(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 106973387 A
(43)申请公布日 2017.07.21

(21)申请号 201710169111.9

(22)申请日 2017.03.21

(71)申请人 北京大学
地址 100871 北京市海淀区颐和园路5号

(72)发明人 王韬 李晓光 吴浩洋 吕松武

(74)专利代理机构 北京万象新悦知识产权代理事务所(普通合伙) 11360
代理人 黄凤茹

(51)Int.Cl.
H04W 12/12(2009.01)
H04W 84/12(2009.01)

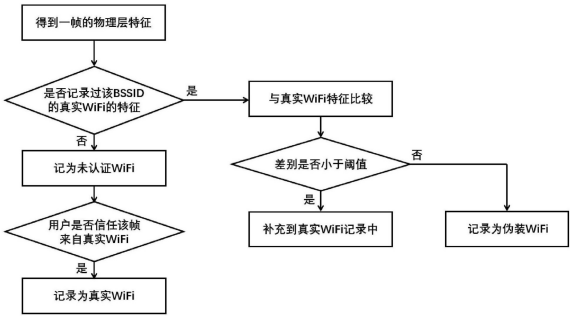
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种利用物理层信息识别伪装WiFi的方法和系统

(57)摘要

本发明公布了一种利用物理层信息识别伪装WiFi的方法和wifi系统,包括对物理层信息的采集处理和对伪装WiFi的识别;对物理层信息的采集处理过程是对WiFi接收端接收到的信号采集物理层信息,再从物理层信息中计算得到物理层特征;对伪装WiFi的识别过程是:根据所述物理层特征,对WiFi接收端接收到的信号的物理层帧的来源进行识别,识别来源是否是伪装WiFi还是真实WiFi。WiFi系统在GRT系统的基础上还包括物理层信息采集接口、物理层特征计算模块、伪装WiFi判定模块和用户交互接口。本发明技术方案可以解决多种场景下的伪装WiFi攻击问题,提高WiFi网络的安全性,具有安全性高、使用场景多样、可兼容已有WiFi网络的技术优势。



CN 106973387 A

1.一种利用物理层信息识别伪装WiFi的方法,包括对物理层信息的采集处理过程和对伪装WiFi的识别过程;所述对物理层信息的采集处理过程是对WiFi接收端接收到的信号采集物理层信息,所述采集的物理层信息是与设备相关性高、与环境相关性低的物理层信息,再从物理层信息中计算得到物理层特征;所述对伪装WiFi的识别过程是:根据所述物理层特征,对WiFi接收端接收到的信号的物理层帧的来源进行识别,识别来源是否是伪装WiFi还是真实WiFi。

2.如权利要求1所述方法,其特征是,所述采集的物理层信息包括接收信号的频率偏移、接收信号的星座点偏移、接收信号与发送信号的相关度;具体是通过计算接收信号的周期性得到频率偏移;通过对比接收值与理论值的幅度比得到与发送信号的相关度;通过在星座图上计算接收值对应的星座点与理论星座点的偏移向量,得到星座点偏移值。

3.如权利要求1所述方法,其特征是,所述物理层特征包括频偏特征、星座点偏移特征、相关度特征;所述从物理层信息中计算得到物理层特征包括如下步骤:

B1.计算频偏特征:每一个物理层帧前面有160个采样点组成的短训练字和160个采样点组成的长训练字,选取短训练字的后80个采样点进行计算,计算相距16个采样点的两个采样点的相位差,对多采样点计算得到多个相位差,再求平均值,作为单个帧的频偏特征;

B2.计算星座点偏移特征:选取长训练字,计算每个采样点到理论值的偏差向量,再对160个长训练字的采样点的偏差向量求平均,得到单帧的星座点偏移特征;

B3.计算相关度特征:选择短训练字进行相关度计算,将接收信号的短训练字的160个采样值与理论值进行一一比对,根据相关度公式求出归一化的相关系数,作为单帧的相关度特征。

4.如权利要求1所述方法,其特征是,所述对WiFi接收端接收到的信号的物理层帧的来源进行识别,具体是:

对WiFi接收端接收到的当前WiFi的信号,根据计算得到当前WiFi的物理层特征,首先判断是否已记录过与当前WiFi的BSSID相同的真实WiFi;

若有真实WiFi的记录,则将当前WiFi的物理层特征与真实WiFi的物理层特征进行对比,计算得到二者的差异值,再通过设定判决阈限来识别,将当前WiFi记录为伪装WiFi或真实WiFi;

若没有真实WiFi的记录,则暂时记录为未验证的WiFi;再由用户手动指定该WiFi是否为可信任的真实WiFi;

若用户此时指定当前WiFi为可信任,则将未验证的WiFi记录为真实WiFi;

由此实现利用物理层信息识别伪装WiFi。

5.一种可识别伪装WiFi的WiFi系统,所述WiFi系统在GRT系统的基础上还包括物理层信息采集接口、物理层特征计算模块、伪装WiFi判定模块和用户交互接口;其中GRT系统的WiFi接收端多个级联的数据处理模块按数据流方向包括时间同步模块、频偏纠正模块、去保护间隔模块、FFT模块、信道估计模块、相位跟踪模块、解星座映射模块、解交织模块、Viterbi译码模块、解扰码模块;

所述物理层信息采集接口,用于在接收端数据处理模块中引出所需的物理层信息,传输给物理层特征计算模块;

所述物理层特征计算模块,用于根据物理层信息计算出设备相关性高的物理层特征;

所述伪装WiFi判定模块，用来记录真实WiFi的物理层特征，并将当前信号的物理层特征与真实WiFi的物理层特征进行比对，判定是否是伪装WiFi；

所述用户交互接口，包括用户输入当前WiFi是否是可信任的真实WiFi的接口、输出给用户当前WiFi是否是真实WiFi的接口、用户控制发送端是否回复刚才接收到的包的接口。

6.如权利要求5所述系统，其特征是，所述GRT系统是实现WiFi 802.11a/g协议、支持物理层和MAC层编程的基于FPGA的WiFi开放平台。

7.如权利要求5所述系统，其特征是，所述物理层信息采集接口包括频偏接口、星座点偏移接口和相关度接口；分别从时间同步模块、频偏纠正模块、解星座映射模块中引出；所述物理层信息采集接口采集到的物理层信息通过GRT系统提供的USB通信库发送到主机上，传输给物理层特征计算模块。

8.如权利要求7所述系统，其特征是，所述频偏接口，包含一个16位宽的当前帧的频偏值和一个1位宽的有效信号；所述星座点偏移接口，包含两个16位宽的偏移值和1位宽的有效信号，两个16位宽的偏移值分别是实部和虚部的偏移值；所述相关度接口，包含一个32位宽的相关度和1位宽的有效信号。

一种利用物理层信息识别伪装WiFi的方法和系统

技术领域

[0001] 本发明属于无线通信领域，涉及WiFi网络中对伪装行为的识别技术，尤其涉及一种利用物理层信息对伪装成特定网络的WiFi进行识别的方法及系统。

背景技术

[0002] 在现代社会中，随着移动终端的普及和人们对网络的需求增加，WiFi成为生活中必不可少的资源，是连接人与信息网络的重要入口。现在WiFi越来越普及，人们在家中部署WiFi，用于手机、智能电视、笔记本电脑等智能设备的联网；在公司部署WiFi，用于日常工作和团队协作；在机场、咖啡馆等公共场所部署WiFi，商家为客户提供便利；在物联网部署WiFi，如摄像头网络，用于物联网设备间的通信。

[0003] 大范围的普及和多领域的应用也带来了安全隐患，WiFi安全成为人们非常关心的因素。当用户使用手机等WiFi终端寻找网络时，周围WiFi接入点会通过广播特定帧(称为beacon帧)的方式告知WiFi终端自己的存在(见图1)，对于普通用户而来，此时仅能通过WiFi网络名称和是否需要输入密码来区分不同的WiFi接入点，这给了恶意攻击者可乘之机。恶意攻击者搭设与用户信任的WiFi同名的WiFi接入点，这种WiFi称为伪装WiFi，用户难以区分信任的真实WiFi和伪装WiFi。除了WiFi名称外，伪装WiFi甚至连加密方式和BSSID(基本服务集标识，常为设备的MAC地址)也可以与真实WiFi完全相同。利用普通的手机或笔记本电脑，恶意攻击者可以以极低的成本完成欺骗性很强的伪装。当用户的WiFi终端误连入伪装WiFi网络时，恶意攻击者可以通过钓鱼技术获取到用户的账号、密码、支付手势等个人信息，或者发起DoS(Denialof Service，服务失效)攻击，给用户带来损失。在2015年的央视3·15晚会上，网络安全工程师伪装了演播室的免费WiFi，钓鱼得到的现场观众的信息，观众自拍的照片和邮箱密码竟出现在了演播室大屏幕上。

[0004] 在OSI网络分层模型中，物理层是网络的最底层，是WiFi接入的入口，也是WiFi安全的第一道屏障。物理层的某些信息与WiFi设备硬件的固有属性有关，攻击者难以发起伪装。一些研究者希望利用物理层的信息提高WiFi的安全性，例如来自英国的研究者在文献(Junqing Zhang,Roger Woods,Trung Q.Duong,Alan Marshall,Yuan Ding,Yi Huang,Qian Xu,“Experimental Study on Key Generation for Physical Layer Security in Wireless Communications”,IEEE Access,2016)中分析了从WiFi物理层信道中如何生成密钥以及密钥如何用于无线通信中的加密。

[0005] 针对伪装WiFi的问题，现有一些技术和系统原型可以提供识别方法，但存在以下不足：

[0006] 1)安全性不高，仍然存在较大可能发生伪装行为。如在专利(一种识别伪装WiFi的方法、系统及系统工作方法，申请号/专利号201610804042X)中记载，通过发送特定的认证包，利用验证RSA证书的方式对WiFi进行认证，没有通过认证的WiFi则识别为伪装WiFi。然而，此方法只能识别认证包是否来自真实WiFi，无法识别其它包的真实性。具体地，当伪装WiFi与真实WiFi同时存在时，伪装WiFi可以不回复认证包，交由真实WiFi进行回复，然后在

其它包的通信过程中进行伪装。另外，此专利中未提及RSA公钥的发放方式，在RSA公钥的方法过程中，很有可能也发生伪装行为，如伪装WiFi发送假的公钥，完成后续的认证过程。

[0007] 2)识别场景受限，不方便推广使用。具体表现在以下三点。一些识别技术只能用于真实WiFi和伪装WiFi同时存在时对伪装WiFi进行识别，例如来自英国伦敦大学学院的研究者在文献(Jie Xiong,Kyle Jamieson,“SecureArray Improving WiFi Security with Fine-Grained Physical-Layer Information”,MobiCom 2013)中提出利用接收信号的角度对信号来源进行识别，然而这种方法必须在真实WiFi和伪装WiFi同时存在且距离5厘米以上时可以工作，无法在伪装WiFi单独存在时工作。与之相对，一些识别技术只能在伪装WiFi单独存在时进行识别，例如前文1)中提到的专利(一种识别伪装WiFi的方法、系统及系统工作方法，申请号/专利号201610804042X)无法在真实WiFi和伪装WiFi同时存在时工作。一些识别技术需要其他硬件介入，例如来自密歇根大学的研究者在文献(Xianru Du,Dan Shan,Kai Zeng,Lauren Huie,“Physical layer challenge-response authentication in wireless networks with relay”,INFOCOMM2014)中提出使用无线中继的方法对信号来源进行识别，这种方法的缺点是必须工作在部署有已认证的中继节点的场景。

[0008] 3)无法兼容已部署的WiFi网络。具体的，一些识别伪装WiFi的方法对WiFi接入点硬件进行定制或提出较高要求，如果要应用这些方法，已部署的WiFi设备需要更换硬件，这会造成巨大的资源浪费，降低了可实施性。例如南京大学的研究者在文献(YunlongMao,Yuan Zhang,Sheng Zhong,“Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks”,Proceedings of the 2016ACM SIGSAC Conference on Computer and Communications Security)中分析了如何在MU-MIMO(Multi-User Multiple Input Multiple Output，多用户多入多出)无线网络中利用物理层信息中的信道信息防止下行数据被窃听，然而该方法需要WiFi接入点在报文的特定字段需要进行加密，而目前已部署的WiFi接入点设备不支持这样的操作。

[0009] 综上所述，现有的对伪装WiFi的识别方法安全性不高，或无法在多种场景下对伪装WiFi进行识别，或无法兼容已经部署的WiFi网络。

发明内容

[0010] 为了能识别伪装成特定网络的WiFi，本发明提出一种利用物理层信息对伪装WiFi进行识别的方法和系统，从物理层信息中计算得到物理层特征，根据特征判断接收到的物理层帧的来源是真实WiFi还是伪装WiFi，具有安全性高、识别场景广、兼容已有WiFi网络等特点。

[0011] 以下是对术语的约定：

[0012] WiFi终端：指可以连接WiFi的终端设备，如手机、笔记本电脑、平板电脑等。

[0013] WiFi接入点：指提供WiFi接入的设备，是WiFi网络的中心，其它WiFi终端通过连接WiFi接入点加入同一WiFi网络。

[0014] 真实WiFi：指用户可以信任、希望连接的WiFi接入点。

[0015] 伪装WiFi：指伪装成特定真实WiFi的WiFi接入点。

[0016] 物理层帧：在WiFi802.11协议中，物理层和MAC层以帧为单位进行传输，物理层的传输单位即为物理层帧。与此相对，网络层、传输层等以包为单位进行传输。

[0017] 物理层信息:指WiFi协议中属于物理层的信息,既包括物理上的信道特征、无线信号特征,也包括物理层数据处理中的调制方式、编码方式等。

[0018] 物理层特征:特指将采集到的多种物理层信息经过本发明提出的特殊处理,得到的与发送设备相关的特征。

[0019] 本发明的原理是:

[0020] 伪装WiFi常用的技术是模仿真实WiFi的名称、IP地址、BSSID、加密方式、认证网页等,这些信息所具有的共同点是与WiFi设备本身硬件无关。本发明用来识别伪装WiFi的方法是利用物理层信息中接收到的无线信号的偏差,由于无线发射机和接收机硬件的不完美性,接收到的无线信号与理论值会有偏差,无线接收端信号处理过程会消除偏差并获取真实信号,一个典型的WiFi接收机结构如图2。一般认为无线信号的偏差干扰了原始信息,但从另一角度讲,无线信号偏差与硬件电路关系密切,利用这部分信息通过精心设计的算法可以计算得到与发送设备相关的特征,称为物理层特征。同一个设备的物理层特征随时间变化不大,两个不同设备之间物理层特征差别较大。通过记录真实WiFi的物理层特征,与当前接收信号的物理层特征进行比对,可以判断当前接收信号来自真实WiFi还是伪装WiFi。

[0021] 本发明提供的技术方案是:

[0022] 一种利用物理层信息识别伪装WiFi的方法,包括对物理层信息的采集和处理及对伪装WiFi的识别;所述对物理层信息的采集和处理的方法,包括对物理层信息进行挑选,选出与设备相关性高、与环境相关性低的物理层信息,在WiFi接收端对接收的信号采集这些信息,对信息通过本发明提出的特定算法进行处理,计算得到物理层特征;所述对伪装WiFi的识别方法,包括当收到一个新的物理层帧时,暂时记录为未验证WiFi,若没有真实WiFi记录且用户指定此WiFi为信任的WiFi时,则记录为真实WiFi,当用户不指定时则保持为未验证WiFi;若已有真实WiFi的记录,则将当前接收信号的物理层特征与真实WiFi进行比对,计算差异值,设定判决阈限判断来自真实WiFi还是伪装WiFi。上述识别方法的流程图见图3。

[0023] 本发明的利用物理层信息识别伪装WiFi的方法,包括以下步骤:

[0024] A)设计物理层信息的挑选策略和采集方法。在WiFi系统中有很多种类的物理层信息,有与传输速率相关的调制方式、编码方式等,有与传输环境相关的RSSI(接收的信号强度指示)、CSI(信道状态信息)等。不同物理层信息在WiFi接收端的获取位置不同,采集方式也不同。挑选与采集物理层信息包括以下步骤:

[0025] A1.挑选与发送端硬件相关、受其他因素影响小的物理层信息。物理层信号多种多样,经过挑选,我们保留三种物理层信息作为参考依据,接收信号的频率偏移、星座点偏移、与发送信号的相关度。接收信号的频率偏移是指经过接收端解调后得到数字基带信号与发送端发出的基带信号的频率差,来源于发送端与接收端的本振频率的微小差别,与发送端和接收端硬件相关,受环境影响小。接收信号星座点偏移是指接收信号在星座图上的分布与发送信号理论值的偏差,偏移值在BPSK星座图和QPSK星座图见图4。接收信号与发送信号的相关度是指接收信号与发送信号的相似程度。接收信号星座点偏移和与发送信号相关度受发送端硬件、信道、接收端硬件影响,当取多采样点求平均时,可以降低信道的影响。

[0026] A2.采集物理层信息,具体表现为采集接收信号的频率偏移、星座点偏移、与发送信号的相关度。物理层信息可从WiFi接收端数据处理过程中采集,以WiFi的802.11a/g协议为例,每一个物理层帧前面会有固定内容的长训练字和短训练字,接收端对比长短训练字

信号的接收值与理论值，可以得到所需的物理层信息。具体地，短训练字具有周期性，通过计算接收信号的周期性得到频率偏移，通过对比接收值与理论值的幅度比得到与发送信号的相关度，通过在星座图上计算接收值对应的星座点与理论星座点的偏移向量，得到星座点偏移值。

[0027] B)设计物理层特征的计算方法，对步骤A)采集到的物理层信息进行计算，包括频率偏移、星座点偏移、与发送信号的相关度，得到对应的物理层特征，包括频偏特征、星座点偏移特征、相关度特征，具体包括如下步骤：

[0028] B1.计算频偏特征。在802.11a/g协议中，每一个物理层帧前面会有160个采样点组成的短训练字和160个采样点组成的长训练字，短训练字每16个采样值为一个周期进行循环，共10个周期，其中前80个采样点往往受自动增益控制影响较大，我们选取短训练字的后80个采样点进行计算，计算相距16个采样点的两个采样点的相位差，对多采样点计算求平均值，即为单个帧的频偏特征。

[0029] B2.计算星座点偏移特征。在802.11a/g协议中，共有BPSK、QPSK、QAM16、QAM64四种符号调制方式，而训练字只会使用BPSK调制，我们选取长训练字，计算每个采样点到理论值的偏差向量，偏差向量见图4。对160个长训练字的采样点的偏差向量求平均，得到单帧的星座点偏移特征。

[0030] B3.计算相关度特征。我们选择用短训练字进行相关度计算，将接收信号的短训练字的160个采样值与理论值进行一一比对，根据相关度公式求出归一化的相关系数，作为单帧的相关度特征。

[0031] C)设计对伪装WiFi的识别方法，包括记录真实WiFi的物理层特征和将当前WiFi与真实WiFi物理层特征进行比对。具体地，由用户手动指定当前发现的WiFi是否为可信任的真实WiFi，在步骤B)计算得到当前WiFi的物理层特征后，判断是否已记录过与当前WiFi的BSSID相同的真实WiFi：若没有真实WiFi的记录，则暂时记录为未验证的WiFi，若用户指定此WiFi为信任的WiFi，则将未验证的WiFi记录为真实WiFi，用户不指定时则保持为未验证WiFi；若有真实WiFi的记录，则将当前WiFi与真实WiFi进行对比，若对比不相同则记录为伪装WiFi。伪装WiFi判断流程图见图3。

[0032] 上述利用物理层信息识别伪装WiFi的方法可在多种场景下工作，具体地：当真实WiFi和伪装WiFi同时存在时，因为上述设计对每一个接收到的物理层帧进行真实性判断，可以有效地区分来自真实WiFi的帧和来自伪装WiFi的帧；当伪装WiFi单独存在时，因为预存过真实WiFi的物理层特征，可以直接用来对当前WiFi进行判断；上述设计不需要介入其它硬件。另外，上述设计可以兼容已有WiFi网络，因为只对WiFi终端进行了修改，没有对WiFi接入点提出任何要求，所以已经部署的WiFi网络可以继续使用。

[0033] 本发明还提供一种可识别伪装WiFi的WiFi系统，在GRT系统的基础上(GRT系统是一个基于FPGA的WiFi开放平台，实现了WiFi 802.11a/g协议，并且支持物理层、MAC层编程)，另外还包括物理层信息采集接口、物理层特征计算模块、伪装WiFi判定模块和用户交互接口；其中，物理层信息采集接口，在接收端数据处理模块中引出所需的物理层信息，传输给物理层特征计算模块；物理层特征计算模块，根据物理层信息计算出设备相关性高的物理层特征；伪装WiFi判定模块，用来记录真实WiFi的物理层特征，并将当前信号的物理层特征与真实WiFi的物理层特征进行比对，判定是否是伪装WiFi；用户交互接口，包括用户输

入当前WiFi是否是可信任的真实WiFi的接口，输出给用户当前WiFi是否是真实WiFi的接口，用户控制发送端是否回复刚才接收到的包的接口。

[0034] 与现有技术相比，本发明的有益效果是：

[0035] 本发明提供一种利用物理层信息对伪装WiFi进行识别的方法和一种可识别伪装WiFi的WiFi系统，从物理层信息中根据本发明提出的计算方法得到物理层特征，根据特征判断接收到的物理层帧的来源是真实WiFi还是伪装WiFi。通过本发明提供的利用物理层信息识别伪装WiFi的方法，可以解决多种场景下的伪装WiFi攻击问题，提高了WiFi网络的安全性。本发明具有安全性高、使用场景多样、可兼容已有WiFi网络的技术优势。

附图说明

[0036] 图1是WiFi终端设备发现周边多个WiFi接入点的示意图；

[0037] 其中，(a)是用户的WiFi终端，如手机、笔记本电脑、平板电脑；(b)、(c)是无密码的公共WiFi；(d)是用户可信任的办公室的WiFi；(e)是恶意攻击者搭建的伪装成用户信任WiFi的伪装WiFi。

[0038] 图2是一个典型的WiFi接收机结构图。

[0039] 图3是本发明利用物理层特征识别伪装WiFi的方法流程图。

[0040] 图4是星座点偏移示意图；

[0041] 其中，(a)为QPSK调制方式下星座点偏移示意图；(b)为BPSK调制方式下星座点偏移示意图，WiFi的符号调制方式有多种，此处以QPSK和BPSK为例。

[0042] 图5是本发明实施例提供的可识别伪装WiFi的WiFi系统的总体结构框图。

具体实施方式

[0043] 下面结合附图，通过实施例进一步描述本发明，但不以任何方式限制本发明的范围。

[0044] 本发明提供一种利用物理层信息识别伪装WiFi的方法，包括对物理层信息的采集方法、对物理层特征的计算方法以及对伪装WiFi的识别方法；其中，对物理层信息的采集方法分为两步，第一步是挑选合适的物理层信息，挑选策略为选取与设备相关的信息，排除与环境等其他因素相关的信息，挑选结果为接收信号的频率偏移、星座点偏移、与发送信号的相关度，第二步是采集这些物理层信息，采集方法是在接收端的相应模块中增加信号接口，引出采集到的信号；对物理层特征的计算方法是对三种物理层信息分别通过特定算法进行处理，计算得到物理层特征，包括频偏特征、星座点偏移特征、相关度特征；对伪装WiFi的识别方法，包括记录来自真实WiFi的信号的物理层特征，将当前接收的每一帧的物理层特征与真实WiFi进行比对，计算出差异值，设定判决阈限判断来自真实WiFi还是伪装WiFi。

[0045] 本发明的一个应用实例是可识别伪装WiFi的WiFi系统，通过本实例对本发明的具体实施方式进行描述，以便本领域的技术人员更好地理解本发明。

[0046] 本实例在现有WiFi系统上进行扩展，所选用的WiFi系统是来自北京大学的研究者发布的GRT系统(Jiahua Chen,Tao Wang,Haoyang Wu,Jian Gong,Xiaoguang Li,Yang Hu,Gaohan Zhang,Zhiwei Li,Junrui Yang,and Songwu Lu,“A High-performance and High-programmability Reconfigurable Wireless Development Platform”,ICFPT

2014),GRT系统是一个基于FPGA的WiFi开放平台,实现了WiFi 802.11a/g协议,并且支持物理层、MAC层编程。本实例在GRT系统的基础上,增加以下四个模块或接口:物理层信息采集接口,在接收端数据处理模块中引出所需的物理层信息,传输给物理层特征计算模块;物理层特征计算模块,根据物理层信息计算出设备相关性高的物理层特征;伪装WiFi判定模块,用来记录真实WiFi的物理层特征,并将当前信号的物理层特征与真实WiFi的物理层特征进行比对,判定是否是伪装WiFi;用户交互接口,包括用户输入当前WiFi是否是可信任的真实WiFi的接口,输出给用户当前WiFi是否是真实WiFi的接口,用户控制发送端是否回复刚才接收到的包的接口。

[0047] 本实例系统结构总体设计见图5,本发明提供的对伪装WiFi的识别方法在本实例中的实现方法如下:

[0048] A)物理层信息采集接口

[0049] WiFi接收端有多个级联的数据处理模块,按数据流方向包括时间同步模块、频偏纠正模块、去保护间隔模块、FFT(快速傅里叶变换)模块、信道估计模块、相位跟踪模块、解星座映射模块、解交织模块、Viterbi译码模块、解扰码模块,物理层信息从同步模块、频偏纠正模块、解星座映射三个模块中采集。采集到的数据经过了预处理,预处理的过程属于物理层特征计算过程,为了提高计算效率和降低接口复杂度,没有放在物理层特征计算模块中做,而是分散在三个采集模块中做,预处理的算法仍在物理层特征计算模块设计中介绍。采集到的物理层信息通过GRT系统提供的USB通信库发送到主机上。具体接口设计如下:

[0050] A1.从频偏纠正模块引出的频偏接口,包含一个16位宽的当前帧的频偏值和一个1位宽的有效信号,16位宽的频偏值单位是角度,有效信号为高时表示频偏值有效,一帧内只会有效一次。

[0051] A2.从解星座映射模块中引出的星座点偏移接口,包含两个16位宽的偏移值,分别是实部和虚部的偏移值,1位宽的有效信号,同样是一帧出现一次有效。

[0052] A3.从同步模块中引出相关度接口,包含一个32位宽的相关度,1位宽的有效信号,同样是一帧出现一次有效。

[0053] B)物理层特征计算模块设计

[0054] 物理层特征计算模块在主机上实现,此处也会介绍A)中提到的在各个接收端采集模块中实现的预处理算法,预处理是为了提高计算效率和降低接口复杂度,FPGA硬件的计算效率高于计算机主机软件的计算效率。

[0055] B1.计算频偏特征。在802.11a/g协议中,每一个物理层帧前面会有160个采样点组成的短训练字和160个采样点组成的长训练字,短训练字每16个采样值为一个周期进行循环,共10个周期,其中前80个采样点往往受自动增益控制影响较大,我们选取短训练字的后80个采样点进行计算。

[0056] 假设k_1、k_2时刻的采样值分别为:

[0057]
$$s(k_1)=r(k_1)\cdot e^{j2\pi\Delta f k_1/f_s}$$
$$s(k_2)=r(k_2)\cdot e^{j2\pi\Delta f k_2/f_s} \qquad \text{(式 1)}$$

[0058] 式1由无线通信中接收信号的数学模型带入k_1、k_2所得,其中,$r(k_1)$、$r(k_2)$为k_1、k_2时刻的采样点的理论值,$s(k_1)$、$s(k_1)$为k_1、k_2时刻的采样点的实际接收值,Δf为频率偏移,

f_s为采样频率，$r(k_1)$、$r(k_2)$、$s(k_1)$、$s(k_1)$、f_s均已知，我们经过以下推导可以求出Δf。根据短训练字每16个数据点就重复一次的特性，可知，当$k_2=k_1+16$时，由式1代入$k_2=k_1+16$可推出：

[0059] $$A+Bj=\frac{s(k_1)}{s(k_2)} \qquad (式\ 2.1)$$

[0060] $$\Delta f=\frac{f_s}{2\pi\cdot 16}\cdot\arctan\left[\frac{B}{A}\right] \qquad (式\ 2.2)$$

[0061] 式2.1由复数的性质推出，$s(k_1)$、$s(k_1)$都是复数，相除的结果也是复数，复数总是可以写成A+Bj的形式，A、B为实数，是为了推导式2.2的中间变量。式2.2由式1和式2.1推导得到。为了消除噪声的影响，对80个采样点计算64次Δf的值，并求平均值，平均值公式为：

[0062] $$\overline{\Delta f}=\frac{1}{64}\sum_{k=0}^{63}\Delta f_k \qquad (式\ 3)$$

[0063] 其中，Δf_k为由第k点计算出的频偏。$\overline{\Delta f}$即为我们想要的单帧的频偏特征。

[0064] B2.计算星座点偏移特征。在802.11a/g协议中，训练字字段只会使用BPSK调制，我们选取长训练字，计算每个采样点到理论值的偏差向量，偏差向量见图4。在BPSK调制方式下，星座图上星座点的理论值有两个点(+1,0)和(-1,0)，对长训练字采样点计算实际值和理论值的偏差，160个采样点按两个理论点分别求平均，得到的是两个星座点的平均偏移值，组成一个偏移向量$\left(\overline{\Delta p_1},\overline{\Delta p_2}\right)$，即为星座点偏移特征。

[0065] B3.计算相关度特征。我们选择用短训练字进行相关度计算，将接收信号的短训练字的160个采样值与理论值进行一一比对，采用的是相关算法，每L个点组成一组，L取为16，共10组，在组内计算接收信号和发送信号的互相关系数和接收信号的能量，接收信号的能量用于判决统计的归一化，即：

$$C_n=\sum_{k=0}^{L-1}r_{n+k}\cdot s_{n+k}^{*}$$

[0066] $$P_n=\sum_{k=0}^{L-1}s_{n+k}\cdot s_{n+k}^{*}=\sum_{k=0}^{L-1}\left|s_{n+k}\right|^2 \qquad (式\ 4)$$

$$L=16$$

$$n=0,L,2L,3L,...,9L$$

[0067] 式4由本发明提出，其中r_{n+k}为n+k采样点的理论值，s_{n+k}为n+k采样点的实际接收值，C_n为未归一化的互相关系数，P_n为实际信号能量，作为归一化系数。互相关系数除以接收信号的能力可以得到归一化的互相关系数，对10组取平均，统计判决的M为：

[0068] $$M=\frac{1}{10}\sum_{n=0}^{9}\frac{\left|C_n\right|^2}{P_n^{\,2}} \qquad (式\ 5)$$

[0069] M即为我们想要的相关度特征。

[0070] C)伪装WiFi判断模块

[0071] 在物理层特征计算模块计算得到当前帧的单帧物理层特征后,伪装WiFi判断模块会按BSSID对单帧特征值进行记录,WiFi物理层特征数据库表设计见表1。

[0072] 表1实施例中WiFi物理层特征数据库表设计

[0073]

关键字BSSID	WiFi名称	状态	记最次数N	频偏特征	星座点偏移特征	相关度特征

[0074] 状态分为:未验证,真实

[0075] 具体地,使用BSSID作为关键字去物理层特征数据库表中寻找记录,若未找到此BSSID状态的记录,则将此帧的物理层特征作为初始值,标记状态为未验证的WiFi,记录次数为1;若找到此BSSID作为未验证WiFi的记录且用户手动指定为真实WiFi,则修改数据库中状态为真实,其余值不变;若找到此BSSID作为真实WiFi的记录,将当前帧的物理层特征与记录进行对比,对比方法是分别比较三种特征,差别小于一定阈限时(实施例设为±20%),认为是来自真实WiFi的帧,按式6计算物理层特征的平均值newVal:

[0076] $$newVal=\frac{1}{N+1}\left(oldVal\times N+curVal\right)$$ (式6)

[0077] oldVal为原数据库中的物理层特征,curVal为当前帧的物理层数值,curVal与oldVal的差异小于20%,N为数据库表中记录过的帧的个数。将newVal更新到数据库中,并将N加1存入数据库。

[0078] 当前帧的物理层特征与记录的差别超过阈限时,说明此帧是伪装WiFi,通过用户交互接口发出预警信号,不记录到数据库中。

[0079] D)用户交互接口设计

[0080] 用户交互接口分为三组,第一组是验证当前WiFi为真实WiFi的接口,第二组是反馈收到来自伪装WiFi的帧的接口,第三组是控制发送端行为的接口。

[0081] D1.验证当前WiFi为真实WiFi的接口,输出给用户64字节的WiFi名称、48字节的BSSID,用户输入1字节是否信任。此处用字节为单位而不是A)中以位为单位,是因为在硬件设计中的端口以位为单位,而软件的接口以字节为单位,以下相同。

[0082] D2.反馈收到来自伪装WiFi的帧的接口,输出给用户64字节的WiFi名称、48字节的BSSID、8字节的相似度、1字节的判断结果,判断结果为1时表示来自真实WiFi,判断结果为0时表示来自伪装WiFi,判断结果为-1时表示来自未经验证的WiFi。

[0083] D3.控制发送端行为的接口,此接口的目的是用户可以指定当收到伪装WiFi或未经验证的WiFi时发送端的行为,用户输入48字节的WiFi名称、48字节的BSSID、1字节收到的帧的类型、1字节收到此类帧时的行为。收到的帧的类型包括来自伪装WiFi、来自未经验证的WiFi。收到此类帧的行为包括停止回复该BSSID、允许回复该BSSID。

[0084] 需要注意的是,公布实施例的目的在于帮助进一步理解本发明,但是本领域的技术人员可以理解:在不脱离本发明及所附权利要求的精神和范围内,各种替换和修改都是可能的。因此,本发明不应局限于实施例所公开的内容,本发明要求保护的范围以权利要求书界定的范围为准。

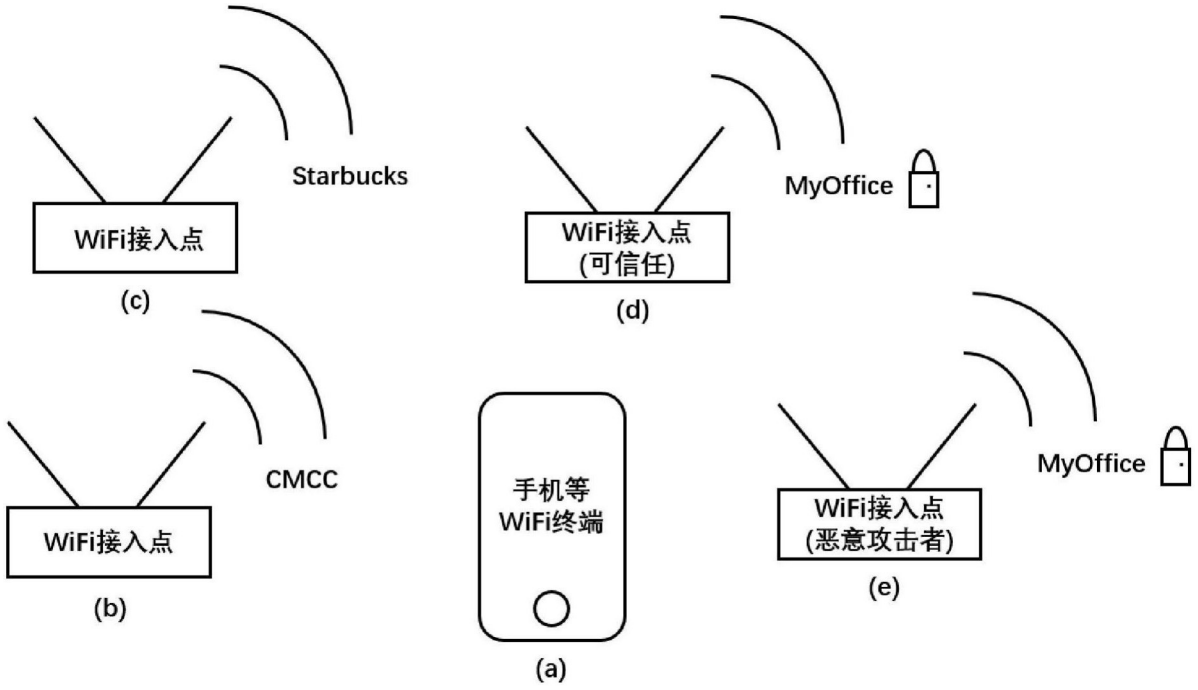

Starbucks
WiFi接入点
(c)
MyOffice
WiFi接入点
(可信任)
(d)
CMCC
WiFi接入点
(b)
手机等
WiFi终端
(a)
MyOffice
WiFi接入点
(恶意攻击者)
(e)

图1

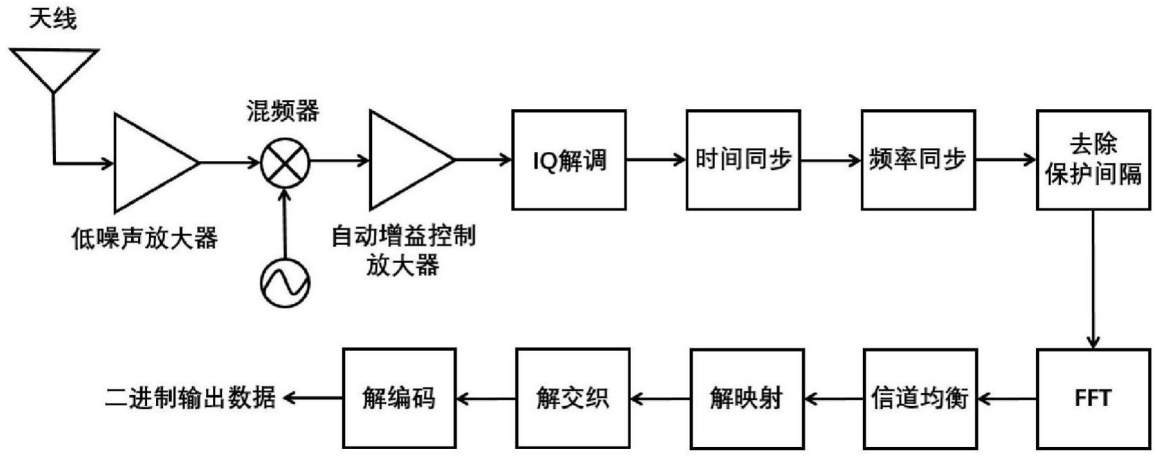

天线
混频器
低噪声放大器
自动增益控制
放大器
IQ解调
时间同步
频率同步
去除
保护间隔
FFT
信道均衡
解映射
解交织
解编码
二进制输出数据

图2

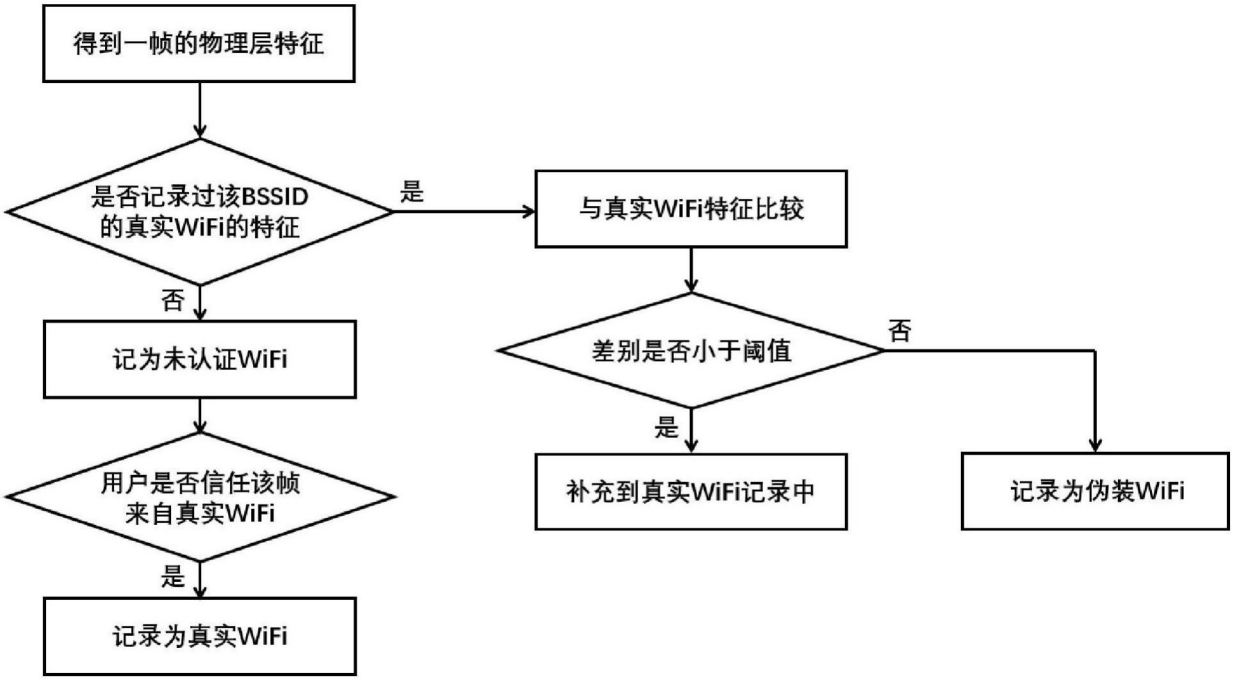
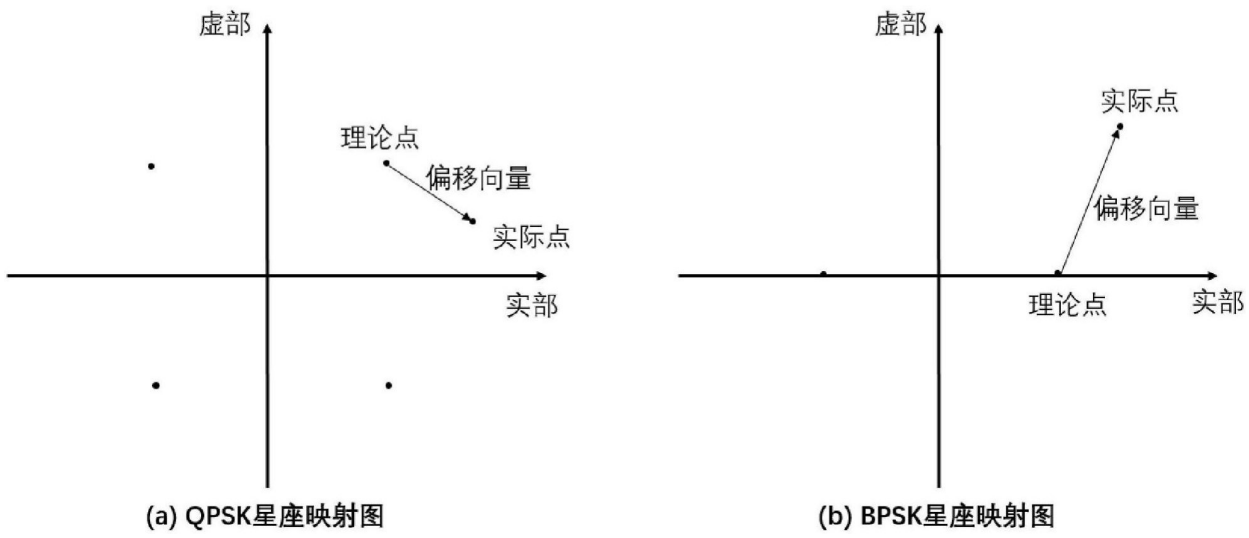


图3



(a) QPSK星座映射图 (b) BPSK星座映射图

图4

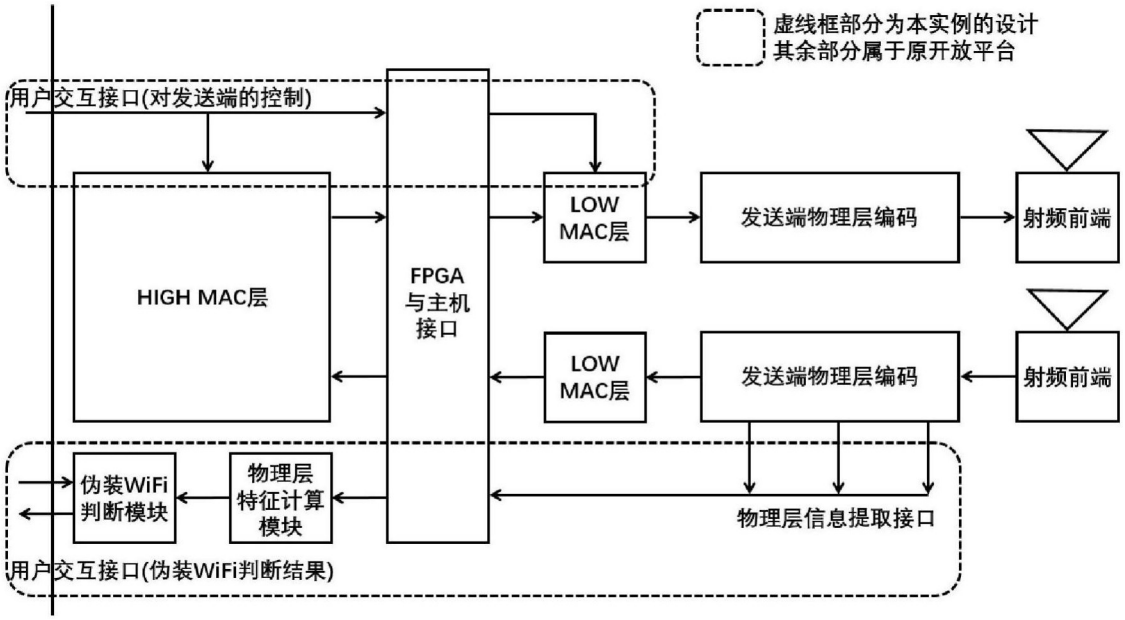

虚线框部分为本实例的设计
其余部分属于原开放平台
用户交互接口(对发送端的控制)
HIGH MAC层
FPGA
与主机
接口
LOW
MAC层
发送端物理层编码
射频前端
LOW
MAC层
发送端物理层编码
射频前端
伪装WiFi
判断模块
物理层
特征计算
模块
物理层信息提取接口
用户交互接口(伪装WiFi判断结果)

图5