(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108156102 B
(45)授权公告日 2020.06.26

(21)申请号 201711336107.3

(22)申请日 2017.12.13

(65)同一申请的已公布的文献号
申请公布号 CN 108156102 A

(43)申请公布日 2018.06.12

(73)专利权人 深圳大学
地址 518060 广东省深圳市南山区南海大道3688号

(72)发明人 谢宁 张莉

(74)专利代理机构 深圳舍穆专利代理事务所（特殊普通合伙）44398
代理人 黄贤炬

(51)Int.Cl.
H04L 25/03(2006.01)
H04L 25/02(2006.01)
H04W 12/06(2009.01)

(56)对比文件
CN 106664194 A,2017.05.10,
CN 103733560 A,2014.04.16,
CN 107196920 A,2017.09.22,
CN 105635125 A,2016.06.01,
US 2013159722 A1,2013.06.20,
季新生等.“基于哈希方法的物理层认证机制”.《电子与信息学报》.2016,

审查员 郑骏

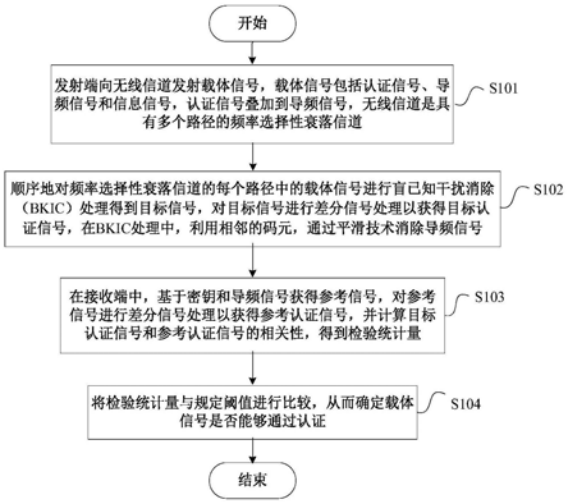
权利要求书2页 说明书12页 附图3页

(54)发明名称

基于平滑技术的频率选择性衰落信道的盲认证方法和系统

(57)摘要

本发明公开一种基于平滑技术的频率选择性衰落信道的盲认证方法，其包括向具有多个路径的频率选择性衰落信道发射载体信号，载体信号包括认证信号、导频信号和信息信号，认证信号叠加到导频信号；接收载体信号，顺序地对每个路径中的载体信号进行盲已知干扰消除(BKIC)处理得到目标信号，对目标信号进行差分信号处理以获得目标认证信号，BKIC处理利用相邻的码元，通过平滑技术消除导频信号；基于密钥和导频信号获得参考信号，对参考信号进行差分信号处理以获得参考认证信号，并计算目标认证信号和参考认证信号的相关性，得到检验统计量；并且将检验统计量与规定阈值进行比较，从而确定载体信号是否能够通过认证。



CN 108156102 B

1.一种基于平滑技术的频率选择性衰落信道的盲认证方法，是具有发射端和接收端的无线通信系统的无线通信的物理层认证方法，其特征在于，

包括：

所述发射端向无线信道发射载体信号，所述载体信号包括认证信号、导频信号和信息信号，所述认证信号叠加到所述导频信号，所述无线信道是具有多个路径的频率选择性衰落信道；

所述接收端接收所述载体信号，顺序地对所述频率选择性衰落信道的每个路径中的所述载体信号进行盲已知干扰消除处理得到目标信号，对所述目标信号进行差分信号处理以获得目标认证信号，在所述盲已知干扰消除处理中，利用相邻的码元，通过平滑技术消除所述导频信号；

在所述接收端中，基于密钥和所述导频信号获得参考信号，对所述参考信号进行差分信号处理以获得参考认证信号，并计算所述目标认证信号和所述参考认证信号的相关性，得到检验统计量；并且

将所述检验统计量与规定阈值进行比较，从而确定所述载体信号是否能够通过认证。

2.根据权利要求1所述的盲认证方法，其特征在于：

所述载体信号以数据块的形式分块发射。

3.根据权利要求2所述的盲认证方法，其特征在于：

在每块所述载体信号中，所述导频信号的信号长度与所述信息信号的信号长度和等于所述载体信号的信号长度。

4.根据权利要求1所述的盲认证方法，其特征在于，

利用哈希矩阵，基于所述密钥和所述导频信号获得所述参考信号。

5.根据权利要求1所述的盲认证方法，其特征在于，

若所述检验统计量不小于所述规定阈值，则所述载体信号通过认证。

6.根据权利要求1所述的盲认证方法，其特征在于，

所述规定阈值基于所述导频信号的统计特性以及预设的虚警概率上限得到。

7.一种基于平滑技术的频率选择性衰落信道的盲认证设备，其特征在于，

包括：

处理器，其执行存储器存储的计算机程序以实现如权利要求1至6任一项所述的盲认证方法；以及

所述存储器。

8.一种计算机可读存储介质，其特征在于，

所述计算机可读存储介质存储有至少一个指令，所述至少一个指令被处理器执行时实现如权利要求1至6任一项所述的盲认证方法。

9.一种基于平滑技术的频率选择性衰落信道的盲认证系统，其特征在于，

发射装置，其向无线信道发射载体信号，所述载体信号包括认证信号、导频信号和信息信号，所述认证信号叠加到所述导频信号，所述无线信道是具有多个路径的频率选择性衰落信道；以及

接收装置，其包括：第一处理模块，其接收所述载体信号，顺序地对所述频率选择性衰落信道的每个路径中的所述载体信号进行盲已知干扰消除处理得到目标信号，对所述目标

信号进行差分信号处理以获得目标认证信号，在所述盲已知干扰消除处理中，利用相邻的码元，通过平滑技术消除所述导频信号；第二处理模块，其基于密钥和所述导频信号获得参考信号，对所述参考信号进行差分信号处理以获得参考认证信号，并计算所述目标认证信号和经过差分信号处理的所述参考认证信号的相关性，得到检验统计量；以及判定模块，其将所述检验统计量与规定阈值进行比较，从而确定所述载体信号是否能够通过认证。

10.根据权利要求9所述的盲认证系统，其特征在于，

所述第二处理模块利用哈希矩阵基于所述密钥和所述导频信号获得所述参考信号。

11.根据权利要求9所述的盲认证系统，其特征在于，

在所述判定模块中，所述规定阈值基于所述导频信号的统计特性和预设的虚警概率上限得到。

基于平滑技术的频率选择性衰落信道的盲认证方法和系统

技术领域

[0001] 本发明涉及无线通信技术领域，具体涉及一种基于平滑技术的频率选择性衰落信道的盲认证方法和系统。

背景技术

[0002] 当前物理层认证技术主要有三种，第一种认证技术是扩频技术(Auth-SS)，基本思想是采用传统的直接序列扩频或者调频技术，由于不同的脉冲采用了不同的频率，因此这种技术实现认证需要牺牲一定的带宽。此外，Auth-SS技术的一个关键的限制是只允许了解扩频技术相关先验知识的用户参与通信。因此这种技术的适用范围比较窄。

[0003] 第二种是基于时分复用认证技术(Auth-TDM)，基本思想是，发射端周期性的交替发送信息信号和认证信号。接收端接收到信号后直接提取期望的认证信息实现信号的认证目的。Auth-TDM是无线通信发展早期提出的认证技术，它的优点是操作简单，发射信号之前不需要对认证信号和信息进行预处理(出于安全考虑可能会进行加密)。认证信号是独立于信息信号发送的，因此需要占用一定的带宽，随着无线信息数量的不断增加，及用户对信息隐私性的进一步提高和敌对方攻击技术的不断增强，这种认证技术的安全性受到极大的挑战，已经无法满足用户的需求。

[0004] 第三种认证技术是认证叠加技术(Auth-SUP)，基本思想是将认证信号叠加在信息信号上(叠加的方式可以任意，由密钥决定)，再由发射端同时发射出去，接收端接收到信号之后利用密钥对叠加信号中的认证信号进行提取，达到信号认证的目的。

[0005] 比起早期的Auth-TDM技术，Auth-SUP认证技术在信号发射前需要对认证信号和信息信号进行处理，对发射端的信号处理能力提出了一定的要求，实现起来比Auth-TDM技术要复杂一些，认证信号和信息信号是同时发送的，因此不会占用额外的带宽。此时，由于将认证信号叠加在信息信号中，接收端接收到信号后需要对信息进行提取，信号处理难度要比Auth-TDM技术高，但认证信息的隐蔽性较Auth-TDM高。此外，由于认证信号对于信息信号的提取来说相当于扮演了噪声的作用，使得接收端的SNR相应降低，对信息信号的提取带来不利影响。

[0006] 现有的Auth-TDM和Auth-SUP认证技术除了发射信息信号和认证信号，还发射了另一个导频信号。这是由于，这两种认证技术都需要接收端接收到信号之后对信道参数进行估计并进行码元恢复，之后才能对认证信号进行提取，此时对接收端的信号处理能力也提出了一定的要求，在一些特定的场合，这些信号处理技术可能并不可行，且在对信道参数估计和码元恢复过程中容易引起估算误差，将对最终认证信号的提取带来不利影响。

[0007] 此外，Auth-TDM、Auth-SS和Auth-SUP均把包含认证信息这一事实暴露出来了，其中Auth-SS和Auth-TDM技术相较于不包含认证信息的常规信号，极易引起场景中其他用户尤其是敌对用户的注意，敌对用户对信号进行分析，假冒或者篡改，合法接收端将无法对期望信号进行认证。相对而言，Auth-SUP认证技术的隐蔽性要明显高于Auth-SS和Auth-TDM。然而，这种优越性是基于敌对用户的计算能力具有一定限制的前提下的，一旦敌对用户计

算能力提高,也很有可能提取甚至破坏认证信息。

[0008] 不得不提的是,现有的Auth-SS技术和Auth-SUP技术频率选择性衰落信道场景下性能衰退得很厉害。而现实是,随着无线通信用户数量的不断增加,通信环境也会愈加复杂,被干扰的可能性越来越大,而随着市区通信用户数的增加及城市的不断发展,单纯的时不变衰落信道或简单的时变衰落信道已经不足以刻画当前的通信环境。尤其因为城市建筑物的阻挡,使得多径衰落成为常态,因此不得不考虑基于频率选择性衰落信道下的无线通信物理层认证技术,来提高无线通信的安全性,满足用户的通信安全性要求。

发明内容

[0009] 本发明是有鉴于上述的状况而提出的,其目的在于提供一种不需要占用额外的信号带宽、且认证信号不成为影响载体信号中信息信号提取的噪声,不影响接收端噪声的统计特性的基于平滑技术的频率选择性衰落信道的盲认证方法和系统。

[0010] 为此,本发明的第一方面提供了一种基于平滑技术的频率选择性衰落信道的盲认证方法,是具有发射端和接收端的无线通信系统的无线通信的物理层认证方法,其特征在于,包括:所述发射端向无线信道发射载体信号,所述载体信号包括认证信号、导频信号和信息信号,所述认证信号叠加到所述导频信号,所述无线信道是具有多个路径的频率选择性衰落信道;所述接收端接收所述载体信号,顺序地对所述频率选择性衰落信道的每个路径中的所述载体信号进行盲已知干扰消除(Blind Known Interference Cancellation,简称BKIC)处理得到目标信号,对所述目标信号进行差分信号处理以获得目标认证信号,在所述BKIC处理中,利用相邻的码元,通过平滑技术消除所述导频信号;在所述接收端中,基于密钥和所述导频信号获得参考认证信号,并计算所述目标认证信号和所述参考认证信号的相关性,得到检验统计量;并且判断所述检验统计量是否不小于规定阈值,从而确定所述载体信号是否能够通过认证。

[0011] 在本发明中,所述认证信号叠加到所述导频信号。由此,可以不影响接收端的信干噪比。所述BKIC处理利用相邻的码元,通过平滑技术消除所述导频信号。在这种情况下,能够在避免估计信道情况下,消除导频信号。

[0012] 在本发明第一方面所涉及的盲认证方法中,所述载体信号以数据块的形式分块发射。由此,便于对数据进行操作。

[0013] 在本发明第一方面所涉及的盲认证方法中,在每块所述载体信号中,所述导频信号的信号长度与所述信息信号的信号长度和等于所述载体信号的信号长度。

[0014] 另外,在本发明第一方面所涉及的盲认证方法中,利用哈希矩阵,基于所述密钥和所述导频信号获得所述参考信号。由此,参考信号经过处理得到参考认证信号,可以根据参考认证信号与目标认证信号的相关性,确定目标认证信号是否通过认证。

[0015] 在本发明第一方面所涉及的盲认证方法中,若所述检验统计量不小于所述规定阈值,则所述载体信号通过认证。

[0016] 在本发明第一方面所涉及的盲认证方法中,所述规定阈值基于所述导频信号的统计特性以及预设的虚警概率上限得到。

[0017] 本发明的第二方面提供了一种基于平滑技术的频率选择性衰落信道的盲认证设备,其包括处理器,其执行所述存储器存储的计算机程序以实现上述任一项所述的物理层

盲认证方法;以及存储器。

[0018] 本发明的第三方面提供了一种计算机可读存储介质。所述计算机可读存储介质存储有至少一个指令,所述至少一个指令被处理器执行时实现上述第一方面任一项所述的盲认证方法。

[0019] 本发明的第四方面提供了一种基于平滑技术的频率选择性衰落信道的盲认证系统,其包括发射装置,其向无线信道发射载体信号,所述载体信号包括认证信号、导频信号和信息信号,所述认证信号叠加到所述导频信号,所述无线信道是具有多个路径的频率选择性衰落信道;接收装置包括第一处理模块、第二处理模块和判定模块,所述第一处理模块接收所述载体信号,顺序地对所述频率选择性衰落信道的每个路径中的所述载体信号进行盲已知干扰消除(BKIC)处理得到目标信号,对所述目标信号进行差分信号处理以获得目标认证信号,在所述BKIC处理中,利用相邻的码元,通过平滑技术消除所述导频信号;第二处理模块,其基于密钥和所述导频信号获得参考信号,对所述参考信号进行差分信号处理以获得参考认证信号,并计算所述目标认证信号和经过差分信号处理的所述参考认证信号的相关性,得到检验统计量;以及判定模块,其将所述检验统计量与规定阈值进行比较,从而确定所述载体信号是否能够通过认证。

[0020] 在本发明中,盲认证系统的发射装置将认证信号叠加到导频信号。由此,能够不占用额外发射带宽资源。盲认证系统的接收装置BKIC处理利用相邻的码元,通过平滑技术消除所述导频信号。在这种情况下,接收装置能够在避免估计信道情况下,消除导频信号。

[0021] 在本发明第四方面所涉及的盲认证系统中,所述第二处理模块,利用哈希矩阵,基于所述密钥和所述导频信号获得所述参考信号。由此,参考信号经过处理得到参考认证信号,可以根据参考认证信号与目标认证信号的相关性,确定目标认证信号是否通过认证。

[0022] 在本发明第四方面所涉及的盲认证系统中,所述判定模块中所述规定阈值基于所述导频信号的统计特性以及预设的虚警概率上限得到。

[0023] 与现有技术相比,本发明实施方式具备以下有益效果:

[0024] 与现有的Auth-SS、Auth-SUP、Auth-TDM相比,本发明实现无线通信的物理层的认证不需要占用额外的信号带宽,认证信号不成为影响接收信号提取的噪声,不影响接收端噪声的统计特性。本发明提出的盲认证技术处理的是频率选择性衰落信道,更加适应于实际通信场景中复杂多变的无线通信环境。此外,由于本发明中,认证信号是叠加在导频信号中的,如果将认证信号与导频叠加后的信号的整体当成导频信号,用来进行信道估计,还能提高信道估计的准确性。

附图说明

[0025] 图1是示出了本发明的实施方式所涉及的物理层盲认证方法的信号传输示意图。

[0026] 图2是示出了本发明的实施方式所涉及的物理层盲认证方法流程示意图。

[0027] 图3是示出了本发明的实施方式所涉及的物理层盲认证方法发射端发射信号的结构示意图。

[0028] 图4是示出了本发明的实施方式所涉及的物理层盲认证方法接收端盲已知干扰消除(BKIC)处理流程示意图。

[0029] 图5是示出了本发明的实施方式所涉及的物理层盲认证系统发射端信号处理模块

示意图。

[0030] 图6是示出了本发明的实施方式所涉及的物理层盲认证系统接收端信号处理模块示意图。

[0031] 图7是示出了本发明的实施方式所涉及的一种物理层盲认证设备的结构示意图。

具体实施方式

[0032] 以下，参考附图，详细地说明本发明的优选实施方式。在下面的说明中，对于相同的部件赋予相同的符号，省略重复的说明。另外，附图只是示意性的图，部件相互之间的尺寸的比例或者部件的形状等可以与实际的不同。

[0033] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0034] 本实施方式公开了一种基于平滑技术的频率选择性衰落信道的盲认证方法、设备和系统，是具有发射端和接收端的无线通信系统的无线通信的物理层认证方法、设备和系统。也即本实施方式公开了一种基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证方法、设备和系统。其能够更加准确地对进行物理层认证。以下结合附图进行详细描述。

[0035] 图1是示出了本发明的实施方式所涉及的物理层盲认证方法的信号传输示意图。

[0036] 在本实施方式中，如图1所示，基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证方法基于一个通用的信号传输模型。在这个信号传输模型中，共包含4个用户，其中发送方(发射端)是合法发送方，发射端发射信号给合法接收方，即接收端，另外两个接收方分别为系统中监听用户和敌对用户。敌对用户一旦发现发射端发出的信号中可能有认证信息，将对该信号进行分析并试图提取、破坏、甚至篡改认证信息。但本实施方式不限于此，发射端可以是两个或两个以上，合法接收方可以是两个或两个以上，监听用户和敌对用户也可以分别是两个或两个以上。

[0037] 在本实施方式中，假设发射端和接收端共同拥有用于认证的密钥，使得接收端可以利用该密钥从发射端发射的信号中提取认证信息。认证信号包含有认证信息。在本实施方式中，载体信号包含认证信号，常规信号不包含认证信号。监听用户对于认证方法一无所知，尽管可以接受并恢复发射端发送的信号，但是不会对信号进行深入的分析，不影响认证过程。敌对用户通过分析信号的特点可以察觉到认证信号的存在，并意图破坏认证信号。

[0038] 在本实施方式中，上述的信号模型中的发射端可以包括基站或用户设备。基站(例如接入点)可以是指接入网中在空中接口上通过一个或多个扇区与无线终端通信的设备。基站可用于将收到的空中帧与IP分组进行相互转换，作为无线终端与接入网的其余部分之间的路由器，其中，接入网的其余部分可包括网际协议(IP)网络。基站还可以协调对空中接口的属性管理。例如，基站可以是GSM或CDMA中的基站(BTS，Base Transceiver Station)，也可以是WCDMA中的基站(NodeB)，还可以是LTE中的演进型基站(NodeB或eNB或e-NodeB，

evolutional Node B)，本实施方式不做限定。

[0039] 用户设备可以包括但不限于智能手机、笔记本电脑、个人计算机(Personal Computer,PC)、个人数字助理(Personal Digital Assistant,PDA)、移动互联网设备(Mobile Internet Device,MID)、穿戴设备(如智能手表、智能手环、智能眼镜)等各类电子设备，其中，该用户设备的操作系统可包括但不限于Android操作系统、IOS操作系统、Symbian(塞班)操作系统、Black Berry(黑莓)操作系统、Windows Phone8操作系统等等，本实施方式不做限定。

[0040] 在本实施方式中，上述的信号模型中的发射端发送信号经过无线信道到达接收端，其中，接收端可以包括基站。基站(例如接入点)可以是指接入网中在空中接口上通过一个或多个扇区与无线终端通信的设备。基站可用于将收到的空中帧与IP分组进行相互转换，作为无线终端与接入网的其余部分之间的路由器，其中，接入网的其余部分可包括网际协议(IP)网络。基站还可以协调对空中接口的属性管理。例如，基站可以是GSM或CDMA中的基站(BTS,Base Transceiver Station)，也可以是WCDMA中的基站(NodeB)，还可以是LTE中的演进型基站(NodeB或eNB或e-NodeB,evolutional Node B)，本实施方式不做限定。

[0041] 接收端还可以包括用户设备，用户设备可以包括但不限于智能手机、笔记本电脑、个人计算机(Personal Computer,PC)、个人数字助理(Personal Digital Assistant,PDA)、移动互联网设备(Mobile Internet Device,MID)、穿戴设备(如智能手表、智能手环、智能眼镜)等各类电子设备，其中，该用户设备的操作系统可包括但不限于Android操作系统、IOS操作系统、Symbian(塞班)操作系统、Black Berry(黑莓)操作系统、Windows Phone8操作系统等等，本实施方式不做限定。

[0042] 本实施方式公开一种基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证方法。图2是示出了本发明的实施方式所涉及的物理层盲认证方法流程示意图。图3是示出了本发明的实施方式所涉及的物理层盲认证方法发射端发射信号的结构示意图。

[0043] 在本实施方式中，基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证方法是具有发射端和接收端的无线通信系统的无线通信的物理层认证方法。基于上述的信号传输模型，如图2所示，发射端向无线信道发射载体信号。载体信号包括认证信号、导频信号和信息信号。认证信号叠加到导频信号。无线信道是具有多个路径的频率选择性衰落信道(步骤S101)。

[0044] 在步骤S101中，如图3所示，载体信号包括认证信号、导频信号和信息信号，认证信号叠加到导频信号上。认证信号的信号长度等于导频信号的信号长度。由此，认证信号叠加到导频信号可以避免占用额外的信号带宽。

[0045] 在本实施方式中，信息信号包含发射端用户所要传递的信息。发射端发送的载体信号是以数据块的形式分块发射的。每块载体信号包括导频部分和信息部分。导频部分包括认证信号和导频信号，信息部分包括信息信号。另外，载体信号以数据块的形式分块发射，有利于对数据进行操作。

[0046] 在本实施方式中，认证信号或导频信号的信号长度是第一长度，信息信号的信号长度是第二长度，每块载体信号的长度是总长度。认证信号或导频信号的信号长度与信息信号的信号长度和等于每块载体信号的长度。即第一长度与第二长度的和等于总长度。

[0047] 在本实施方式中，认证信号是通过导频信号和密钥得到的。也即导频信号和密钥

利用哈希矩阵得到了认证信号。将得到的认证信号叠加到导频信号上，得到了每块载体信号的导频部分，导频部分的信号表达式是如下：

[0048] $m_i=\rho_s p_i+\rho_t t_i$ (1)

[0049] 上述导频部分的信号表达式(1)中，ρ_s^2 和 ρ_t^2 为导频信息和认证信号的功率分配因子。假设认证信号和导频信号是相互独立的，则有 $\mathbb{E}\left\{\mathbf{p}_i^H\mathbf{t}_i\right\}=0$。

[0050] 在本实施方式中，将导频部分的信号和信息部分的信息信号组合在一起，构成了每块载体信号。

[0051] 另外，在本实施方式中，载体信号的传输信道是无线信道，并且是频率选择性衰落信道。频率选择性衰落信道具有多个路径，即频率选择性衰落信道是多路径信道。经过频率选择性衰落信道后载体信号表达式是如下：

[0052] $y_{iL+k}=h_{iL+k}x_{iL+k}+n_{iL+k}$ (2)

[0053] 在本实施方式中，频率选择性衰落信道的信道响应 h_{iL+k}，服从0均值方差为 σ_h^2 的复高斯分布，$n_{iL+k}\sim\mathcal{CN}\left(0,\sigma_n^2\right)$ 为接收端的噪声，服从0均值方差为 σ_n^2 的高斯随机变量。

[0054] 在本实施方式中，在信道响应中，$\omega_{iL+k}\sim\mathcal{CN}\left(0,\sigma_\omega^2\right)$ 为动态噪声，且 $\sigma_\omega^2=\left(1-a^2\right)\sigma_h^2$。一般情况下，频率选择性衰落信道的衰落相关系数a，由信道多普勒扩展和发射带宽所决定。特别地，a值较小时表示快衰落，a值较大时表示慢衰落。在许多类型的场景中，a的值在接收端是可以获取的。而在实际无线系统场景中，a的取值范围在一个非常小的区间内，如 $a\in[0.9,1]$。

[0055] 在本实施方式中，物理层盲认证方法还包括接收端接收载体信号，顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除(BKIC)处理得到目标信号。在BKIC处理中，利用相邻的码元，通过平滑技术消除导频信号(步骤S102)。

[0056] 在本实施方式中，接收端接收载体信号。载体信号中包含导频部分和信息部分。本实施方式所涉及的物理层盲认证方法在接收端主要是针对载体信号的导频部分进行处理。接收端接收的载体信号的导频部分的表达式是如下：

[0057] $$y_k=\sum_{d=0}^{D_{\max}}h_{k,d}\left(\rho_s p_{k-d}+\rho_t t_{k-d}\right)+n_k,\quad iL\le k\le iL+L_1 \qquad (3)$$

[0058] 在本实施方式中，无线信道是频率选择性衰落信道。频率选择性衰落信道具有多个路径。其中，D_{max} 为多径中最大的延时信息，通常在宽带无线通信系统中 D_{max} 都是已知的。例如，在正交频分复用(OFDM)系统中，预定义的循环前缀决定了所有路径中最大的延时。

[0059] 在本实施方式中，下述针对载体信号的处理指的是针对载体信号的导频部分的处理。

[0060] 在本实施方式中，对频率选择性衰落信道的每个潜在的路径上使用盲认证技术。具体而言，首先，可以对频率选择性衰落信道的第一路径中的载体信号进行盲已知干扰消除(BKIC)处理，然后，类似的可以用相同的盲已知干扰消除(BKIC)处理方法除去频率选择性衰落信道的第二路径中的载体信号中的导频信号，重复 $D_{max}+1$ 次上述的盲已知干扰消除(BKIC)处理过程，使得频率选择性衰落信道的每个路径中的载体信号中的导频信号被顺序

地消除。也即顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除(BKIC)处理。

[0061] 步骤S102中，接收端接收载体信号，顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除(BKIC)处理得到目标信号。其中，盲已知干扰消除(BKIC)处理是利用相邻的码元，通过平滑技术消除载体信号中的导频信号。通常将载体信号中的导频信号消除需要估计信道情况，若信道响应不能进行有效估计，载体信号中的导频信号很难消除。盲已知干扰消除方法可以在避免估计信道情况下，消除导频信号。

[0062] 在本实施方式中，接收端接收到的载体信号可能包含认证信号，也可能不包含认证信号。设载体信号包含认证信息为第一条件，设载体信号不包含认证信号为第二条件。

[0063] 图4是示出了本发明的实施方式所涉及的物理层盲认证方法接收端盲已知干扰消除(BKIC)处理流程示意图。

[0064] 在本实施方式中，如图4所示，在频率选择性衰落信道的每个路径上，消除载体信号中导频信号的方法一样。具体而言，频率选择性衰落信道的每个路径上的载体信号都是通过BKIC处理方法消除导频信号的。BKIC处理方法包括确定不同条件下每个码元的表达式(步骤S401)和利用码元的表达式，估算目标信号(步骤S402)。

[0065] 在步骤S401中，确定不同条件下每个码元的表达式。

[0066] 其中，在第一条件下，每个码元的表达式如下：

[0067] $$b_k|H_1 = y_k - \frac{p_k}{ap_{k+1}}y_{k+1} = h_k\rho_t t_k + n_k - \frac{p_k}{ap_{k+1}}\left(h_{k+1}\rho_t t_{k+1} + n_{k+1}\right) - \frac{\omega_{k+1}\rho_s p_k}{a} \quad (4)$$

[0068] $k \in \{1,2,\cdots,L_1-1\}$

[0069] 在第二条件下，每个码元的表达式如下：

[0070] $$b_k|H_0 = n_k - \frac{p_k}{ap_{k+1}}n_{k+1} + \frac{\omega_{k+1}p_k}{a} \quad (5)$$

[0071] 从上述的公式中可以看出，相邻的码元间存在相关噪声，表达式(4)中的相关噪声不能用普通的噪声白化技术来校正，需要通过步骤S402来消除相关噪声，估算出$h_k\rho_t t_k+n_k$。

[0072] 在步骤S402中，利用码元的表达式，估算目标信号，将上述表达式(4)表示如下：

[0073] $$u_1 = b_1 = h_1\rho_t t_1 + n_1 - \frac{p_1}{ap_2}\left(h_2\rho_t t_2 + n_2\right) - \frac{\omega_2\rho_s p_1}{a} \quad (6)$$

[0074] $$\begin{aligned} u_k &= u_{k-1} + \frac{p_1}{a^{k-1}p_k}b_k = p_1\sum_{m=1}^{k}\frac{b_m}{a^{m-1}p_m} \\ &= h_1\rho_t t_1 + n_1 - \frac{p_1}{a^k p_{k+1}}\left(h_{k+1}\rho_t t_{k+1} + n_{k+1}\right) - \rho_s p_1\sum_{m=1}^{k}\frac{\omega_{m+1}}{a^m},\ k \in \{2,\cdots,L_1-1\} \end{aligned} \quad (7)$$

[0075] 可以得到估算结果如下：

[0076] $$z_1 = \frac{1}{L_1-1}\sum_{k=1}^{L_1-1}u_k = h_1\rho_t t_1 + n_1 + \varepsilon_1 \quad (8)$$

[0077] $$z_k = \frac{a^{k-1}p_k}{p_1}\left(z_1 - u_{k-1}\right) = h_k\rho_t t_k + n_k + \varepsilon_k \quad (9)$$

[0078] 其中，表达式(9)中ε_k是由于BKIC模块进行干扰消除过程中产生的残余信号，ε_k可以被建模成高斯分布，对于慢衰落来说，$(a\rightarrow 1)$，ε_k的方差很小，因此可以将y_k中的ε_k去除，得到估算的$h_k\rho_t t_k+n_k$。将每个路径中估算的$h_k\rho_t t_k+n_k$相加，得到估算的不含导频信号的目标

信号。

[0079] 另外，在步骤S102中，载体信号经过BKIC处理后得到目标信号，目标信号进行差分信号处理，得到目标认证信号。

[0080] 在本实施方式中，差分信号处理的方法如下：

[0081] 第一条件下，差分信号处理的表达式如下：

[0082] $$r_k\left|H_1=\frac{1}{\rho_t^2}z_k z_{k+1}^*=a\left|h_k\right|^2 t_k t_{k+1}^*+\Delta_k,\ iL\le k\le iL+L_1-1 \qquad (10)$$

[0083] 其中Δ_k为残余信号，可以近似建模为0均值方差为$\sigma_{\Delta_k}^2$的高斯随机变量。

[0084] 在第二条件下，差分信号处理的表达式如下：

[0085] $$r_k\left|H_0=\frac{1}{\rho_t^2}\left(n_k+\varepsilon_k\right)\left(n_{k+1}+\varepsilon_{k+1}\right)^*=\nabla_k \qquad (11)$$

[0086] 其中∇_k为零均值复高斯随机变量。

[0087] 在本实施方式中，物理层盲认证方法还包括在接收端中，基于密钥和导频信号获得参考信号，对参考信号进行差分信号处理以获得参考认证信号，并计算目标认证信号和参考认证信号的相关性，得到检验统计量(步骤S103)。

[0088] 在步骤S103中，基于密钥和导频信号获得参考信号是指利用哈希矩阵，由密钥和导频信号获得参考信号。由此，参考信号经过处理得到参考认证信号，可以根据参考认证信号与目标认证信号的相关性，确定目标认证信号是否通过认证。

[0089] 在步骤S103中，对参考信号进行差分信号处理以获得参考认证信号，计算目标认证信号和参考认证信号的相关性，得到检验统计量，可以根据检验统计量的值进行下一步判断。

[0090] 在本实施方式中，对参考信号进行差分信号处理以获得参考认证信号。差分信号处理的方法与上述步骤S102中的差分处理方法相同。

[0091] 在上述步骤S102中，接收端接收到的载体信号可能包含认证信号，设载体信号包含认证信息为第一条件，设载体信号不包含认证信号为第二条件。

[0092] 其中，在接收端，载体信号顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除(BKIC)处理得到目标信号，对目标信号进行差分信号处理以获得目标认证信号。在接收端，基于密钥和导频信号获得参考信号，参考信号经过差分(DP)信号处理后得到参考认证信号。接收端的哈希矩阵、密钥和导频信号生成参考信号的规则与发送端的哈希矩阵、密钥和导频信号生成认证信号的规则相同。参考认证信号可以看做是第一条件中的认证信号，目标认证信号可以看做是第一条件中的载体信号。由此，第一条件可以表示为目标认证信号中包括参考认证信号；第二条件可以表示为目标认证信号中不包括参考认证信号。

[0093] 在本实施方式中，物理层盲认证方法还包括将检验统计量与规定阈值进行比较，从而确定载体信号是否能够通过认证(步骤S104)。

[0094] 在步骤S104中，若检验统计量不小于规定阈值，则判定载体信号通过认证；若检验统计量小于规定阈值，则判定载体信号没有通过认证。

[0095] 在本实施方式中，若检验统计量不小于规定阈值，则载体信号中包含参考认证信

号，即载体信号通过认证；若检验统计量小于规定阈值，则载体信号中不包含参考认证信号，即载体信号没有通过认证。

[0096] 另外，在本实施方式中，规定阈值是通过假设验证条件得到的，上述的第一条件和第二条件分别是假设验证条件的第一条件H_1和第二条件H_0。

[0097] 在本实施方式中，第一条件H_1下，检验统计量的表达式如下：

[0098] $$\tau_i \left| H_1 = \mathbf{d}_i^H \mathbf{r}_i = a\sum_{k=1}^{L_1-1} \left| h_{iL+k} t_{iL+k} t_{iL+k+1} \right|^2 + v_i \right. \qquad (12)$$

[0099] 第二条件H_0下，检验统计量的表达式如下：

[0100] $$\tau_i \left| H_0 = \phi_i = \sum_{k=1}^{L_1-1} t_k^* t_{k+1} \nabla_k \right. \qquad (13)$$

[0101] 其中，$v_i = \sum_{k=1}^{L_1-1} t_k^* t_{k+1} \Delta_k$为0均值方差为$\sigma_{v_i}^2 = (L_1-1)\sigma_\Delta^2 \sigma_p^4$的高斯随机变量，$\Phi_i$是0均值方差为$\sigma_{\phi_i}^2 = (L_1-1)\sigma_\nabla^2 \sigma_p^4$的高斯随机变量。

[0102] 另外，规定阈值τ_i^0由$(\tau_i | H_0)$分布相关的虚警概率ε_{FA}决定，表示如下：

[0103] $$\tau_i^0 = \arg\min_{\tau} \Phi\left(\tau / \sigma_{\phi_i}\right) \geq 1 - \varepsilon_{\mathrm{FA}} \qquad (14)$$

[0104] 其中$(\tau_i | H_0)$是在第二条件下得到的检验统计量，也即导频信号的统计特性。由此，规定阈值可以基于导频信号的统计特性以及预设的虚警概率上限得到。

[0105] 另外，在本实施方式中，如果发射端的身份被认证后，将认证信号可以当成额外的导频信号来恢复信号。由此，可以提高信号码元恢复的性能和对信道响应的估计性能。

[0106] 另外，在本实施方式中，认证信号叠加到导频信号，避免了对常规信号的提取带来的不利影响。由此，避免降低接收端的信干噪比(SINR)。

[0107] 本实施方式中，基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证方法不需要占用额外的信号带宽。另外，在接收端，对载体信号进行信息信号提取时，认证信号不会成为信息信号的噪声，即认证信号不会影响信息信号的提取。认证信号不影响接收端噪声的统计特性。

[0108] 在本实施方式中，物理层盲认证方法处理的是具有多个路径的频率选择性衰落信道，也即多路径信道，更加适应于实际通信场景中复杂多变的无线通信环境。另外，认证信号是叠加在导频信号中的，如果将认证信号与导频叠加后的信号的整体当成导频信号，用来进行信道估计，还能提高信道估计的准确性。

[0109] 本实施方式公开一种基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证系统。图5是示出了本发明的实施方式所涉及的物理层盲认证系统发射端信号处理模块示意图。图6是示出了本发明的实施方式所涉及的物理层盲认证系统接收端信号处理模块示意图。

[0110] 在本实施方式中，如图5所示，物理层盲认证系统包括发射装置20。发射装置20包括第一生成模块201、第二生成模块202和合成模块203。

[0111] 在本实施方式中，如图5所示，第一生成模块201生成认证信号。也即密钥和导频信号经过第一生成模块201生成认证信号。第一生成模块201中包含哈希矩阵。认证信号是密

钥和导频信号利用哈希矩阵得到的。其中，得到的认证信号与导频信号的信号长度相同。

[0112] 在本实施方式中，如图5所示，第二生成模块202生成了载体信号的导频部分。也即认证信号通过第二生成模块202加载到导频信号上，生成载体信号的导频部分。载体信号的导频部分的表达式为公式(1)，另外，载体信号的导频部分的长度为认证信号的信号长度或导频信号的信号长度。

[0113] 在本实施方式中，如图5所示，合成模块203生成了载体信号。也即载体信号的导频部分和信息部分通过合成模块203组合在一起，生成载体信号。载体信号的信息部分是信息信号。

[0114] 在本实施方式中，载体信号是按数据块分块发送的。每块载体信号包括导频部分和信息部分。认证信号或导频信号的信号长度与信息信号的信号长度和等于每块载体信号的长度。另外，载体信号是以数据块的形式分块发射有利于对数据进行操作。

[0115] 在本实施方式中，发射端的发射装置20生成的载体信号经过无线信道到达接收端的接收装置30。另外，无线信道是具有多个路径的频率选择性衰落信道。

[0116] 在本实施方式中，物理层盲认证系统还包括接收装置30。接收装置30包括第一处理模块、第二处理模块和判定模块。

[0117] 在本实施方式中，第一处理模块包括盲已知干扰消除(BKIC)模块301。载体信号经过盲已知干扰消除(BKIC)模块301。具体而言，频率选择性衰落信道的每个路径中的载体信号顺序地经过盲已知干扰消除(BKIC)模块301进行盲已知干扰消除(BKIC)处理，消除了载频信号中的导频信号。

[0118] 在本实施方式中，盲已知干扰消除(BKIC)模块301运用了步骤S102中利用相邻的码元，通过平滑技术消除导频信号的BKIC处理方法。具体步骤如图4所示，BKIC处理包括确定不同条件下每个码元的表达式(步骤S401)和利用码元的表达式，估算目标信号(步骤S402)。

[0119] 在本实施方式中，如图6所示，第一处理模块还包括差分(DP)处理模块302。DP处理模块302运用了步骤S102中差分信号处理方法。DP处理模块302对目标信号进行差分信号处理，得到目标认证信号。由此，消除了目标认证信号中h_k的影响，也即消除信道对载体信号的影响。

[0120] 在DP处理模块302中，第一条件下，差分信号处理的表达式为公式(10)，其中Δ_k为残余信号，可以近似建模为0均值方差为$\sigma_{\Delta_k}^2$的高斯随机变量。在第二条件下，差分信号处理的表达式为公式(11)，其中∇_k为零均值复高斯随机变量。

[0121] 在本实施方式中，如图6所示，第二处理模块还包括哈希矩阵处理模块303。导频信号和密钥通过哈希矩阵处理模块303得到参考信号。哈希矩阵处理模块303运用了步骤S103中生产参考信号的方法。哈希矩阵处理模块303中包括哈希矩阵。

[0122] 在本实施方式中，如图6所示，第二处理模块还包括差分(DP)处理模块304。差分(DP)处理模块304对参考信号进行差分信号处理，得到参考认证信号。DP处理模块304运用了步骤S103中差分信号处理方法。

[0123] 在本实施方式中，如图6所示，第二处理模块还包括运算模块305。运算模块305用来计算目标认证信号和参考认证信号的检验统计量。运算模块305运用的计算方法是步骤

S103中的计算方法。

[0124] 在本实施方式中，如图6所示，第二处理模块还包括判定模块306。判定模块306通过比较检验统计量和规定阈值，确定目标认证信号是否通过认证。也即确定载体信号是否能够通过认证。

[0125] 在本实施方式中，判定模块306中的规定阈值是基于导频信号的统计特性以及预设的虚警概率上限得到。规定阈值的计算方法为步骤S103中的阈值计算方法。

[0126] 本实施方式公开一种基于平滑技术的无线通信频率选择性衰落信道的物理层盲认证设备50。图7是示出了本发明的实施方式所涉及的一种物理层盲认证设备的结构示意图。在本实施方式中，发射端与接收端都包含如图7所示的认证设备50。

[0127] 在本实施方式中，如图7所示，认证设备50包括处理器501和存储器502。其中，处理器501以及存储器502分别连接通信总线。存储器502可以是高速RAM存储器，也可以是非易失性的存储器(non-volatile memory)。本领域技术人员可以理解，图7中示出的认证设备50的结构并不构成对本发明的限定，它既可以是总线形结构，也可以是星型结构，还可以包括比图7所示的更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0128] 其中，处理器501为认证设备的控制中心，可以是中央处理器(Central Processing Unit，CPU)，处理器501利用各种接口和线路连接整个认证设备的各个部分，通过运行或执行存储在存储器502内的软件程序和/或模块，以及调用存储在存储器502内存储的程序代码，用于执行以下操作：

[0129] 发射端向无线信道发射载体信号，载体信号包括认证信号、导频信号和信息信号，认证信号叠加到导频信号，无线信道是具有多个路径的频率选择性衰落信道(由发射端的认证设备50执行)。

[0130] 接收端接收载体信号，顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除(BKIC)处理得到目标信号，对目标信号进行差分信号处理以获得目标认证信号，在BKIC处理中，利用相邻的码元，通过平滑技术消除导频信号；在接收端中，基于密钥和导频信号获得参考信号，对参考信号进行差分信号处理以获得参考认证信号，并计算目标认证信号和参考认证信号的相关性，得到检验统计量；并且将检验统计量与规定阈值进行比较，从而确定载体信号是否能够通过认证(由接收端的认证设备50执行)。

[0131] 在本实施方式中，发射端的认证设备50的处理器501的还执行以下操作：载体信号以数据块的形式分块发射。

[0132] 在本实施方式中，发射端的认证设备50的处理器501的还执行以下操作：在每块载体信号中，导频信号的信号长度与信息信号的信号长度和等于载体信号的信号长度。

[0133] 在本实施方式中，接收端的认证设备50的处理器501的还执行以下操作：利用哈希矩阵，基于密钥和导频信号获得参考信号。

[0134] 在本实施方式中，接收端的认证设备50的处理器501的还执行以下操作：若检验统计量不小于规定阈值，则载体信号通过认证。

[0135] 在本实施方式中，接收端的认证设备50的处理器501的还执行以下操作：规定阈值基于导频信号的统计特性以及预设的虚警概率上限得到。

[0136] 在本实施方式中，应该理解到，所揭露的设备，可通过其它的方式实现。例如，以上所描述的设备实施方式仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，

实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

[0137] 作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0138] 另外，在本发明实施方式中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0139] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储器中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储器中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储器包括：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0140] 本实施方式公开一种计算机可读存储介质，本领域普通技术人员可以理解上述实施方式的各种物理层盲认证方法中的全部或部分步骤是可以通过程序(指令)来指令相关的硬件来完成，该程序(指令)可以存储于计算机可读存储器(存储介质)中，存储器可以包括：闪存盘、只读存储器(英文：Read-Only Memory，简称：ROM)、随机存取器(英文：Random Access Memory，简称：RAM)、磁盘或光盘等。

[0141] 虽然以上结合附图和实施例对本发明进行了具体说明，但是可以理解，上述说明不以任何形式限制本发明。本领域技术人员在不偏离本发明的实质精神和范围的情况下可以根据需要对本发明进行变形和变化，这些变形和变化均落入本发明的范围内。

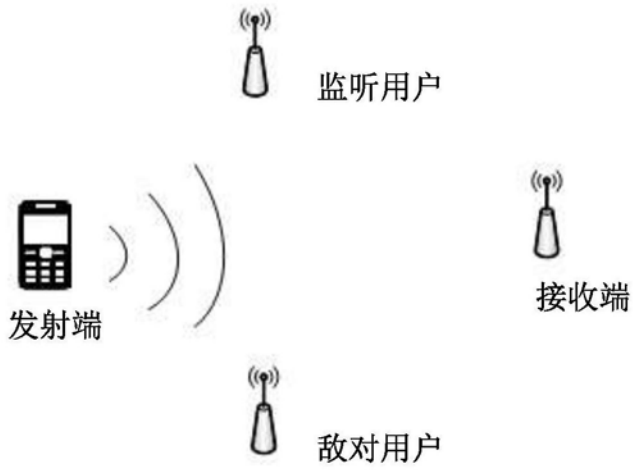

监听用户
发射端
接收端
敌对用户

图1

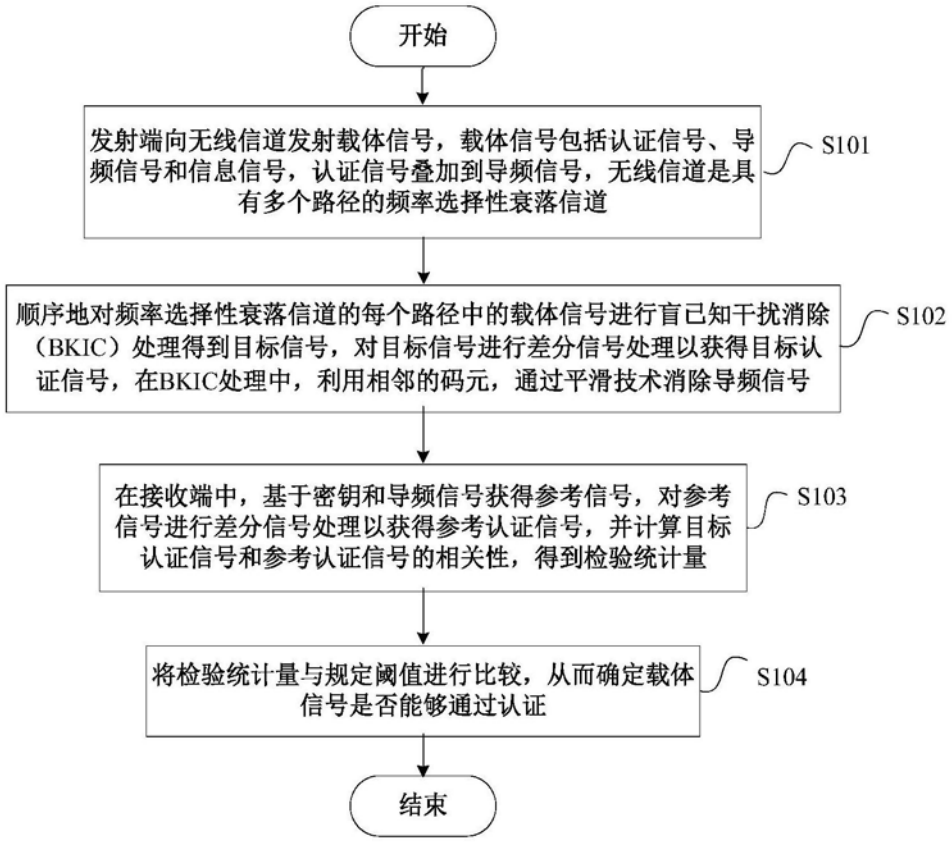

开始
发射端向无线信道发射载体信号，载体信号包括认证信号、导频信号和信息信号，认证信号叠加到导频信号，无线信道是具有多个路径的频率选择性衰落信道
S101
顺序地对频率选择性衰落信道的每个路径中的载体信号进行盲已知干扰消除（BKIC）处理得到目标信号，对目标信号进行差分信号处理以获得目标认证信号，在BKIC处理中，利用相邻的码元，通过平滑技术消除导频信号
S102
在接收端中，基于密钥和导频信号获得参考信号，对参考信号进行差分信号处理以获得参考认证信号，并计算目标认证信号和参考认证信号的相关性，得到检验统计量
S103
将检验统计量与规定阈值进行比较，从而确定载体信号是否能够通过认证
S104
结束

图2

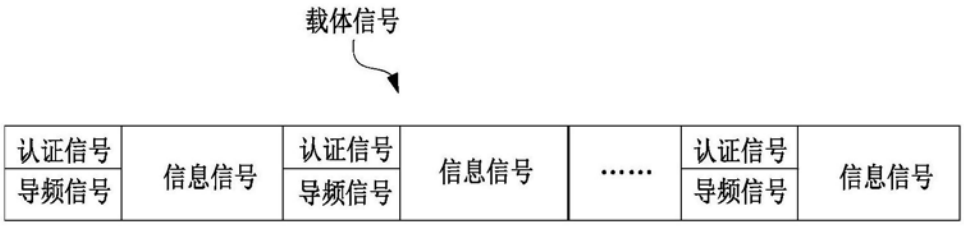

载体信号
认证信号
导频信号
信息信号
认证信号
导频信号
信息信号
……
认证信号
导频信号
信息信号

图3

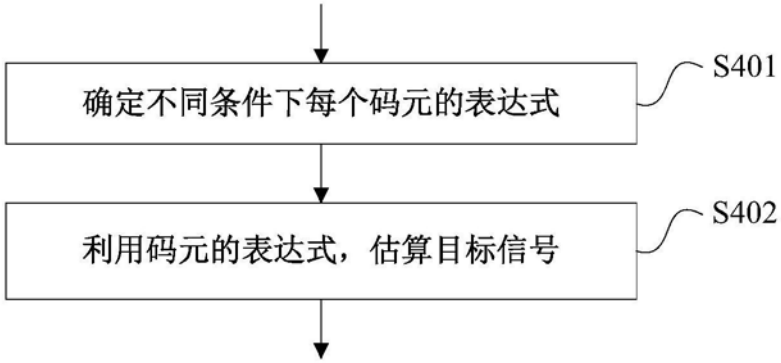

确定不同条件下每个码元的表达式
S401
利用码元的表达式，估算目标信号
S402

图4

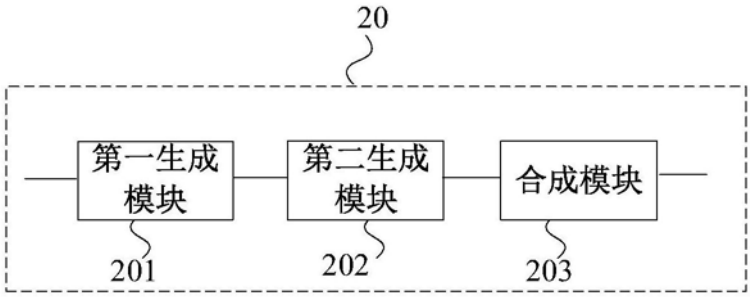

20
第一生成模块
第二生成模块
合成模块
201
202
203

图5

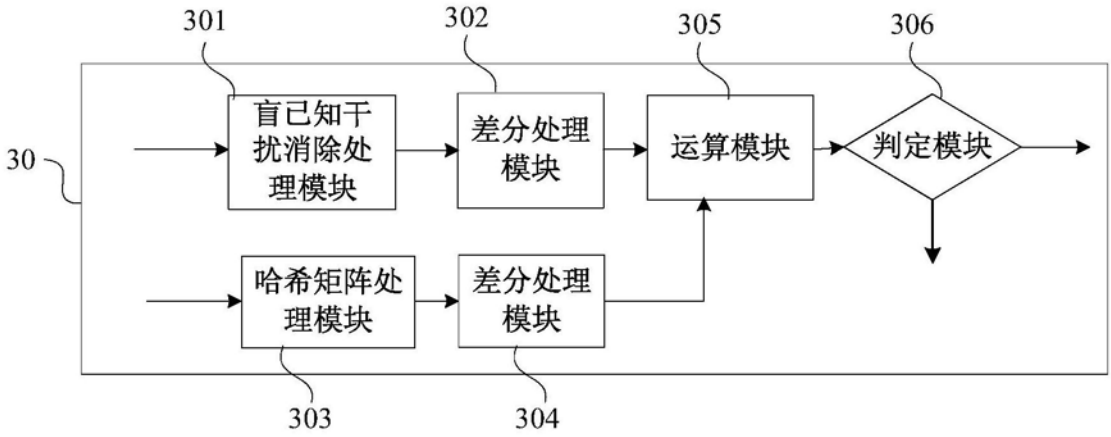

301
302
305
306
30
盲已知干扰消除处理模块
差分处理模块
运算模块
判定模块
哈希矩阵处理模块
差分处理模块
303
304

图6

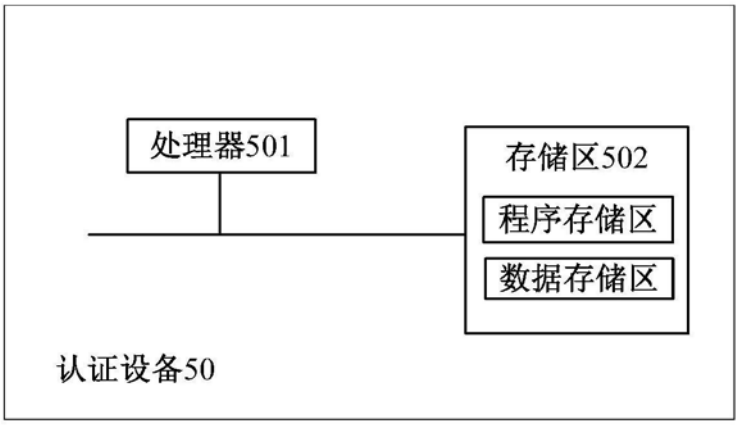

处理器501
存储区502
程序存储区
数据存储区
认证设备50

图7