(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 12 月 19 日 (19.12.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/237476 A1

(51) 国际专利分类号:
H04B 17/391 (2015.01) *H04L 25/02* (2006.01)

(21) 国际申请号: PCT/CN2018/099051

(22) 国际申请日: 2018 年 8 月 6 日 (06.08.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810616004.0 2018年6月14日 (14.06.2018) CN

(71) 申请人: 西 安 交 通 大 学 (**XI'AN JIAOTONG UNIVERSITY**) [CN/CN]; 中国陕西省西安市咸宁西路28号, Shaanxi 710049 (CN)。

(72) 发明人: 任 品 毅 (**REN, Pinyi**); 中国陕西省西安市咸宁西路 28 号, Shaanxi 710049 (CN)。 徐 东 阳 (**XU, Dongyang**); 中国陕西省西安市咸宁西路 28 号, Shaanxi 710049 (CN)。 王 熠 晨 (**WANG, Yichen**); 中国陕西省西安市咸宁西路28号, Shaanxi 710049 (CN)。

(74) 代理人: 西 安 通 大 专 利 代 理 有 限 责 任 公 司(**XI'AN TONG DA PATENT AGENCY CO., LTD.**); 中国陕西省西安市高新区锦业路 32 号, Shaanxi 710049 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) **Title:** OFDM CHANNEL TRAINING AUTHENTICATION METHOD BASED ON INDEPENDENT CHECK CODING

(54) 发明名称: 一种基于独立性校验编码的OFDM信道训练鉴权方法

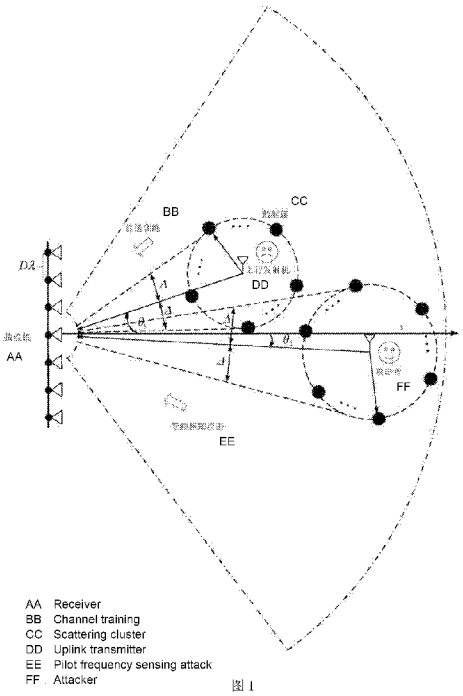

图 1

(57) **Abstract:** An OFDM channel training authentication method based on independent check coding. The method is used for preventing interference, zeroing and cheating risks suffered by pilot frequencies. The pilot frequencies are randomized, are inserted into subcarriers and are coded to correspond to subcarrier activation patterns (SAPs). Although the coded SAPs are masked by malicious signals, the coded SAPs may be identified and decoded into original pilot frequency signals and are further used for high-precision channel impulse response (CIR) estimation, thereby successfully solving the problem of channel estimation in a pilot frequency attack environment. In the present invention, subcarrier coding and channel estimation are combined, and high-security and high-stability wireless channel training authentication is implemented in an attack environment by means of bit rate optimization and channel estimation.

(57) 摘要: 一种基于独立性校验编码的OFDM信道训练鉴权方法，用以避免导频遭受的干扰、归零和欺骗风险。导频不仅仅被随机化并插入到子载波中，同时也被编码、对应为子载波激活模式(SAP)。这些经过编码的SAP虽然被恶意信号掩盖，却是可以被识别并解码成原始导频信号，并进一步被用于高精度的信道冲击响应(CIR)估计，成功解决导频攻击环境下的信道估计难题。本发明联合子载波编码和信道估计，通过优化码率和信道估计，实现了攻击环境下高安全性、高稳定性的无线信道训练鉴权。

WO 2019/237476 A1

[见续页]

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种基于独立性校验编码的 OFDM 信道训练鉴权方法

技术领域

本发明涉及到无线通信领域，特别涉及一种基于独立性校验编码的 OFDM 信道训练鉴权方法。

背景技术

当前无线通信技术面临严重的安全风险，这种风险源于无线信道的广播特性，具体表现为有害信号源危害干扰其他正常节点的通信链路。虽然上层的密码加密解密体制可以在一定程度上保证无线通信环境的安全性，但是随着计算机技术的发展，上层的加密体制面临被破译的风险，合法用户的信息进而完全暴露于敌对目标。基于此，物理层安全机制引起了广泛的关注和研究，鉴于 OFDM 系统作为当前主流的无线通信系统架构并且被广泛应用于各个实际的无线通信系统中，针对该系统的攻击逐渐成为热点话题，攻击者可以获取该系统的协议和架构特征，对其造成严重的威胁。

研究物理层的信道训练协议。在 OFDM 系统中，信道训练的目的是利用公共已知的导频进行信道估计,这些导频信号可被攻击者获知， 当攻击者获悉合法收发机的帧同步信息和导频信息后，可发动导频感知攻击，期间，该攻击者通过与某一合法用户同步地发送特定的导频信号，干扰合法收发机配对之间信道估计，瘫痪系统的下一步数据传输服务。而且，导频感知攻击一旦成功实施后，合法收发机很难再获取精确的合法链路信道状态信息。因此，关键在于如何设计导频鉴权机制来抵抗和削弱 OFDM 系统中的导频感知攻击对信道训练的影响。

发明内容

本发明的目的在于提供一种基于独立性校验编码的 OFDM 信道训练鉴权方法，以解决上述问题。

为实现上述目的，本发明采用以下技术方案：

一种基于独立性校验编码的 OFDM 信道训练鉴权方法，包括以下步骤：

步骤 1，建立系统模型；采用随机导频机制，上行发射机采用随机导频进行信道估计，主动攻击者可采取混合攻击模式；混合攻击模式包括部分频带干扰合法信道的信道训练、全频带干扰合法信道训练和保持静默；

步骤 2，通过对各个子载波激活模式的编码，创建了码频域，构建了独立性校验编码准则；考虑 3 个 OFDM 符号时间，对任意单个子载波上收到的信号进行能量检测，通过配置阈值，实现每个子载波上精准的信号个数检测，若存在信号，则该子载波被编码为 1，反之则为 0；根据得到的二进制编码，得到二元码字向量集合为：$S=\left\{\mathbf{s}=\left[s_{1\le m\le L_s}\right]\middle| s_m\in\{0,1\},1\le m\le L_s\right\}$，其中，$L_s$ 表示码字的长度，s_m 表示第 m 个码字单元，；建立码频域为：$(\mathbf{s},b),\mathbf{s}\subset S,1\le b\le N$，其中 b 表示码字 $\mathbf{s}$ 对应频域的位置，N 表示占用的子载波个数；最后得到一个 $N\times C$ 的二元码本 $\mathbf{C}=\left[c_{i,j}\right]$，码本中第 i 个码字定义为 $\mathbf{c}_i=\left[c_{1,i}\quad\cdots\quad c_{N,i}\right]^{\mathrm{T}}$；

构建独立性校验编码准则，包括编码准则和解码准则，用以抵抗混合攻击；

步骤 3，构建基于独立性校验编码 ICC 的反攻击信道训练鉴权 CTA 协议，包括导频的表示，分离和识别；

步骤 4，优化码率，实现最稳定信道估计。

进一步的，步骤 1 中，考虑一对合法收发机和一个导频感知攻击者，两个上行通信链路，分别为上行发射机→接收机，导频感知攻击者→接收机；接收机拥有 N_T 根天线，上行发射机和导频感知攻击者均为单天线；频域上，每条上行链路的每根天线在每个 OFDM 符号内都同时占用 N 个子载波. 时域上, 每个通信链路均采样 L 条路径, 信道模型为: $\mathbf{h}_B^i$ 代表上行发射机与接收机的第 i 根接收天线之间的信道冲激响应，$\sigma_{B,l}^2$ 代表第 l 条路径的功率时延谱；$\mathbf{h}_A^i$ 代表导频感知攻击者与接收机的第 i 根接收天线之间的信道冲激响应，并独立于 $\mathbf{h}_B^i$，$\sigma_{A,l}^2$ 代表第 l 条路径的功率时延谱。若上行发射机采用确定性导频，当导频感知攻击发生时，攻击者会在与合法发射机相同的导频点位置，发射相同的导频信号，导频信号

配置为：在第k个 OFDM 符号期间，上行发射机在第i个子载波上的的导频信号为$x_B^i[k]=\sqrt{\rho_B}e^{j\phi_k}$，其中，$\rho_B$为其导频发射功率，$\phi_k$表示第$k$个时隙对应的导频相位；导频感知攻击者在第$i$个子载波上的的导频信号为$x_A^i[k]=\sqrt{\rho_A}e^{j\varphi_{k,i}}$，其中，$\rho_A$为其导频发射功率，$\varphi_{k,i}$表示第$k$个OFDM符号时间第$i$个子载波上的导频相位。

进一步的，步骤 2 中，编码准则：对于一个$N\times C$的二元码本$\mathbf{C}=\left[c_{i,j}\right]$，当且仅当，对于码本矩阵内任意两个列向量集合$\mathcal{Q}$，最少存在$s$个行向量集合$\mathcal{S}$使得，$\forall i,j,i\in\mathcal{S},j\in\mathcal{Q}$，$c_{i,j}=1$ 成立。

进一步的，步骤 2 中，解码准则：考虑到混合攻击环境，接收机可以在第 i 个子载波 i∈[1，NB]上识别出三种类型的结果：情况 1：上行发射机和攻击者没有传输信号； 情况 2：上行发射机和攻击者都传输信号； 情况 3：一个未知节点传输信号；情况 3 进一步识别的方法为：对相邻子载波上收集到的信号进行差分编码，得到两种码字，对两种码字进行判定，当且仅当解码出来的码字权重与编码准则一致，判决该码字为正确的码字。

进一步的，步骤 3 中，导频表示阶段： 上行发射机和攻击者选择随机导频相位，根据码本，建立导频相位到码字的一对一映射，在该映射原理下，码字进一步映射为子载波激活模式，具体原理是，如果码字的元素数值等于 1，则导频信号该子载波上发送，否则该子载波被置于空闲状态；上行发射机和攻击者都产生各自的子载波激活模式，并且保持同步传输，经由无线环境，各个子载波上信号的叠加产生干扰，最终被接收机获取；导频分离阶段： 根据观察到的子载波激活模式，接收机对各个子载波进行能量检测，判断每一个子载波上是否存在信号，根据结果，得到一个二元码字向量,借助于解码准则，接收机能够识别具体的攻击类型；得到每个攻击类型下上行发射机和攻击者使用的码字；导频识别阶段:通过搜索码本中的码字，接收机识别分离出的码字，在混合攻击环境下，识别错误概率可定义为：

$$P_r=\frac{N!-\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}{2^{N+1}\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}。$$

进一步的，步骤 4 中，衡量信道估计的不稳定性，定义稳定性条件为：重合的子载波

等间隔分布并且重合的子载波个数满足$s \geq L$；衡量稳定性，定义指标P_s：

$$P_s\left(N,w,s^*\right)=\frac{\kappa\left(N,w,s^*\right)}{C^2\left(N,w,s^*\right)},0 \leq P_s\left(N,w,s^*\right) \leq 1$$

其中$C^2\left(N,w,s^*\right)$表示上行发射机和攻击者所有可能的两两码字组合可能，w为码字权重，$s^*=\frac{L-1}{L}N+1$；$\kappa\left(N,w,s^*\right)$表示满足CS条件的所有可能码字组合；建立一个优化问题，目标是最大化$\log_2\left[\frac{N!}{\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}\right]^{1/N}$，约束条件为：$P_s\left(N,w,s^*\right)=1,s^*=\frac{L-1}{L}N+1$；通过解决这个优化条件，得到最稳定信道估计下的码率表达式为：

$$R\left(N,w,s^*\right)=\log_2\left[\frac{N!}{\left(\frac{s^*\left(N+1\right)}{s^*+1}\right)!\left(\frac{N-s^*}{s^*+1}\right)!}\right]^{1/N}$$

其中，$w=\frac{s^*}{s^*+1}\left(N+1\right),s=\frac{\left(s^*-1\right)N+2s^*}{s^*+1}$。导频识别错误概率为：

$$P_r=\frac{N!-\left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}{2^{N+1}\left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}。$$

与现有技术相比，本发明有以下技术效果：

本发明利用随机导频的特性来弱化导频感知攻击为混合攻击模式，同时根据信道的独立特性建立独立性校验编码准则，来实现导频干扰环境下合法用户导频信号的，通过优化码率及其对应的天线、时隙和子载波资源配置，进一步实现稳定而又高精度的信道估计。

附图说明

图1是系统模型图。

图2是所提协议框架图。

图 3 是安全性与稳定性的折衷曲线图。

图 4 是导频识别错误概率图。

图 5 是信道均方误差与合法导频信噪比曲线图。

具体实施方式

以下结合附图对本发明进一步说明：

图 1 给出的系统模型图，考虑一对合法收发机和一个导频感知攻击者，两个上行通信链路，分别为上行发射机→接收机，导频感知攻击者→接收机。接收机拥有 N_T 根天线，上行发射机和导频感知攻击者均为单天线。频域上，每条上行链路的每根天线在每个 OFDM 符号内都同时占用 N 个子载波. 时域上, 每个通信链路均采样 L 条路径, 信道模型为: $\mathbf{h}_B^i$ 代表上行发射机与接收机的第 i 根接收天线之间的信道冲激响应，$\sigma_{B,l}^2$ 代表第 l 条路径的功率时延谱； $\mathbf{h}_A^i$ 代表导频感知攻击者与接收机的第 i 根接收天线之间的信道冲激响应，并独立于 $\mathbf{h}_B^i$， $\sigma_{A,l}^2$ 代表第 l 条路径的功率时延谱。若上行发射机采用确定性导频，当导频感知攻击发生时，攻击者会在与合法发射机相同的导频点位置，发射相同的导频信号，导频信号配置为：在第 k 个 OFDM 符号期间，上行发射机在第 i 个子载波上的的导频信号为 $x_B^i[k]=\sqrt{\rho_B}e^{j\phi_k}$，其中， ρ_B 为其导频发射功率，ϕ_k 表示第 k 个时隙对应的导频相位；导频感知攻击者在第 i 个子载波上的的导频信号为 $x_A^i[k]=\sqrt{\rho_A}e^{j\varphi_{k,i}}$，其中，$\rho_A$ 为其导频发射功率，$\varphi_{k,i}$ 表示第 k 个 OFDM 符号时间第 i 个子载波上的导频相位。为了防止导频污染，上行发射机采用随机导频进行信道估计，此时，主动攻击者可采取混合攻击模式：1. 采用随机导频，部分频带干扰合法信道的信道训练；2 采用随机导频，全频带干扰合法信道训练；3. 保持静默。

图 2 给出了所提协议的框架图，包括如下步骤：

Step 1：考虑 3 个 OFDM 符号时间，对任意单个子载波上收到的信号进行能量检测，通过配置阈值，实现每个子载波上精准的信号个数检测，若存在信号，则该子载波被编码为 1，反之则为 0。根据得到的二进制编码，得到二元码字向量集合为：$S=\left\{\mathbf{s}=\left[s_{1\le m\le L_s}\right]\middle| s_m\in\{0,1\},1\le m\le L_s\right\}$，其中，$L_s$ 表示码字的长度，s_m 表示第 m 个码字单元,；建立码频域为：$(\mathbf{s},b),\mathbf{s}\subset S,1\le b\le N$，其中 b 表示码字 $\mathbf{s}$ 对应频域的位置，N 表

示占用的子载波个数；最后得到一个$N\times C$的二元码本$\mathbf{C}=\left[c_{i,j}\right]$，码本中第$i$个码字定义为$\mathbf{c}_i=\left[c_{1,i}\quad\cdots\quad c_{N,i}\right]^{\mathrm{T}}$；

Step 2：构建独立性检验编码准则，具体可包括编码准则和解码准则。

编码准则：对于一个$N\times C$的二元码本$\mathbf{C}=\left[c_{i,j}\right]$，当且仅当，对于码本矩阵内任意两个列向量集合$\mathcal{Q}$，最少存在$s$个行向量集合$\mathcal{S}$使得，$\forall i,j,i\in\mathcal{S},j\in\mathcal{Q}$，$c_{i,j}=1$ 成立。

解码准则：

考虑到混合攻击环境，接收机可以在第 i 个子载波 i∈[1，NB]上识别出三种类型的结果：情况 1：上行发射机和攻击者没有传输信号。 情况 2：上行发射机和攻击者都传输信号。 情况 3：一个未知节点（上行发射机或者攻击者）传输信号。 显然，接收机可以识别前两种情况下的行为，但由于子载波上信号叠加的模糊性，情况 3 需要进一步识别，具体方法为，对相邻子载波上收集到的信号进行差分编码，得到两种码字，对两种码字进行判定，当且仅当解码出来的码字权重与编码准则一致，判决该码字为正确的码字。

Step 3:如图 2 所示，导频表示阶段： 上行发射机和攻击者选择随机导频相位，根据 Step 2 的码本，建立导频相位到码字的一对一映射，在该映射原理下，码字进一步映射为子载波激活模式，具体原理是，如果码字的元素数值等于 1，则导频信号该子载波上发送，否则该子载波被置于空闲状态。上行发射机和攻击者都产生各自的子载波激活模式，并且保持同步传输，经由无线环境，各个子载波上信号的叠加产生干扰，最终被接收机获取。导频分离阶段： 根据观察到的子载波激活模式，接收机对各个子载波进行 Step1 采用的能量检测，判断每一个子载波上是否存在信号，根据结果，得到一个二元码字向量，借助于 Step2 的解码准则，接收机可：1 识别具体的攻击类型；2 得到每个攻击类型下上行发射机和攻击者使用的码字。导频识别阶段:通过搜索码本中的码字，接收机识别分离出的码字，在混合攻击环境下，识别错误概率P_r可定义为：

$$P_r=\frac{N!-\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}{2^{N+1}\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}$$

Step 4：考虑 2 个 OFDM 符号时间，标记为k_0和k_1，并且考虑s个子载波重叠,则，接收机的信号模型可表示为：

$$\mathbf{Y}_{\mathrm{L}}=\mathbf{X}_{\mathrm{L}}\mathbf{H}_{\mathrm{L}}+\mathbf{N}_{\mathrm{L}}$$

其中，$\mathbf{X}_{\mathrm{L}}$是一个2×2导频信号矩阵，等于$\mathbf{X}_{\mathrm{L}}=\left[\mathbf{x}_{\mathrm{L},1}\quad\mathbf{x}_{\mathrm{L},2}\right]$，其中

$\mathbf{x}_{\mathrm{L},1}=\left[x_{\mathrm{B}}\left[k_0\right]\ \ x_{\mathrm{B}}\left[k_1\right]\right]^{\mathrm{T}},\mathbf{x}_{\mathrm{L},2}=\left[x_{\mathrm{A}}\left[k_0\right]\ \ x_{\mathrm{A}}\left[k_1\right]\right]^{\mathrm{T}}$，$\mathbf{H}_{\mathrm{L}}$ 是一个 $2\times N_{\mathrm{T}}s$ 矩阵，等于 $\mathbf{H}_{\mathrm{L}}=\left[\mathbf{h}_{\mathrm{B,L}}^{\mathrm{T}}\ \ \mathbf{h}_{\mathrm{A,L}}^{\mathrm{T}}\right]^{\mathrm{T}}$，其中，$N_{\mathrm{T}}$ 表示发射天线个数，$\mathbf{h}_{\mathrm{B,L}}=\left[\left(\mathbf{F}_{\mathrm{L},s}\mathbf{h}_{\mathrm{B}}^{1}\right)^{\mathrm{T}}\ \ ,\ldots,\ \ \left(\mathbf{F}_{\mathrm{L},s}\mathbf{h}_{\mathrm{B}}^{N_{\mathrm{T}}}\right)^{\mathrm{T}}\right]$，$\mathbf{h}_{\mathrm{A,L}}=\left[\left(\mathbf{F}_{\mathrm{L},s}\mathbf{h}_{\mathrm{A}}^{1}\right)^{\mathrm{T}}\ \ ,\ldots,\ \ \left(\mathbf{F}_{\mathrm{L},s}\mathbf{h}_{\mathrm{A}}^{N_{\mathrm{T}}}\right)^{\mathrm{T}}\right]$。$\mathbf{F}_{\mathrm{L},s}$ 是 $s\times L$ 维 DFT 矩阵。$\mathbf{N}_{\mathrm{L}}$ 是 $2\times N_{\mathrm{T}}s$ 维矩阵，满足 $\mathbf{N}_{\mathrm{L}}=\left[\mathbf{w}_{\mathrm{L}}^{\mathrm{T}}\left[k_0\right]\ \ \mathbf{w}_{\mathrm{L}}^{\mathrm{T}}\left[k_1\right]\right]^{\mathrm{T}},\mathbf{w}_{\mathrm{L}}\left[k\right]=\left[\mathbf{w}_{s}^{1^{\mathrm{T}}}\left[k\right]\ \ ,\ldots,\ \ \mathbf{w}_{s}^{N_{\mathrm{T}}{}^{\mathrm{T}}}\left[k\right]\right],k=k_0,k_1$，$1\times s$ 维向量 $\mathbf{w}_{s}^{i^{\mathrm{T}}}\left[k\right]$表示第 i 根天线第 k 个 OFDM 符号时间内的噪声矢量。根据此模型，得到子载波信道估计为：

$$\bar{\mathbf{h}}_{\mathrm{B,L}}=\mathbf{W}_{\mathrm{B,L}}\mathbf{Y}_{\mathrm{L}},\bar{\mathbf{h}}_{\mathrm{A,L}}=\mathbf{W}_{\mathrm{A,L}}\mathbf{Y}_{\mathrm{L}}$$

信道归一化均方误差为：$\varepsilon_{\mathrm{B}}^{2}=\dfrac{\mathbb{E}\left\{\left\|\bar{\mathbf{h}}_{\mathrm{B,L}}-\mathbf{h}_{\mathrm{B,L}}\right\|^{2}\right\}}{N_{\mathrm{T}}s},\varepsilon_{\mathrm{A}}^{2}=\dfrac{\mathbb{E}\left\{\left\|\bar{\mathbf{h}}_{\mathrm{A,L}}-\mathbf{h}_{\mathrm{A,L}}\right\|^{2}\right\}}{N_{\mathrm{T}}s}$

Step 5：为了衡量信道估计的不稳定性，定义稳定性条件为：重合的子载波等间隔分布并且重合的子载波个数满足 $s\geq L$。为了衡量稳定性，定义指标 P_{s}：

$$P_{\mathrm{s}}\left(N,w,s^{*}\right)=\frac{\kappa\left(N,w,s^{*}\right)}{C^{2}\left(N,w,s^{*}\right)},0\leq P_{\mathrm{s}}\left(N,w,s^{*}\right)\leq 1$$

其中 $C^{2}\left(N,w,s^{*}\right)$ 表示上行发射机和攻击者所有可能的两两码字组合可能，w 为码字权重，$s^{*}=\dfrac{L-1}{L}N+1$；$\kappa\left(N,w,s^{*}\right)$ 表示满足 CS 条件的所有可能码字组合。建立一个优化问题，目标是最大化 $\log_{2}\left[\dfrac{N!}{\left(\dfrac{N+s}{2}\right)!\left(\dfrac{N-s}{2}\right)!}\right]^{1/N}$，约束条件为：$P_{\mathrm{s}}\left(N,w,s^{*}\right)=1,s^{*}=\dfrac{L-1}{L}N+1$。通过解决这个优化条件，得到最稳定信道估计下的码率表达式为：

$$R\left(N,w,s^{*}\right)=\log_{2}\left[\frac{N!}{\left(\dfrac{s^{*}\left(N+1\right)}{s^{*}+1}\right)!\left(\dfrac{N-s^{*}}{s^{*}+1}\right)!}\right]^{1/N}$$

其中， $w=\frac{s^*}{s^*+1}(N+1), s=\frac{(s^*-1)N+2s^*}{s^*+1}$。导频识别错误概率为：

$$P_r=\frac{N!-\left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}{2^{N+1}\left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}$$ 。

本发明的仿真验证分别表示为图 3，图 4 和图 5。图 3 表示了此发明在导频感知攻击环境下对信道估计精度的提高。图 4 表明了本发明在最稳定信道估计下导频识别错误概率随子载波个数 N 的变化情况。 图 5 表示了本发明在最稳定信道估计下所提独立性校验编码的码率随着子载波个数 N 的变化情况。

权 利 要 求 书

1、一种基于独立性校验编码的OFDM信道训练鉴权方法，其特征在于，包括以下步骤：

步骤1，建立系统模型；采用随机导频机制，上行发射机采用随机导频进行信道估计，主动攻击者采取混合攻击模式；混合攻击模式包括部分频带干扰合法信道的信道训练、全频带干扰合法信道训练和保持静默；

步骤2，通过对各个子载波激活模式的编码，创建了码频域，构建了独立性校验编码准则；考虑3个OFDM符号时间，对任意单个子载波上收到的信号进行能量检测，通过配置阈值，实现每个子载波上精准的信号个数检测，若存在信号，则该子载波被编码为1，反之则为0；根据得到的二进制编码，得到二元码字向量集合为：$S=\left\{\mathbf{s}=\left[s_{1\le m\le L_s}\right]\middle| s_m\in\{0,1\},1\le m\le L_s\right\}$，其中，$L_s$ 表示码字的长度，s_m 表示第 m 个码字单元，；建立码频域为：$(\mathbf{s},b),\mathbf{s}\subset S,1\le b\le N$，其中 b 表示码字 $\mathbf{s}$ 对应频域的位置，N 表示占用的子载波个数；最后得到一个 $N\times C$ 的二元码本 $\mathbf{C}=\left[c_{i,j}\right]$，码本中第 i 个码字定义为 $\mathbf{c}_i=\left[c_{1,i}\quad\cdots\quad c_{N,i}\right]^{\mathrm{T}}$；

构建独立性校验编码准则，包括编码准则和解码准则，用以抵抗混合攻击；

步骤3，构建基于独立性校验编码ICC的反攻击信道训练鉴权CTA协议，包括导频的表示，分离和识别；

步骤4，优化码率，实现最稳定信道估计。

2、根据权利要求1所述的一种基于独立性校验编码的OFDM信道训练鉴权方法，其特征在于，步骤1中，考虑一对合法收发机和一个导频感知攻击者，两个上行通信链路，分别为上行发射机→接收机，导频感知攻击者→接收机；接收机拥有 N_T 根天线，上行发射机和导频感知攻击者均为单天线；频域上，每条上行链路的每根天线在每个OFDM符号内都同时占用 N 个子载波.时域上,每个通信链路均采样 L 条路径，信道模型为：$\mathbf{h}_B^i$ 代表上行发射机与接收机的第 i 根接收天线之间的信道冲激响应，$\sigma_{B,l}^2$ 代表第 l 条路径的功率时延谱；$\mathbf{h}_A^i$ 代表导频感知攻击者与接收机的第 i 根接收天线之间的信道冲激响应，并独立于 $\mathbf{h}_B^i$，$\sigma_{A,l}^2$ 代表第 l 条路径的功率时延谱；若上行发射机采用确定性导频，当导频感知攻击

发生时，攻击者会在与合法发射机相同的导频点位置，发射相同的导频信号，导频信号配置为：在第 k 个 OFDM 符号期间，上行发射机在第 i 个子载波上的导频信号为 $x_B^i[k]=\sqrt{\rho_B}e^{j\phi_k}$，其中，$\rho_B$ 为其导频发射功率，ϕ_k 表示第 k 个时隙对应的导频相位；导频感知攻击者在第 i 个子载波上的的导频信号为 $x_A^i[k]=\sqrt{\rho_A}e^{j\varphi_{k,i}}$，其中，$\rho_A$ 为其导频发射功率，$\varphi_{k,i}$ 表示第 k 个 OFDM 符号时间第 i 个子载波上的导频相位。

3、根据权利要求 1 所述的一种基于独立性校验编码的 OFDM 信道训练鉴权方法，其特征在于，步骤 2 中，编码准则：对于一个 $N\times C$ 的二元码本 $\mathbf{C}=\left[c_{i,j}\right]$，当且仅当，对于码本矩阵内任意两个列向量集合 $\mathcal{Q}$，最少存在 s 个行向量集合 $\mathcal{S}$ 使得，$\forall i,j,i\in\mathcal{S},j\in\mathcal{Q}$，$c_{i,j}=1$ 成立。

4、根据权利要求 1 所述的一种基于独立性校验编码的 OFDM 信道训练鉴权方法，其特征在于，步骤 2 中，解码准则：考虑到混合攻击环境，接收机在第 i 个子载波 $i\in[1,N]$ 上识别出三种类型的结果：情况 1：上行发射机和攻击者没有传输信号； 情况 2：上行发射机和攻击者都传输信号； 情况 3：一个未知节点传输信号；情况 3 进一步识别的方法为：对相邻子载波上收集到的信号进行差分编码，得到两种码字，对两种码字进行判定，当且仅当解码出来的码字权重与编码准则一致，判决该码字为正确的码字。

5、根据权利要求 1 所述的一种基于独立性校验编码的 OFDM 信道训练鉴权方法，其特征在于，步骤 3 中，导频表示阶段： 上行发射机和攻击者选择随机导频相位，根据码本，建立导频相位到码字的一对一映射，在该映射原理下，码字进一步映射为子载波激活模式，具体原理是，如果码字的元素数值等于 1，则导频信号该子载波上发送，否则该子载波被置于空闲状态；上行发射机和攻击者都产生各自的子载波激活模式，并且保持同步传输，经由无线环境，各个子载波上信号的叠加产生干扰，最终被接收机获取；导频分离阶段： 根据观察到的子载波激活模式，接收机对各个子载波进行能量检测，判断每一个子载波上是否存在信号，根据结果，得到一个二元码字向量,借助于解码准则，接收机能够识别具体的攻击类型；得到每个攻击类型下上行发射机和攻击者使用的码字；导频识别阶段:通过搜索码本中的码字，接收机识别分离出的码字，在混合攻击环境下，识别错误

概率 P_r 定义为：

$$P_r = \frac{N! - \left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}{2^{N+1}\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}。$$

6、根据权利要求 1 所述的一种基于独立性校验编码的 OFDM 信道训练鉴权方法，其特征在于，步骤 4 中，衡量信道估计的不稳定性，定义稳定性条件为：重合的子载波等间隔分布并且重合的子载波个数满足 $s \geq L$；衡量稳定性，定义指标 P_s：

$$P_s\left(N,w,s^*\right) = \frac{\kappa\left(N,w,s^*\right)}{C^2\left(N,w,s^*\right)}, 0 \leq P_s\left(N,w,s^*\right) \leq 1$$

其中 $C^2\left(N,w,s^*\right)$ 表示上行发射机和攻击者所有可能的两两码字组合可能，w 为码字权重，$s^* = \frac{L-1}{L}N+1$；$\kappa\left(N,w,s^*\right)$ 表示满足 CS 条件的所有可能码字组合；建立一个优化问题，目标是最大化 $\log_2\left[\frac{N!}{\left(\frac{N+s}{2}\right)!\left(\frac{N-s}{2}\right)!}\right]^{1/N}$，约束条件为：$P_s\left(N,w,s^*\right)=1, s^* = \frac{L-1}{L}N+1$；通过解决这个优化条件，得到最稳定信道估计下的码率表达式为：

$$R\left(N,w,s^*\right) = \log_2\left[\frac{N!}{\left(\frac{s^*\left(N+1\right)}{s^*+1}\right)!\left(\frac{N-s^*}{s^*+1}\right)!}\right]^{1/N}$$

其中，$w = \frac{s^*}{s^*+1}\left(N+1\right), s = \frac{\left(s^*-1\right)N+2s^*}{s^*+1}$；导频识别错误概率 P_r 为：

$$P_r = \frac{N! - \left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}{2^{N+1}\left(\frac{N+s^*}{2}\right)!\left(\frac{N-s^*}{2}\right)!}。$$

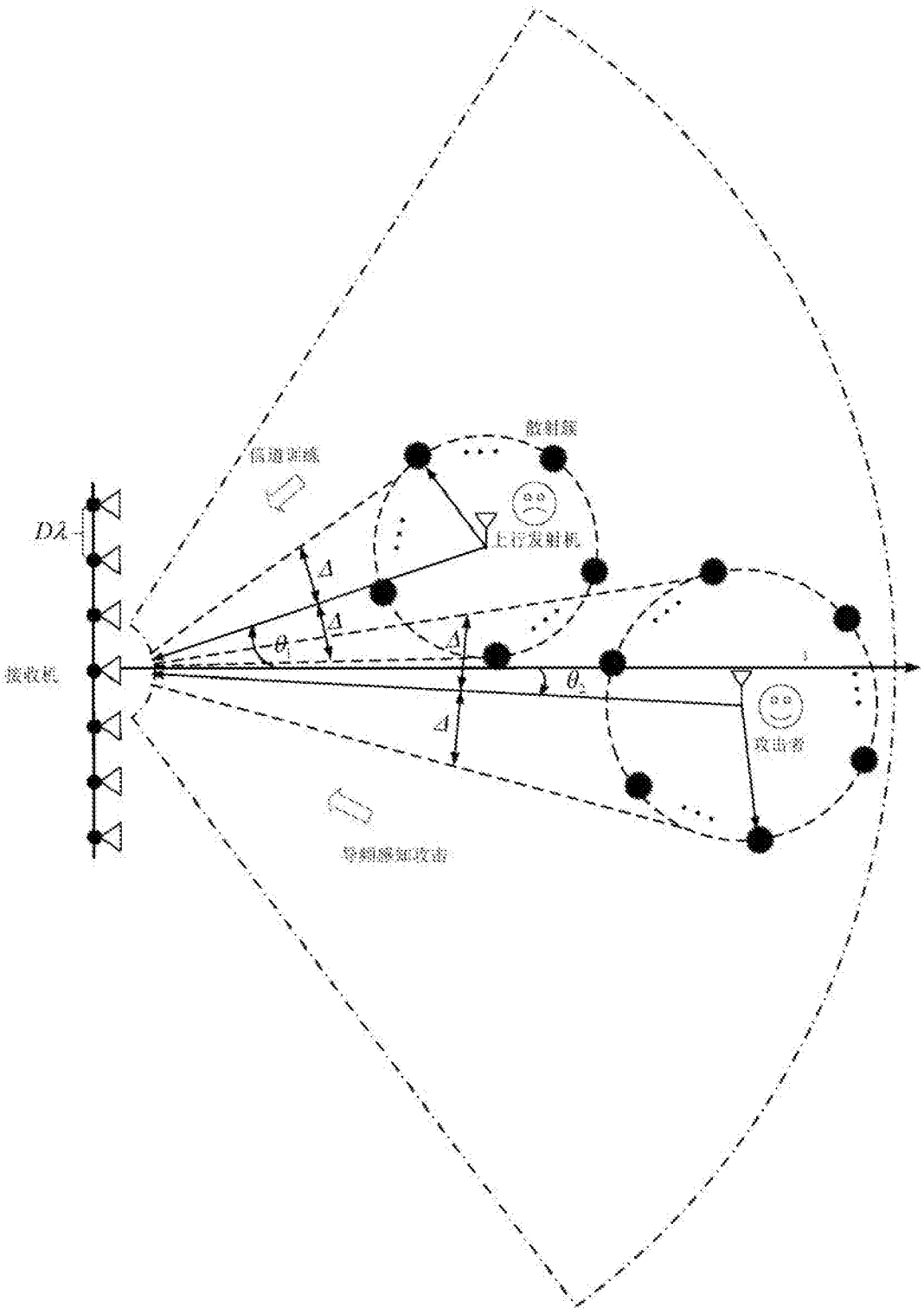

图 1

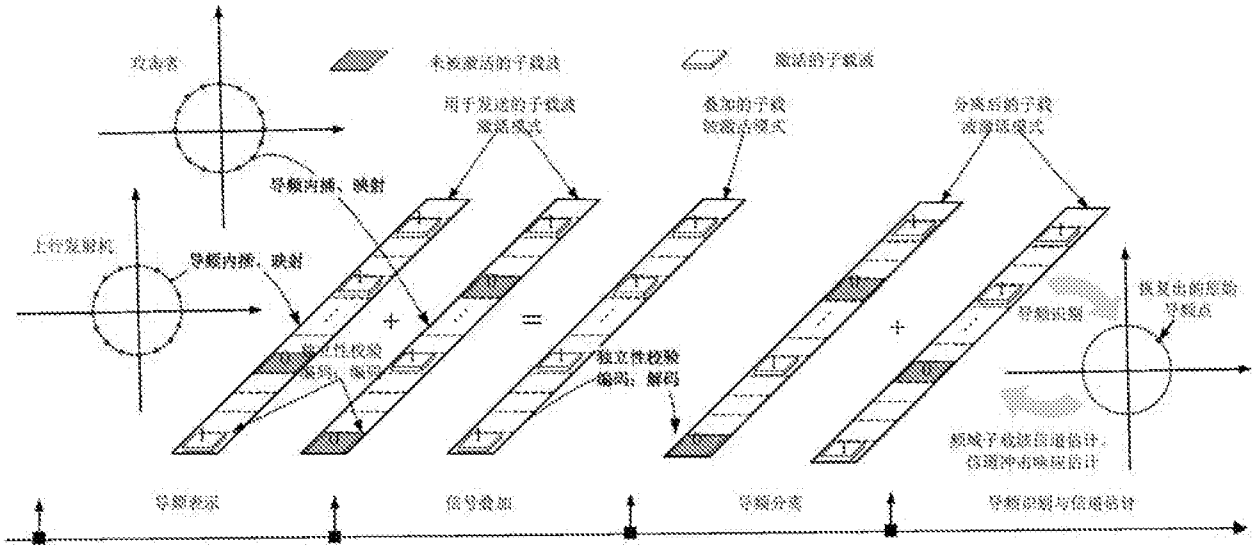

图 2

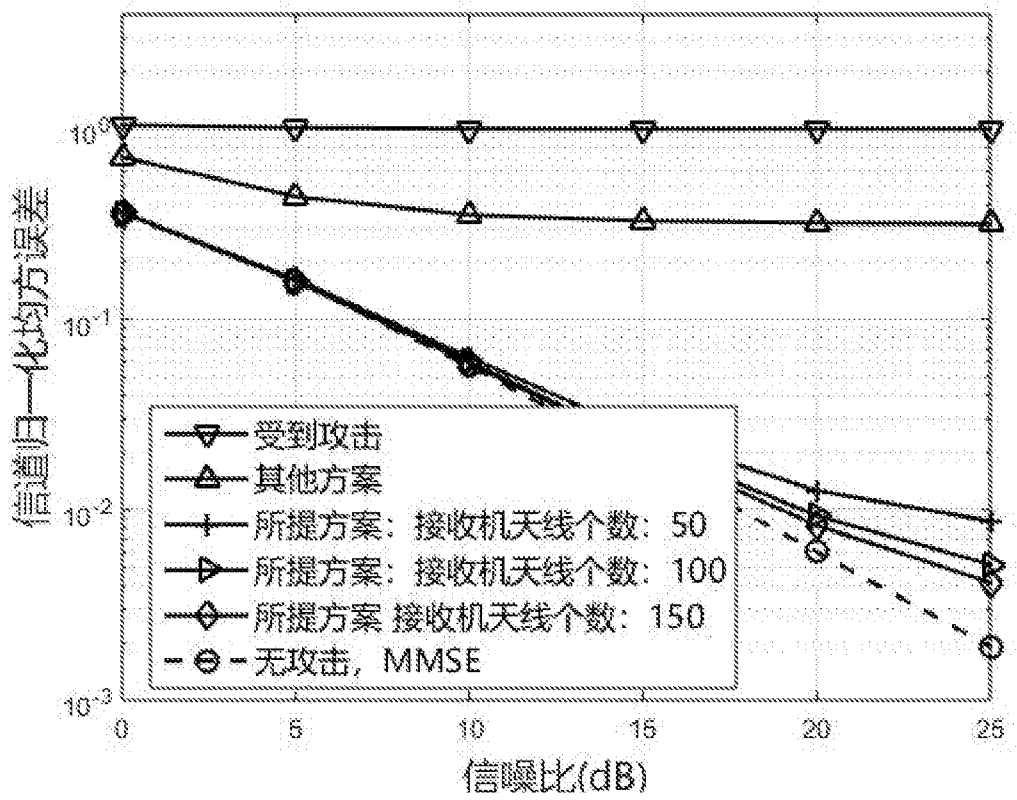
信道归一化均方误差
信噪比(dB)
受到攻击
其他方案
所提方案：接收机天线个数：50
所提方案：接收机天线个数：100
所提方案 接收机天线个数：150
无攻击，MMSE

图 3

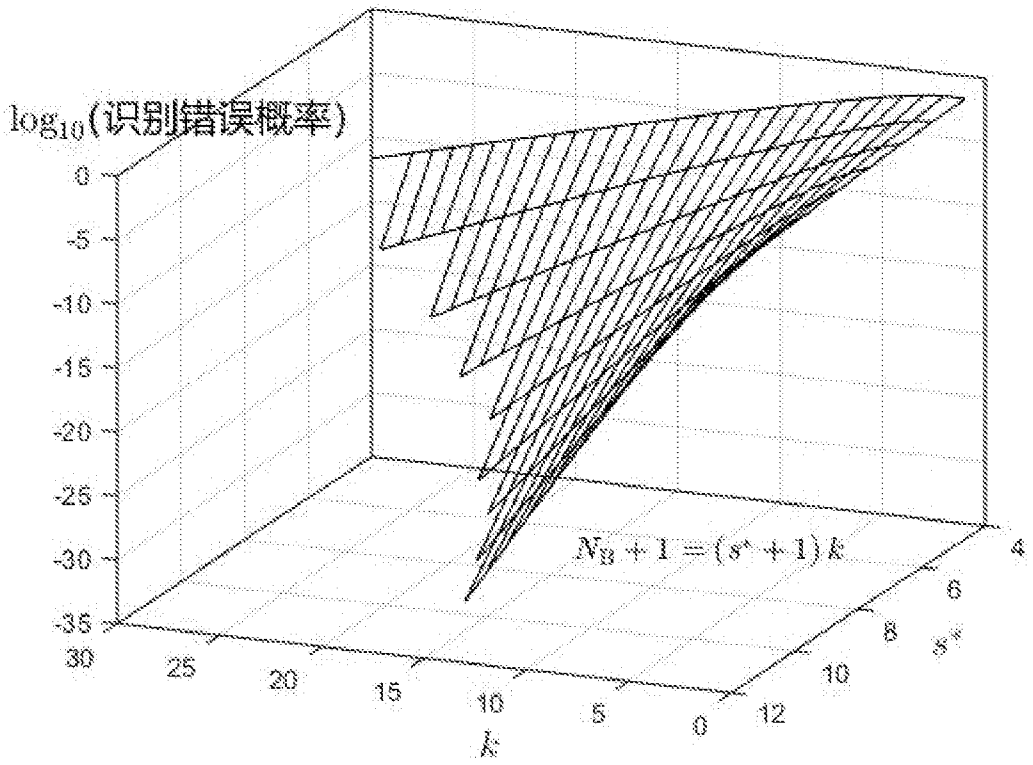
$\log_{10}$(识别错误概率)
0
-5
-10
-15
-20
-25
-30
-35
30
25
20
15
10
5
0
k
12
10
8
6
4
s^*
$N_B + 1 = (s^* + 1)k$

图 4

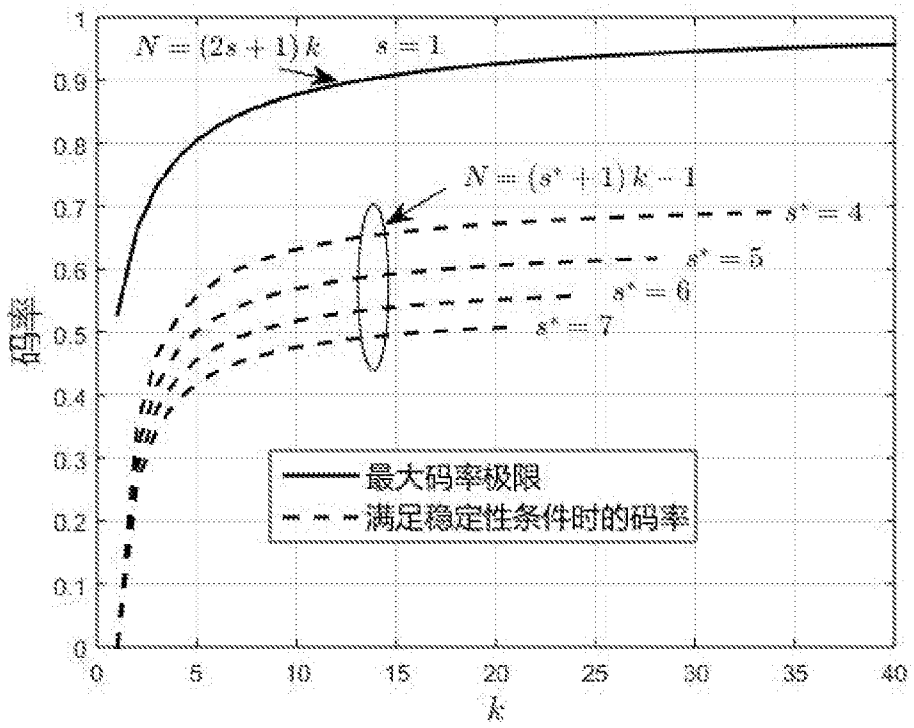
$N = (2s + 1)k$ $s = 1$
$N = (s^* + 1)k - 1$
$s^* = 4$
$s^* = 5$
$s^* = 6$
$s^* = 7$
码率
最大码率极限
满足稳定性条件时的码率
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
5
10
15
20
25
30
35
40
k

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/099051

A. CLASSIFICATION OF SUBJECT MATTER

H04B 17/391(2015.01)i; H04L 25/02(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04B;H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT, IEEE: 编码, OFDM, 鉴权, 攻击, cod???, identification, spoof??? attack, pilot

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	XU, Dongyang et al. "Code-Frequency Block Group Coding for Anti-Spoofing Pilot Authentication in Multi-Antenna OFDM Systems" *IEEE*, 01 February 2018 (2018-02-01), pp. 1778-1789	1-6
A	XU Dongyang et al. "ICA-SBDC:A Channel Estimation and Identification Mechanism for MISO-OFDM Systems under Pilot Spoofing Attack" *IEEE*, 31 December 2017 (2017-12-31), entire document	1-6
A	CN 106161297 A (XI'AN JIAOTONG UNIVERSITY) 23 November 2016 (2016-11-23) entire document	1-6
A	CN 102238116 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 09 November 2011 (2011-11-09) entire document	1-6

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2019	**07 March 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/099051

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106161297 A	23 November 2016	None	
CN 102238116 A	09 November 2011	CN 102238116 B	09 July 2014

国际检索报告

国际申请号
PCT/CN2018/099051

A. 主题的分类

H04B 17/391(2015.01)i; H04L 25/02(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04B;H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI, EPODOC, CNKI, CNPAT, IEEE: 编码，OFDM，鉴权，攻击，cod???,identification,spoof??? attack,pilot

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	XU Dongyang等. "Code-Frequency Block Group Coding for Anti-Spoofing Pilot Authentication in Multi-Antenna OFDM Systems" IEEE, 2018年 2月 1日 (2018-02-01), 第1778-1789页	1-6
A	XU Dongyang等. "ICA-SBDC:A Channel Estimation and Identification Mechanism for MISO-OFDM Systems under Pilot Spoofing Attack" IEEE, 2017年 12月 31日 (2017-12-31), 全文	1-6
A	CN 106161297 A (西安交通大学) 2016年 11月 23日 (2016-11-23) 全文	1-6
A	CN 102238116 A (北京邮电大学) 2011年 11月 9日 (2011-11-09) 全文	1-6

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 2月 13日	2019年 3月 7日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	林竑 电话号码 86-10-53961632

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/099051

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 106161297 A	2016年 11月 23日	无	
CN 102238116 A	2011年 11月 9日	CN 102238116 B	2014年 7月 9日