鱼Wi-Fi的识别往往依赖于与路由器生产厂家进行合作,从而获得相应的可信路由器白名单,以此来识别当前Wi-Fi是否合法可信。相反,该系统更注重从用户角度出发,认为用户能安全连接上网的,

就是合法AP。

[0070] 2.可信判断不要求预先设置可信的AP。以往的技术会要求在当前区域中，有一个确认可信的AP作为判断基准，将其他AP的连接属性和路由信息与其比对，从而得出可信判断。然而，当用户进入一个完全陌生的场景，往往很难确定一个可信的AP，作出判断的基础也因此是薄弱的。该系统不要求这一点，它是通过众多用户提交的路由历史纪录和基本连接信息，基于统计找出最稳定最可靠的那个路由。

[0071] 3.简单的开放式系统。在某些企业中，为了实现无线安全，会对无线发射器和接入设备都进行严格的登记和控制，一旦不属于特定白名单中的设备出现，即会遭受封杀。同时有某些钓鱼Wi-Fi检测框架，对于客户端有着很高的设备要求，包括具有分布式检测模块，恶意AP抢占引擎、恶意AP检测引擎等。这两者都不利于在公共场合下，保障基于手机移动端和路由器所构建的Wi-Fi环境的安全推广。本专利则无论对于路由器和移动端都没有所谓的安全限制和控制，而是基于当前位置下的无线网络环境，来给出安全可靠的Wi-Fi连接指引。本产品并非旨在100％正确划分安全Wi-Fi和钓鱼Wi-Fi，而是希望在低成本低控制的框架下，尽可能地降低用户接入钓鱼Wi-Fi的安全风险。

[0072] 以下将结合附图对本发明的构思、具体结构及产生的技术效果作进一步说明，以充分地了解本发明的目的、特征和效果。

附图说明

[0073] 图1是本发明的一个较佳实施例的总体流程示意图；

[0074] 图2为本发明的一个较佳实施例的步骤100的具体流程示意图；

[0075] 图3为本发明的一个较佳实施例的步骤200的具体流程示意图；

[0076] 图4为本发明的一个较佳实施例的步骤300中数据库表属性列表；

[0077] 图5为本发明的一个较佳实施例的步骤400的具体流程示意图；

[0078] 图6为本发明的一个较佳实施例的步骤400中规则判断示意图；

[0079] 图7为本发明的一个较佳实施例的步骤500的具体流程示意图；

[0080] 图8为现有技术中公司使用无线网络可能存在的安全隐患示意图。

具体实施方式

[0081] 下面利用两个具体实施场景来阐述本发明所述的钓鱼Wi-Fi的检测方法。

[0082] 实施例一

[0083] 在公共场合，从零开始配置钓鱼Wi-Fi检测系统：

[0084] a.在目标公共场所附近，提前建立Wi-Fi信息收集处理服务器；

[0085] b.配置服务器，使之能够处理用户URL请求、HttpClient请求，并建立相应Wi-Fi信息数据库。

[0086] c.完成移动客户端的创建和基本配置，使之能够完成移动客户端和服务器之间的数据通信，以及周围Wi-Fi基本连接属性的收集工作；

[0087] d.在移动客户端上配置类似返回Traceroute结果的功能，使之可以自动收集当前Wi-Fi环境中，前往目标站点，途径路由器的IP地址信息，并将其上传至服务器。

[0088] e.尽可能地扩大目标公共场所中，移动客户端的使用者数量，例如要求来访者扫

二维码进行下载安装，或者在具有Wi-Fi模块的Android系统嵌入式设备中下载该应用等；

[0089] f.在较长的一段时间内，保持移动客户端的App应用有一定设备数的激活和使用，使它们以较短间隔性地对周围Wi-Fi进行扫描，并上传周围的Wi-Fi基本连接属性信息，以及Traceroute路径信息，用以添加进入服务器的数据库中，以供分析和判断。

[0090] g.在数据量较少的阶段，服务器将对Wi-Fi进行基于规则的可信度判断。主要利用到三条规则：冒名顶替、飘忽不定、路径异常，其中路径异常又包括三种检测方式：路径固定性检测、路径可探测性检测、外网连通性检测。三条规则中，一旦某一Wi-Fi满足其中一条，则很大程度上具有钓鱼Wi-Fi的嫌疑，服务器会将它在数据库中贴上相应的“危险”标签；

[0091] h.当服务器的数据库中，对于某个区域的Wi-Fi数据累计到一定数量之后，即可进行正确率较高的可信度判断。通过机器学习的方法，根据已有的数据，归纳出适合当前位置环境下，钓鱼Wi-Fi可能具有的一些特征，配以不同的权值，作为分类的依据。不过对于机器学习方法判定为“安全”的Wi-Fi，则会再次进行第(g)步基于规则的判断，确保其不会触碰到三条规则，否则依然会判定为“危险”Wi-Fi。

[0092] i.当用户在服务器成功实现判别功能之后，再启动移动客户端，则在上传数据之后，会向服务器周围Wi-Fi的可信度评估返回值，并给Wi-Fi列表中的Wi-Fi打上标记：安全/可疑/未知；

[0093] j.客户端点开地图界面时，则向服务器申请周围位置区域的Wi-Fi信息，通过经度纬度等位置信息，将周围的Wi-Fi信息用图标标记在地图界面上，以供用户查看周围可使用的Wi-Fi。如果用户点击了具体的Wi-Fi，则会使用弹窗显示该Wi-Fi的具体信息，包括基本Wi-Fi连接属性和可信度评估，供用户来判断是否连接该Wi-Fi。

[0094] 实施例二

[0095] 在公司现有的无线网络监管环境下，添加恶意AP检测系统：

[0096] a.在公司现有无线网络的环境下，向服务器中添加AP信息收集处理模块，使之能够处理用户URL请求、HttpClient请求，并建立相应AP信息数据库。

[0097] b.在公司现有的移动客户端中添加配置，使之能够完成移动客户端和AP信息收集处理模块之间的数据通信，以及周围AP基本属性的收集工作；

[0098] c.在移动客户端上配置类似返回Traceroute结果的功能，使之可以自动收集当前无线网络环境中，前往目标站点，途径路由器的IP地址信息，并将其上传至服务器。

[0099] d.在当前公司无线网络环境下，尽可能地扩大移动客户端的使用者数量，例如要求员工的PDA中更新添加相应应用，或者在原有的无线检测设备中添加该应用等；

[0100] e.保持该系统的长时间运行，保证移动客户端的App应用有一定设备数的激活和使用，使它们以较短间隔性地对周围AP进行扫描，并上传周围的AP基本属性信息，以及Traceroute路径信息，用以添加进入服务器的数据库中，以供分析和判断。

[0101] f.在数据量较少的阶段，服务器将对AP进行基于规则的可信度判断。主要利用到三条规则：冒名顶替、飘忽不定、路径异常，其中路径异常又包括三种检测方式：路径固定性检测、路径可探测性检测、外网连通性检测。三条规则中，一旦某一AP满足其中一条，则很大程度上具有恶意AP的嫌疑，服务器会将它在数据库中贴上相应的“危险”标签，并且及时发送警报给无线安全管理部门。

[0102] g.当服务器的数据库中，对于某个区域的AP数据累计到一定数量之后，即可进行

正确率较高的可信度判断。通过机器学习的方法，根据已有的数据，归纳出适合当前位置环境下，恶意AP可能具有的一些特征，配以不同的权值，作为分类的依据。不过对于机器学习方法判定为“安全”的AP，则会再次进行第(f)步基于规则的判断，确保其不会触碰到三条规则，否则依然会判定为“危险”的恶意AP，并且及时发送警报给无线安全管理部门。

[0103] h.当用户在服务器成功实现判别功能之后，再启动移动客户端，则在上传数据之后，会向服务器周围AP的可信度评估返回值，并给AP列表中的AP打上标记：安全/可疑/未知；

[0104] i.客户端点开地图界面时，则向服务器申请周围位置区域的AP信息，通过经度纬度等位置信息，将周围的AP信息用图标标记在地图界面上，以供用户查看周围可使用的AP。如果用户点击了具体的AP，则会使用弹窗显示该AP的具体信息，包括基本AP连接属性和可信度评估，供用户来判断是否连接该AP。

[0105] j.同时在服务器端，也配置相应的AP列表视图和可视化界面，使得网络管理员可以随时通过各种展现方式，监控当前无线网络环境中，是否出现了恶意AP，以及是否存在信息泄露和安全隐患的风险。

[0106] 以上详细描述了本发明的较佳具体实施例。应当理解，本领域的普通技术无需创造性劳动就可以根据本发明的构思作出诸多修改和变化。因此，凡本技术领域中技术人员依本发明的构思在现有技术的基础上通过逻辑分析、推理或者有限的实验可以得到的技术方案，皆应在由权利要求书所确定的保护范围内。

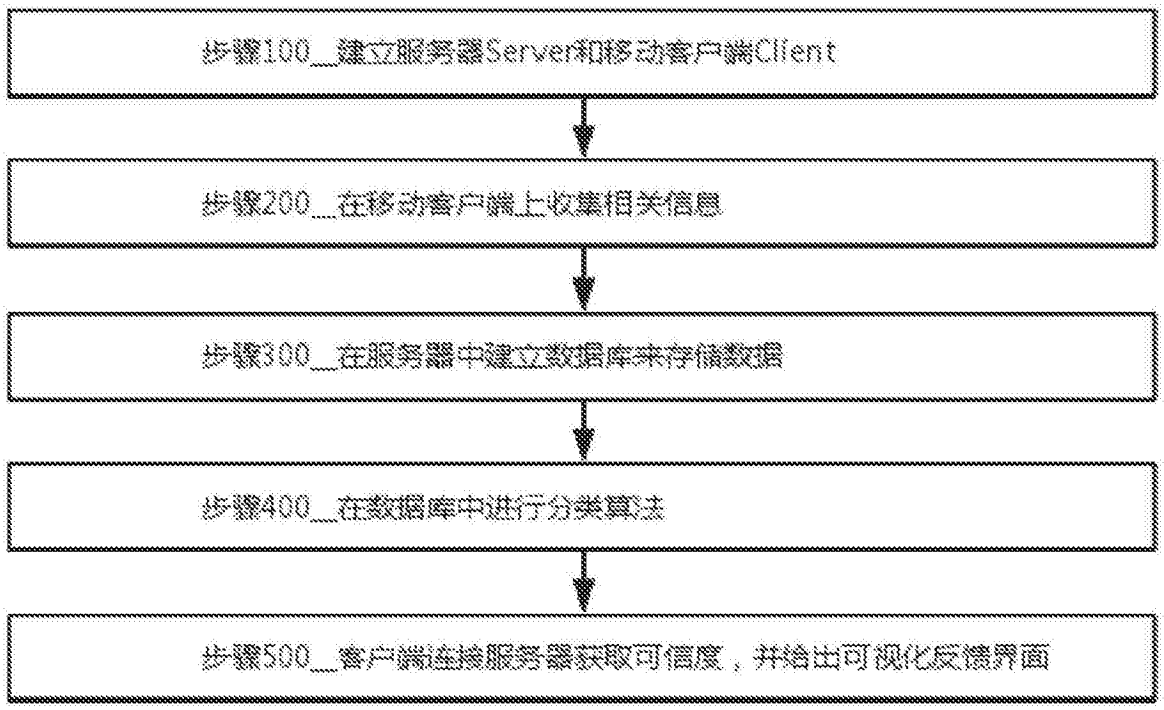

步骤100__建立服务器Server和移动客户端Client
步骤200__在移动客户端上收集相关信息
步骤300__在服务器中建立数据库来存储数据
步骤400__在数据库中进行分类算法
步骤500__客户端连接服务器获取可信度，并给出可视化反馈界面

图1

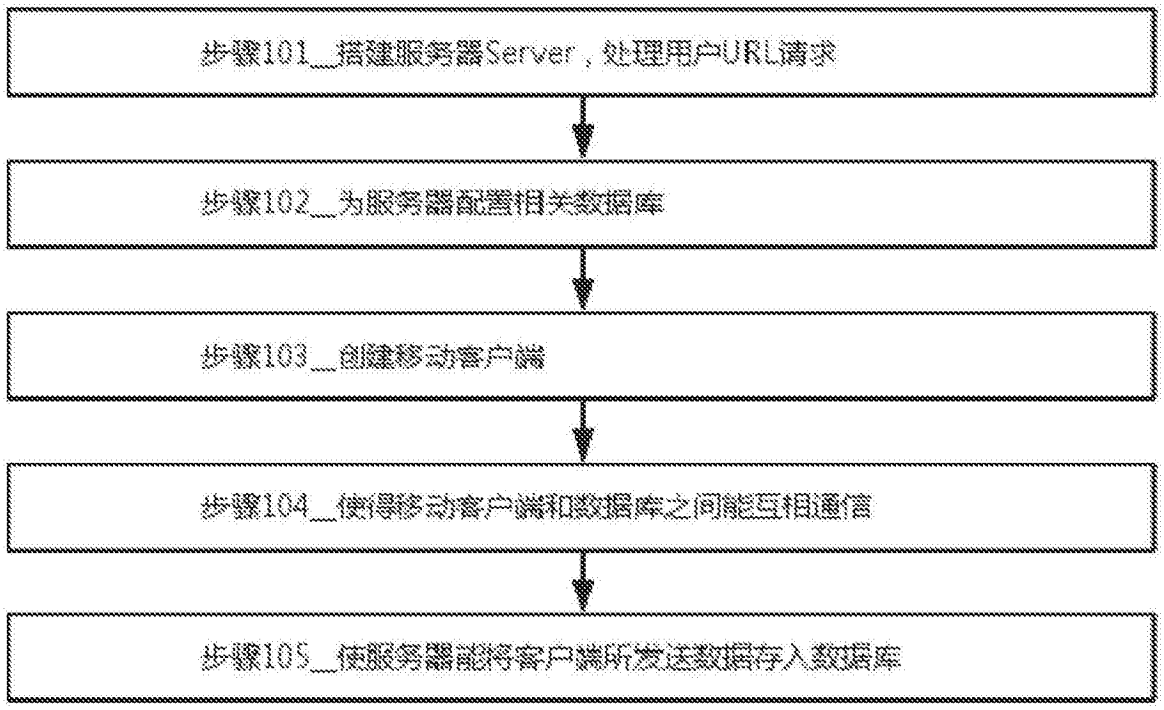

步骤101__搭建服务器Server，处理用户URL请求
步骤102__为服务器配置相关数据库
步骤103__创建移动客户端
步骤104__使得移动客户端和数据库之间能互相通信
步骤105__使服务器能将客户端所关注数据存入数据库

图2

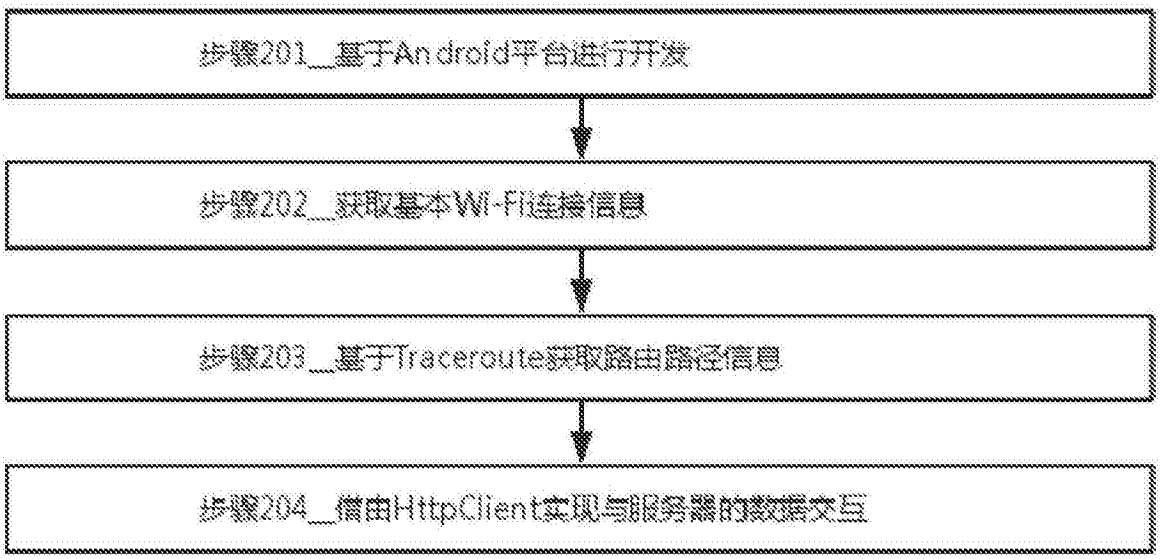

步骤201_基于Android平台进行开发
步骤202_获取基本Wi-Fi连接信息
步骤203_基于Traceroute获取路由路径信息
步骤204_借由HttpClient实现与服务器的数据交互

图3

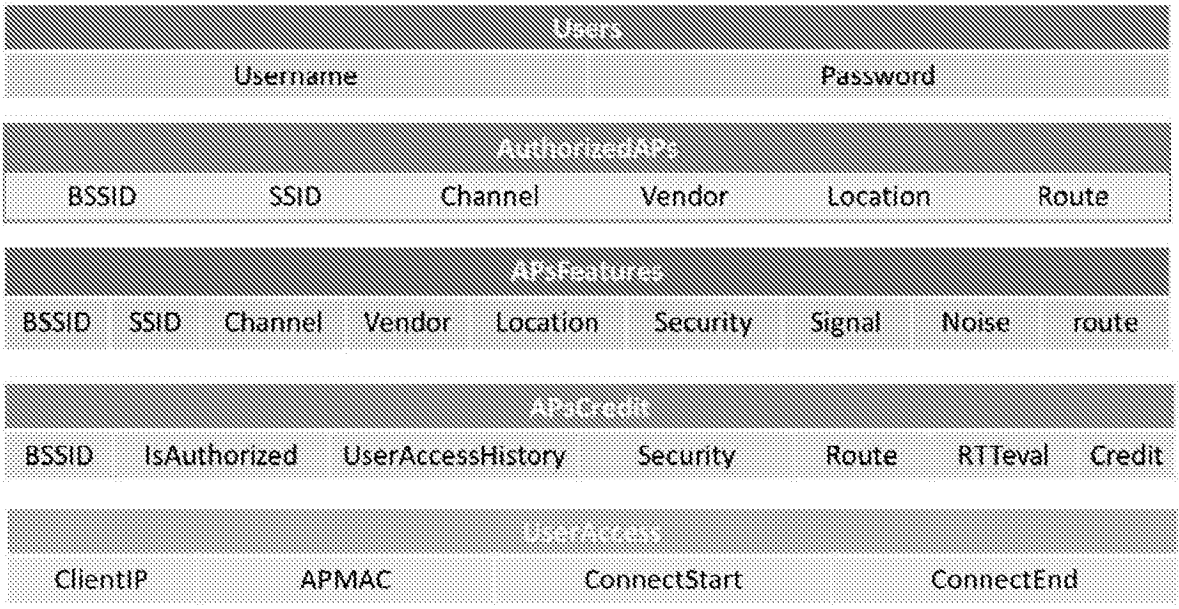

Users
Username
Password
AuthorizedAPs
BSSID
SSID
Channel
Vendor
Location
Route
APsFeatures
BSSID
SSID
Channel
Vendor
Location
Security
Signal
Noise
route
APsCredit
BSSID
IsAuthorized
UserAccessHistory
Security
Route
RTTeval
Credit
UserAccess
ClientIP
APMAC
ConnectStart
ConnectEnd

图4

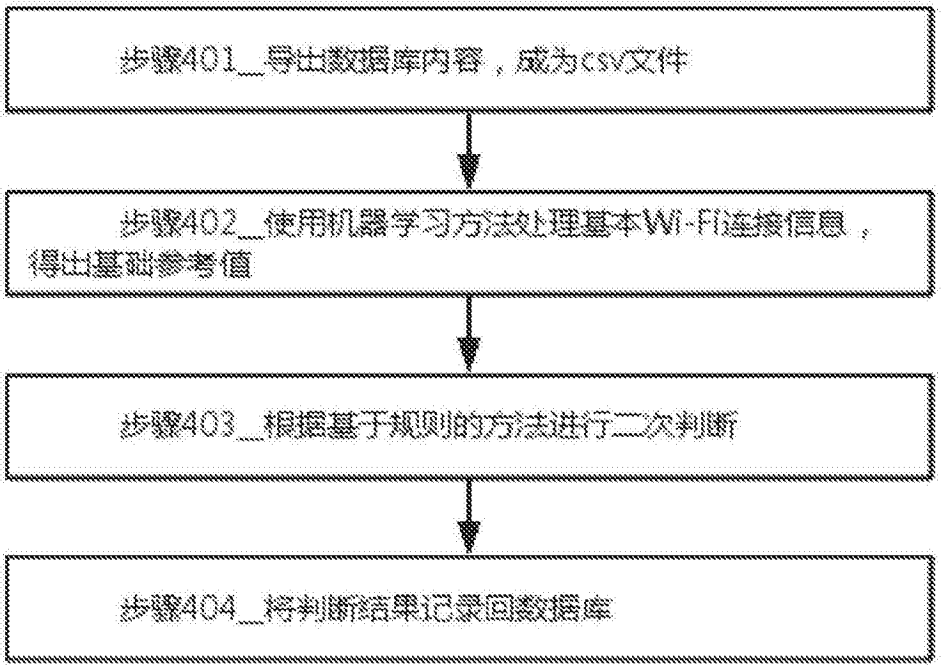

步骤401_导出数据库内容，成为csv文件
步骤402_使用机器学习方法处理基本Wi-Fi连接信息，得出基础参考值
步骤403_根据基于规则的方法进行二次判断
步骤404_将判断结果记录回数据库

图5

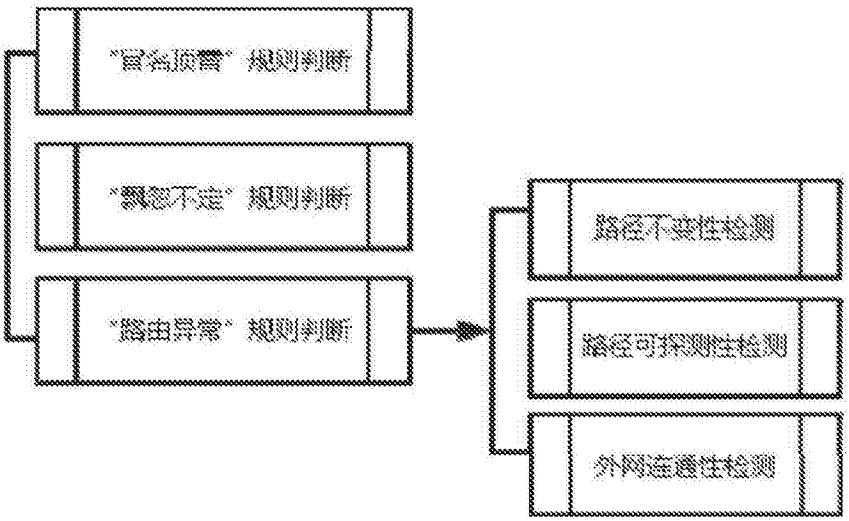

"冒名顶替"规则判断
"飘忽不定"规则判断
"路由异常"规则判断
路径不变性检测
路径可探测性检测
外网连通性检测

图6

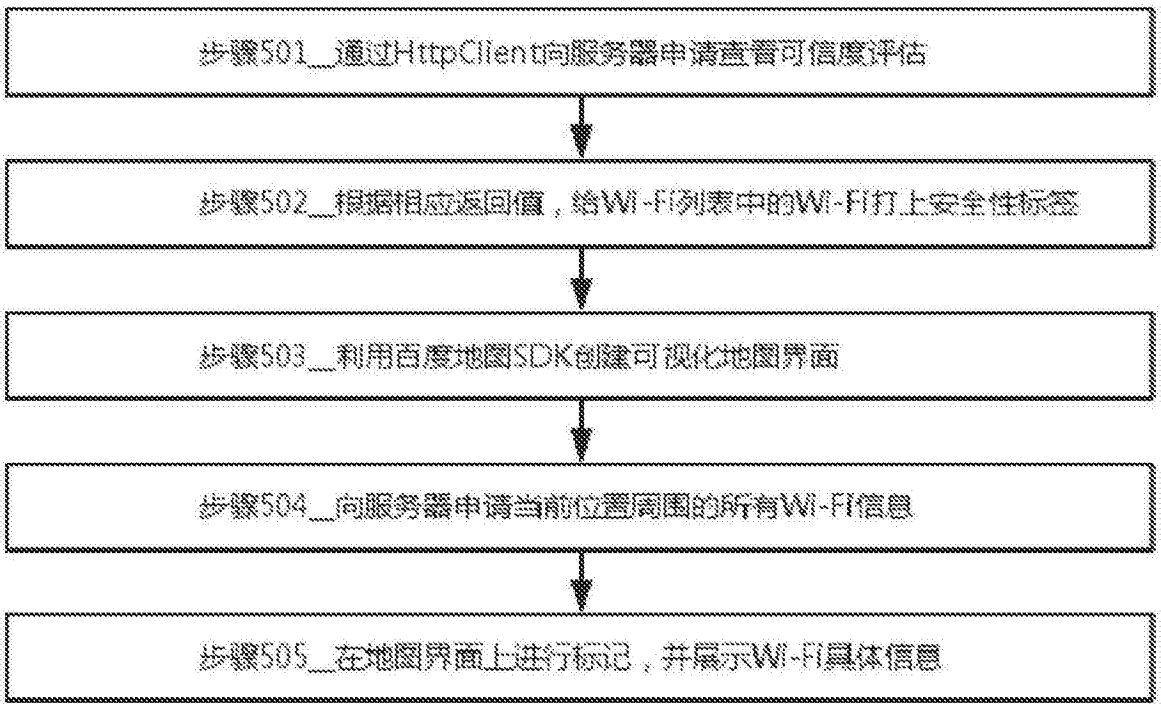

步骤501__通过HttpClient向服务器申请查看可信度评估
步骤502__根据相应返回值，给Wi-Fi列表中的Wi-Fi打上安全性标签
步骤503__利用百度地图SDK创建可视化地图界面
步骤504__向服务器申请当前位置周围的所有Wi-Fi信息
步骤505__在地图界面上进行标记，并显示Wi-Fi具体信息

图7

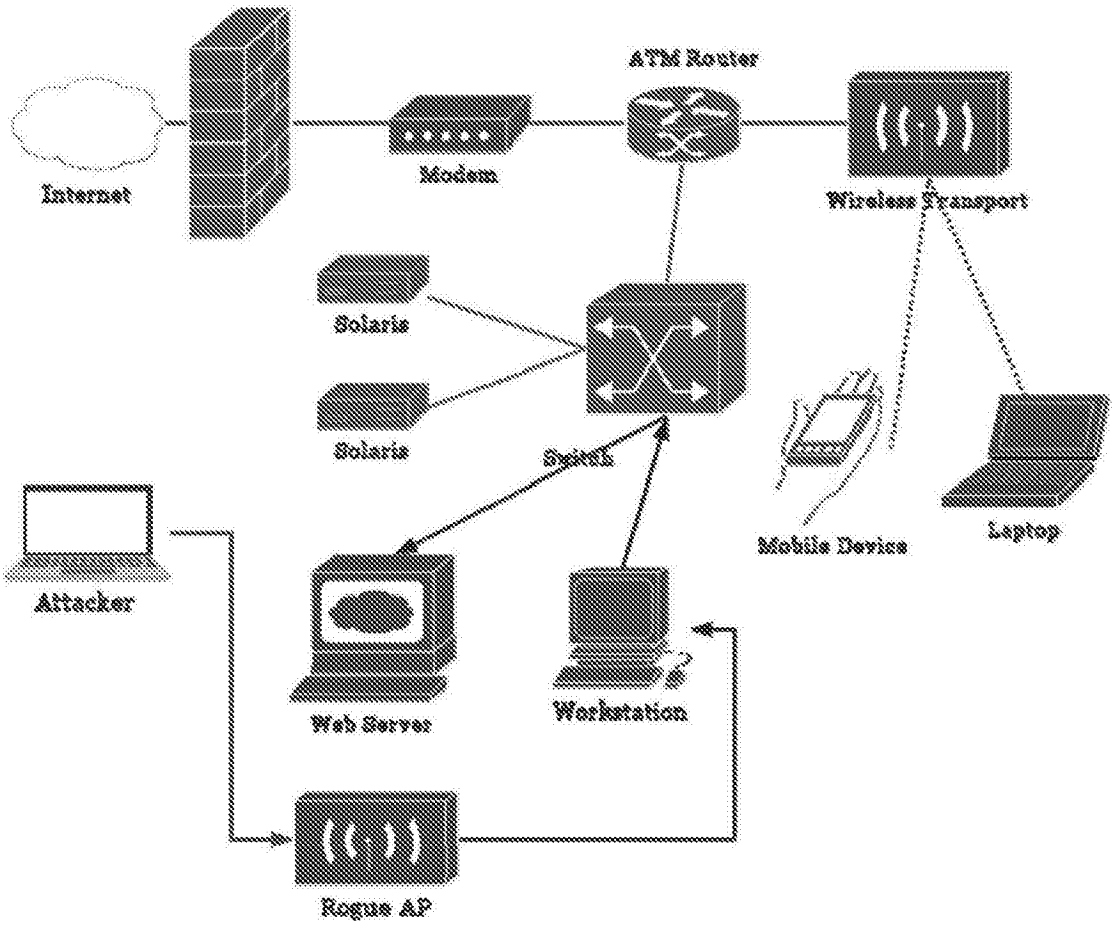

Internet
Modem
ATM Router
Wireless Transport
Solaris
Solaris
Switch
Mobile Device
Laptop
Attacker
Web Server
Workstation
Rogue AP

图8