(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 109714090 B
(45)授权公告日 2021.06.25

(21)申请号 201910072420.3
(22)申请日 2019.01.25
(65)同一申请的已公布的文献号
申请公布号 CN 109714090 A
(43)申请公布日 2019.05.03
(73)专利权人 伍仁勇
地址 410006 湖南省长沙市岳麓区石佳冲109号12栋208房
(72)发明人 伍仁勇 伍清源 段伟
(74)专利代理机构 长沙正奇专利事务所有限责任公司 43113
代理人 卢宏 王娟
(51)Int.Cl.
H04B 7/0456(2017.01)
H04B 7/06(2006.01)
H04B 7/08(2006.01)

(56)对比文件
WO 2014142122 A1,2014.09.18
CN 105027459 A,2015.11.04
CN 106685496 A,2017.05.17
US 2017070277 A1,2017.03.09
Rengyong Wu,.Secure Transmission Against Pilot Contamination:.《IEEE》.2018,

审查员 陈诗华

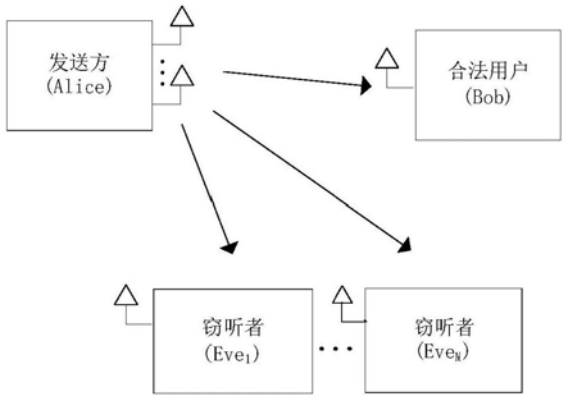
权利要求书4页 说明书11页 附图3页

(54)发明名称

一种多天线二维矢量传输方法及系统

(57)摘要

本发明公开了一种多天线二维矢量传输方法，将现有的一维传输体制扩展到二维传输体制，实现物理层的安全传输。本发明的传输安全性不再依赖于合法用户的信道优势，只需要合法信道和窃听信道之间存在足够的差异性。用于预编码的随机权值系数矩阵不需要传送给接收者。这些都使本发明很容易物理实现。在合法信道和窃听信道之间存在足够的差异性的前提下，本发明能抵抗MUSIC-like一类安全攻击，实现无条件安全，即保持窃听者的误码率在0.5左右，即无法有效解码。



CN 109714090 B

1.一种多天线二维矢量传输方法，其特征在于，包括以下步骤：

1)在第一个时间块，发送方生成随机权值系数矩阵W_1；W_1与每个待发送符号矢量$\bar{\mathbf{x}}(n)$相乘得到$\mathbf{W}_1\bar{\mathbf{x}}(n)$，其中$\mathbf{W}_1\bar{\mathbf{x}}(n)$为J×1的叠加信号矢量；然后将该叠加信号矢量中每个分量分别加载到对应天线上发送；在该时间块的连续N个符号周期内，依次将$\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$发送一次；在下个时间块再生成新的随机权值系数矩阵，重复上述发送过程；

$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T, n=1,2,\cdots,N$表示第n个符号周期待发送的符号矢量；J为发送天线的数量；

x(n)表示待发符号序列的第n个符号，x(n+N)表示待发符号序列的第n+N个符号，x[n+(L-1)N]表示待发符号序列的第n+(L-1)N个符号；

$$\left[\bar{\mathbf{x}}(1)\quad\bar{\mathbf{x}}(2)\quad\cdots\quad\bar{\mathbf{x}}(N)\right]=\begin{bmatrix}x(1) & x(2) & \cdots & x(N)\\ x(1+N) & x(2+N) & \cdots & x(2N)\\ \vdots & \vdots & \ddots & \vdots\\ x[1+(L-1)N] & x[2+(L-1)N] & \cdots & x(LN)\end{bmatrix};$$

2)接收方接收到发送方发送的信号后，利用下式解调，得到信号矢量$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]$：

$$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]$$
$$=\arg\min_{\substack{x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]}}\{|y_{Bob}(n)-\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]|^2\};$$

其中，

$$y_{Bob}(n)=[\lambda_1\|\mathbf{h}_{AB,1}\|\quad\lambda_2\|\mathbf{h}_{AB,2}\|\quad\cdots\quad\lambda_L\|\mathbf{h}_{AB,L}\|]\begin{bmatrix}x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]\end{bmatrix}+v_{Bob}(n)$$
$$=\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]+v_{Bob}(n);$$

$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T$；$||h_{AB,1}||$表示第1个时间块发送方到接收方的信道矢量$h_{AB,1}$的2-范式，$\|\mathbf{h}_{AB,l}\|=\sqrt{\sum_{j=1}^{J}|h_{A_jB,l}|^2}$；$h_{A_jB,l}$表示信道矢量$h_{AB,L}$的第j个分量，$|h_{A_jB,l}|$表示$h_{A_jB,l}$的模；$v_{Bob}(n)$表示接收端的噪声；L为信号矢量的维度，也即传输次数；λ_1，λ_2，…，λ_L为实系数，且λ_1，λ_2，…，λ_L为正数。

2.根据权利要求1所述的多天线二维矢量传输方法，其特征在于，$\lambda_1^2+\lambda_2^2+\cdots+\lambda_L^2=L$。

3.根据权利要求2所述的多天线二维矢量传输方法，其特征在于，λ_1，λ_2，…，λ_L的求解过程包括：

1)设r=0；步长为t；λ_1，λ_2，…，λ_L均初始化为0.1；

2)对于λ_s，递增t，然后计算Min($d_{m,n}$)，1≤s≤L，其中$d_{m,n}=(\lambda_m||h_{AB,m}||-\lambda_n||h_{AB,n}||)^2$，1

≤m≤L,1≤n≤L,m≠n;Min($d_{m,n}$)是指所有$d_{m,n}$值中的最小值;

3)如果Min($d_{m,n}$)>r,则令r=Min($d_{m,n}$),保存当前对应的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,返回步骤2),直至$\lambda_s=\sqrt{L}$;否则直接返回步骤2),直至$\lambda_s=\sqrt{L}$;重复步骤2)和步骤3),直至$\lambda_1,\lambda_2,\cdots,\lambda_L$的值都达到上限,输出最后保存的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,即为最优值。

4.根据权利要求1～3之一所述的多天线二维矢量传输方法,其特征在于,发送方生成的随机权值系数矩阵序列满足下述线性约束

$$\mathbf{h}_{AB,1}^{H}\mathbf{W}_1+\mathbf{h}_{AB,2}^{H}\mathbf{W}_2+\cdots+\mathbf{h}_{AB,L}^{H}\mathbf{W}_L=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|];$$

其中,$\mathbf{h}_{AB,l}^{H}$表示信道矢量$h_{AB,1}$进行艾尔米特变换后得到的矢量,1≤1≤L;W_2、W_L分别表示第2个和第L个权值系数矩阵。

5.根据权利要求4所述的多天线二维矢量传输方法,其特征在于,所述权值系数矩阵的生成过程包括:

1)随机生成前L-1个权值系数矩阵$W_1,W_2,\cdots,W_{L-1}$;

2)对于W_L,随机生成权值$w_{j,l}^{(L)},1\le j\le J-1,1\le l\le L$;

3)权值$w_{J,l}^{(L)}=(\phi_l-\sum_{j=1}^{J-1}h_{A_jB,L}^{*}w_{j,l}^{(L)})/h_{A_JB,L}^{*}$;$w_{j,l}^{(L)}$表示权值系数矩阵$W_L$中第j行、第1列的元素;其中

$[\phi_1,\phi_2,\cdots,\phi_L]=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]-\sum_{l=1}^{L-1}\mathbf{h}_{AB,l}^{H}\mathbf{W}_l$,则

$\mathbf{h}_{AB,L}^{H}\mathbf{W}_L=[\phi_1,\phi_2,\cdots,\phi_L]$;$h_{A_jB,L}^{*}$表示信道矢量$h_{AB,L}$的第j个分量的复共轭;$\mathbf{h}_{AB,l}^{H}$表示信道矢量$h_{AB,1}$进行艾尔米特变换后得到的矢量。

6.一种多天线二维矢量传输系统,其特征在于,包括:

发送方,在第一个时间块,发送方生成随机权值系数矩阵W_1;W_1与每个待发送符号矢量$\bar{\mathbf{x}}(n)$相乘得到$\mathbf{W}_1\bar{\mathbf{x}}(n)$,其中$\mathbf{W}_1\bar{\mathbf{x}}(n)$为J×1的叠加信号矢量;然后将该叠加信号矢量中每个分量分别加载到对应天线上发送;在该时间块的连续N个符号周期内,依次将$\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$发送一次;在下个时间块再生成新的随机权值系数矩阵,重复上述发送过程;

$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T,n=1,2,\cdots,N$表示第n个符号周期待发送的符号矢量;J为发送天线的数量;x(n)表示待发符号序列的第n个符号,x(n+N)表示待发符号序列的第n+N个符号,x[n+(L-1)N]表示待发符号序列的第n+(L-1)N个符号;

$$\left[\bar{\mathbf{x}}(1)\quad\bar{\mathbf{x}}(2)\quad\cdots\quad\bar{\mathbf{x}}(N)\right]=\begin{bmatrix}x(1)&x(2)&\cdots&x(N)\\x(1+N)&x(2+N)&\cdots&x(2N)\\\vdots&\vdots&\ddots&\vdots\\x[1+(L-1)N]&x[2+(L-1)N]&\cdots&x(LN)\end{bmatrix};$$

接收方,用于在接收到发送方发送的信号后,接收到发送方发送的信号后,利用下式解调,得到信号矢量

$[\tilde{x}(n), \tilde{x}(n+N), \cdots, \tilde{x}[n+(L-1)N]]$：

$$[\tilde{x}(n), \tilde{x}(n+N), \cdots, \tilde{x}[n+(L-1)N]] = \arg \min_{\substack{x(n) \\ x(n+N) \\ \vdots \\ x[n+(L-1)N]}} \{| y_{Bob}(n) - \sum_{l=1}^{L} \lambda_l \| \mathbf{h}_{AB,l} \| x[n+(l-1)N] |^2\}$$

；

其中，

$$y_{Bob}(n) = [\lambda_1 \| \mathbf{h}_{AB,1} \| \quad \lambda_2 \| \mathbf{h}_{AB,2} \| \quad \cdots \quad \lambda_L \| \mathbf{h}_{AB,L} \|] \begin{bmatrix} x(n) \\ x(n+N) \\ \vdots \\ x[n+(L-1)N] \end{bmatrix} + v_{Bob}(n)$$

$$= \sum_{l=1}^{L} \lambda_l \| \mathbf{h}_{AB,l} \| x[n+(l-1)N] + v_{Bob}(n)$$

；

$\bar{\mathbf{x}}(n) = [x(n), x(n+N), \cdots, x[n+(L-1)N]]^T$；$||h_{AB,1}||$表示第1个时间块发送方到接收方的信道矢量$h_{AB,1}$的2-范式，$\|\mathbf{h}_{AB,l}\| = \sqrt{\sum_{j=1}^{J} |h_{A_jB,l}|^2}$；$h_{A_jB,l}$表示信道矢量$h_{AB,L}$的第j个分量，$|h_{A_jB,l}|$表示$h_{A_jB,l}$的模；$v_{Bob}(n)$表示接收端的噪声；L为信号矢量的维度，也即传输次数；λ_1，λ_2，…，λ_L为实系数，且λ_1，λ_2，…，λ_L为正数。

7.根据权利要求6所述的系统，其特征在于，$\lambda_1^2+\lambda_2^2+\cdots+\lambda_L^2=L$。

8.根据权利要求7所述的系统，其特征在于，λ_1，λ_2，…，λ_L的求解过程包括：

1)设r＝0；步长为t；λ_1，λ_2，…，λ_L均初始化为0.1；

2)对于λ_s，递增t，然后计算$Min(d_{m,n})$ $1 \leqslant s \leqslant L$，其中

$d_{m,n}=(\lambda_m||h_{AB,m}||-\lambda_n||h_{AB,n}||)^2$，$1 \leqslant m \leqslant L$，$1 \leqslant n \leqslant L$，$m \neq n$；$Min(d_{m,n})$是指所有$d_{m,n}$值中的最小值；

3)如果$Min(d_{m,n})>r$，则令$r=Min(d_{m,n})$，保存当前对应的λ_1，λ_2，…，λ_L值，返回步骤2)，直至$\lambda_s=\sqrt{L}$；否则直接返回步骤2)，直至$\lambda_s=\sqrt{L}$；重复步骤2)和步骤3)，直至λ_1，λ_2，…，λ_L的值都达到上限，输出最后保存的λ_1，λ_2，…，λ_L值，即为最优值。

9.根据权利要求6～8之一所述的系统，其特征在于，发送方生成的随机权值系数矩阵序列满足下述线性约束

$\mathbf{h}_{AB,1}^H \mathbf{W}_1 + \mathbf{h}_{AB,2}^H \mathbf{W}_2 + \cdots + \mathbf{h}_{AB,L}^H \mathbf{W}_L = [\lambda_1 \| \mathbf{h}_{AB,1} \|, \lambda_2 \| \mathbf{h}_{AB,2} \|, \cdots, \lambda_L \| \mathbf{h}_{AB,L} \|]$；其中，$\mathbf{h}_{AB,l}^H$表示信道矢量$h_{AB,1}$进行艾尔米特变换后得到的矢量，$1 \leqslant 1 \leqslant L$；$W_2$、$W_L$分别表示第2个和第L个权值系数矩阵。

10.根据权利要求9所述的系统，其特征在于，所述权值系数矩阵的生成过程包括：

1)随机生成前L-1个权值系数矩阵W_1，W_2，…，W_{L-1}；

2)对于W_L，随机生成权值$w_{j,l}^{(L)}, 1 \leq j \leq J-1, 1 \leq l \leq L$；

3) 权值 $w_{J,l}^{(L)}=(\phi_l-\sum_{j=1}^{J-1}h_{A_jB,L}^{*}w_{j,l}^{(L)})/h_{A_JB,L}^{*}$；$w_{j,l}^{(L)}$表示权值系数矩阵$W_L$中第j行、第l列的元素；其中

$[\phi_1,\phi_2,\cdots,\phi_L]=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]-\sum_{l=1}^{L-1}\mathbf{h}_{AB,l}^{H}\mathbf{W}_l$，则

$\mathbf{h}_{AB,L}^{H}\mathbf{W}_L=[\phi_1,\phi_2,\cdots,\phi_L]$；$h_{A_jB,L}^{*}$表示信道矢量$h_{AB,L}$的第j个分量的复共轭；$\mathbf{h}_{AB,l}^{H}$表示信道矢量$h_{AB1}$进行艾尔米特变换后得到的矢量。

一种多天线二维矢量传输方法及系统

技术领域

[0001] 本发明涉及信息通信领域,特别是一种多天线二维矢量传输方法。

背景技术

[0002] 传统安全理论和方法的理论基础是密码学,其安全性一般建立在计算复杂性基础之上,缺乏严格的数学证明。随着终端计算能力的快速提高和各种新型计算理论(如量子计算)的提出,各种有效的攻击方法不断出现,传统安全理论日益面临挑战。与其不同,物理层安全传输的基本思想是充分利用噪声和无线信道本身具有的不可复制的物理随机特性,辅以合适的信号处理算法,在保证合法用户正常接收的前提下,限制非法用户解码的有效信息"位"数。所以,物理层安全可以作为传统安全理论和方法的一种有益补充。

[0003] 根据信息论安全理论,信道安全容量依赖于合法接收者相对于非法(窃听)用户的信道优势(必须是正值),而这在实际应用中往往难以满足。为改善合法用户的信道优势,现有研究多在发送端采用技术手段降低非法接收者的信道/信号质量。在某些场景下,安全波束赋形是一种有效的(甚至最优)物理层安全传输方案。然而,安全波束赋形技术依赖于窃听信道的精确状态信息用以设计发送方案。当窃听者只接收而不发送任何电磁信号时,意即实行完全的被动窃听,发送端可能完全无法获得窃听信道的任何有用信息,此时其发送方案的设计根本无从着手。这限制了安全波束赋形方案的实际应用。对此,有人提出了随机波束赋形方案:人工噪声方案与随机阵列加权方案,分别产生加性和乘性随机噪声,降低非法接收者的信道/信号质量。但是,无论何种随机波束赋形方案,只要仍旧采用一维传输体制,即每个符号周期每根传输天线只发送一个符号,则窃听者总可以利用更多接收天线得到的空间维度优势来破解(如MUSIC-like算法)。可事实是,现有几乎所有通信系统都是采用一维传输体制。

[0004] 可见,传统安全理论和方法面临挑战,现有物理层安全传输理论和方法也面临困境,无法确保无线传输安全。

发明内容

[0005] 本发明所要解决的技术问题是,针对现有技术不足,提供一种多天线二维矢量传输方法,确保传输安全。

[0006] 为解决上述技术问题,本发明所采用的技术方案是:一种多天线二维矢量传输方法,包括以下步骤:

[0007] 1)在第一个时间块,发送方生成随机权值系数矩阵W_1;W_1与每个待发送符号矢量$\bar{\mathbf{x}}(n)$相乘得到$\mathbf{W}_1\bar{\mathbf{x}}(n)$,其中$\mathbf{W}_1\bar{\mathbf{x}}(n)$为J×1的叠加信号矢量;然后将该叠加信号矢量中每个分量分别加载到对应天线上发送;在该时间块的连续N个符号周期内,依次将$\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$发送一次;在下个时间块再生成新的随机权值系数矩阵,重复上述发送过程;$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T, n=1,2,\cdots,N$表示第n个符号周期待发送的

符号矢量;J为发送天线的数量;x(n)表示待发符号序列的第n个符号;

[0008] 2)接收方接收到发送方发送的信号后,利用下式解调,得到信号矢量$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]$:

[0009] $$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]=\arg\min_{\substack{x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]}}\{|y_{Bob}(n)-\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]|^2\}$$;

[0010] 其中,$y_{Bob}(n)=[\lambda_1\|\mathbf{h}_{AB,1}\|\ \ \lambda_2\|\mathbf{h}_{AB,2}\|\ \cdots\ \lambda_L\|\mathbf{h}_{AB,L}\|]\begin{bmatrix}x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]\end{bmatrix}+v_{Bob}(n)$

$=\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]+v_{Bob}(n)$;$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T$;$||h_{AB,1}||$表示第1个时间块发送方到接收方的信道矢量$h_{AB,1}$的2-范式,$\|\mathbf{h}_{AB,l}\|=\sqrt{\sum_{j=1}^{J}|h_{A_jB,l}|^2}$;$h_{A_jB,l}$表示信道矢量$h_{AB}{}^{,L}$的第j个分量,$|h_{A_jB,l}|$表示$h_{A_jB,l}$的模;$v_{Bob}(n)$表示接收端的噪声;L为信号矢量的维度,也即传输次数;$\lambda_1,\lambda_2,\cdots,\lambda_L$为实系数,且$\lambda_1,\lambda_2,\cdots,\lambda_L$为正数。

[0011] 本发明中,在每个信道系数$||h_{AB,1}||$、$||h_{AB,2}||$…$||h_{AB,L}||$前增加一个权值项,保证信道系数$||h_{AB,1}||$、$||h_{AB,2}||$…$||h_{AB,L}||$足够不同,从而降低接收端的误码率,使接收端性能更好。为了保证信道系数足够不同,$\lambda_1^2+\lambda_2^2+\cdots+\lambda_L^2=L$,且优选利用下述过程求解$\lambda_1,\lambda_2,\cdots,\lambda_L$:

[0012] 1)设r=0;步长为t;$\lambda_1,\lambda_2,\cdots,\lambda_L$均初始化为0.1;

[0013] 2)对于λ_s,递增t,然后计算$Min(d_{m,n})$,1≤s≤L,其中$d_{m,n}=(\lambda_m||h_{AB,m}||-\lambda_n||h_{AB,n}||)^2$,1≤m≤L,1≤n≤L,m≠n;$Min(d_{m,n})$是指所有$d_{m,n}$值中的最小值;

[0014] 3)如果$Min(d_{m,n})>r$,则令$r=Min(d_{m,n})$,保存当前对应的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,返回步骤2),直至$\lambda_s=\sqrt{L}$;否则直接返回步骤2),直至$\lambda_s=\sqrt{L}$;重复步骤2)和步骤3),直至$\lambda_1,\lambda_2,\cdots,\lambda_L$的值都达到上限,输出最后保存的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,即为最优值。

[0015] 发送方生成的随机权值系数矩阵序列满足下述线性约束

$\mathbf{h}_{AB,1}^H\mathbf{W}_1+\mathbf{h}_{AB,2}^H\mathbf{W}_2+\cdots+\mathbf{h}_{AB,L}^H\mathbf{W}_L=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]$;其中,$\mathbf{h}_{AB,l}^H$表示信道矢量$h_{AB,1}$进行艾尔米特变换后得到的矢量,1≤1≤L。

[0016] 所述权值系数矩阵的生成过程包括:

[0017] 1)随机生成前L-1个权值系数矩阵$W_1,W_2,\cdots,W_{L-1}$;

[0018] 2)对于W_L,随机生成权值$w_{j,l}^{(L)},1\le j\le J-1,1\le l\le L$;

[0019] 3)权值$w_{J,l}^{(L)}=(\phi_l-\sum_{j=1}^{J-1}h_{A_jB,L}^*w_{j,l}^{(L)})/h_{A_JB,L}^*$;$w_{j,l}^{(L)}$表示权值系数矩阵$W_L$中第j行、第1列的

元素；其中$[\phi_1,\phi_2,\cdots,\phi_L]=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]-\sum_{l=1}^{L-1}\mathbf{h}_{AB,l}^{H}\mathbf{W}_l$，则$\mathbf{h}_{AB,L}^{H}\mathbf{W}_L=[\phi_1,\phi_2,\cdots,\phi_L]$；$h_{A_jB,L}^{*}$表示信道矢量$h_{AB,L}$的第j个分量的复共轭；$\mathbf{h}_{AB,l}^{H}$表示信道矢量$h_{AB,1}$进行艾尔米特变换后得到的矢量。

[0020] 相应地，本发明还提供了一种多天线二维矢量传输系统，其包括：

[0021] 发送方，在第一个时间块，发送方生成随机权值系数矩阵W_1；W_1与每个待发送符号矢量$\bar{\mathbf{x}}(n)$相乘得到$\mathbf{W}_1\bar{\mathbf{x}}(n)$，其中$\mathbf{W}_1\bar{\mathbf{x}}(n)$为J×1的叠加信号矢量；然后将该叠加信号矢量中每个分量分别加载到对应天线上发送；在该时间块的连续N个符号周期内，依次将$\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$发送一次；在下个时间块再生成新的随机权值系数矩阵，重复上述发送过程；$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T,n=1,2,\cdots,N$表示第n个符号周期待发送的符号矢量；J为发送天线的数量；x(n)表示待发符号序列的第n个符号；接收方，用于在接收到发送方发送的信号后，接收到发送方发送的信号后，利用下式解调，得到信号矢量$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]$：

[0022] $$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]=\arg\min_{\substack{x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]}}\{|y_{Bob}(n)-\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]|^2\}$$；

[0023] 其中，$y_{Bob}(n)=[\lambda_1\|\mathbf{h}_{AB,1}\|\quad\lambda_2\|\mathbf{h}_{AB,2}\|\quad\cdots\quad\lambda_L\|\mathbf{h}_{AB,L}\|]\begin{bmatrix}x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]\end{bmatrix}+v_{Bob}(n)$

$=\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]+v_{Bob}(n)$；$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T$；$\|h_{AB,1}\|$表示第1个时间块发送方到接收方的信道矢量$h_{AB,1}$的2-范式，$\|\mathbf{h}_{AB,l}\|=\sqrt{\sum_{j=1}^{J}|h_{A_jB,l}|^2}$；$h_{A_jB,l}$表示信道矢量$h_{AB,L}$的第j个分量，$|h_{A_jB,l}|$表示$h_{A_jB,l}$的模；$v_{Bob}(n)$表示接收端的噪声；L为信号矢量的维度，也即传输次数；$\lambda_1,\lambda_2,\cdots,\lambda_L$为实系数，且$\lambda_1,\lambda_2,\cdots,\lambda_L$为正数。

[0024] 与现有技术相比，本发明所具有的有益效果为：本发明仍旧服从经典信息论，将现有的一维传输体制(即每个符号周期每根传输天线只发送一个符号)扩展到二维传输体制，实现物理层的安全传输。本发明的传输安全性不再依赖于合法用户的信道优势，只需要合法信道和窃听信道之间存在足够的差异性。用于预编码的随机权值系数矩阵不需要传送给接收者。这些都使本发明很容易物理实现。在合法信道和窃听信道之间存在足够的差异性的前提下，本发明能抵抗MUSIC-like一类安全攻击，实现无条件安全，即保持窃听者的误码率不低于10^{-1}(无法有效解码)。

附图说明

[0025] 图1为本发明通信模型图；

[0026] 图2为MUSIC-like算法破解随机加权方案图；

[0027] 图3为不同矢量维度下的系统接收性能(L＝2,3,4)示意图；

[0028] 图4为不同的发送天线数量(J＝4,6,8)下的性能比较图；

[0029] 图5为不同的块长度(N＝6,8,10)下的性能比较图。

具体实施方式

[0030] 本发明通信模型如图1所示。设发送方Alice有J根天线，合法接收方Bob和多窃听方Eve都为单天线接收。Eve完全被动窃听，不发出任何电磁信号。Alice到Bob的信道记为$\mathbf{h}_{AB}=[h_{A_1B},h_{A_2B},\cdots,h_{A_JB}]^T$，该信道信息能被通信双方准确估计得到；Alice到Eve的信道记为$\mathbf{h}_{AE}=[h_{A_1E},h_{A_2E},\cdots,h_{A_JE}]^T$，该信道信息只能被Eve准确估计，而Alice不可能得到任何有用信息。假设该模型中所有无线信道是独立同分布的平坦衰落瑞利信道。为了下文描述方便，假设信道是块衰落，并统一简记块持续时间长度为N个符号周期。

[0031] 与现有一维传输体制完全不同，在二维矢量传输方案中，每个符号周期每根天线并行发送维度为L的符号矢量。从而，可以将对应N个连续符号周期(一个块)待发送的LN个符号写成L×N符号矩阵的形式。

[0032] 本发明与现有的一维物理层安全传输方案的不同是：现有方案是通过对应多天线的随机(复)权值向量引入随机变化，而本发明既保留了现有方案中利用随机向量扰动接收信号的优点，同时扩展而成的随机矩阵对多维符号进行随机加权预混叠，阻止了窃听者通过联合检测破解信号的可能性。但是因为每次传输的是一个L维符号矢量，根据最大熵原理，每个符号矢量需要重复传输至少L次，接收端才能恢复矢量中每个成分的正确位置信息。

[0033] 1.Alice的发送过程

[0034] 将N个连续符号周期内待发送的总数LN个符号(x(1),x(2),…,x(LN))交织成一个L×N符号矩阵

[0035] $$\mathbf{X}=\left[\bar{\mathbf{x}}(1)\quad\bar{\mathbf{x}}(2)\quad\cdots\quad\bar{\mathbf{x}}(N)\right]=\begin{bmatrix}x(1) & x(2) & \cdots & x(N)\\ x(1+N) & x(2+N) & \cdots & x(2N)\\ \vdots & \vdots & \ddots & \vdots\\ x[1+(L-1)N] & x[2+(L-1)N] & \cdots & x(LN)\end{bmatrix}\tag{1}$$

[0036] 其中，列向量$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T,n=1,2,\cdots,N$表示第n个符号周期待发送的符号矢量。

[0037] Alice用一个随机权值系数矩阵对每个待发送的符号矢量进行预编码，生成一个J维的随机加权叠加信号矢量，再通过J根天线发送出去。因此，Alice需要生成一个J×L随机权值系数矩阵(权值系数矩阵只与信道相关)

[0038] $$\mathbf{W}=\begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,L} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,L} \\ \vdots & \vdots & \ddots & \vdots \\ w_{J,1} & w_{J,2} & \cdots & w_{J,L} \end{bmatrix} \quad (2)$$

[0039] 在连续N个符号周期里，Alice依次将权值系数矩阵与N个符号矢量 $\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$ 相乘，得到一个J×N信号矩阵，其中每个列向量是J维叠加信号，刚好对应J根发送天线。

[0040] 具体的发送过程如下：在第一个时间块(对应块衰落信道的平稳块)，Alice先生成随机权值系数矩阵W_1。W_1与每个待发送符号矢量 $\bar{\mathbf{x}}(n)$ 相乘得到 $\mathbf{W}_1\bar{\mathbf{x}}(n)$，其中 $\mathbf{W}_1\bar{\mathbf{x}}(n)$ 为J×1的叠加信号矢量。然后将该矢量中每个元素(对应一个叠加信号)分别加载到对应天线上发送。这样在连续N个符号周期内，可以依次将 $\bar{\mathbf{x}}(1),\bar{\mathbf{x}}(2),\cdots,\bar{\mathbf{x}}(N)$ 发送一次。在下个时间块再生成新的随机权值系数矩阵，重复同样发送过程。这个发送过程总共重复至少L次，每次对应符号周期数为N。所以，LN个符号发送的总时间依然为LN，与现有一维传输体制一样。

[0041] 本发明中，随机权值系数矩阵中的元素服从均匀分布。

[0042] 2.Bob的接收过程

[0043] 对应第一个时间块第n个符号周期，Alice发送的叠加信号矢量为 $\mathbf{W}_1\bar{\mathbf{x}}(n)$。经过信道矢量$h_{AB,1}$(下标1表示第一个时间块，下同)后，Bob收到的叠加矢量信号为

[0044] $$y_1(n)=\mathbf{h}_{AB,1}^{H}\mathbf{W}_1\bar{\mathbf{x}}(n)+v_B(n),\quad (n=1,2,\cdots,N) \quad (3)$$

[0045] 其中$v_B(n)$为电路噪声(硬件带来的噪声)，一般为加性白高斯噪声。

[0046] 同样，在第l(1≤l≤L)个时间块，信道矢量为$h_{AB,l}$，权值系数矩阵变为W_l。相应地，Bob收到的叠加矢量信号为$y_l(1),y_l(2),\cdots,y_l(N)$。因此，经过L次传输后，即在总时间LN内，Bob依次接收到信号可以写成一个L×N接收信号矩阵

[0047] $$\begin{bmatrix} y_1(1) & y_1(2) & \cdots & y_1(N) \\ y_2(1) & y_2(2) & \cdots & y_2(N) \\ \vdots & \vdots & \ddots & \vdots \\ y_L(1) & y_L(2) & \cdots & y_L(N) \end{bmatrix} \quad (4)$$

[0048] 由于矩阵中每个元素实际代表一个叠加矢量信号，所以该矩阵可以看成一个三维矩阵。矩阵每个列向量的所有分量都来自于同一个发送符号矢量。

[0049] 为恢复原始信号，记累加矢量为$s=[1,1,\cdots,1]_{1\times L}$，Bob将(4)式对应于同一发送符号矢量的叠加信号进行累加

[0050]
$$y_{Bob}(n)=\mathbf{s}\begin{bmatrix}y_1(n)\\y_2(n)\\\vdots\\y_L(n)\end{bmatrix}$$
$$=\mathbf{h}_{AB,1}^H\mathbf{W}_1\bar{\mathbf{x}}(n)+\mathbf{h}_{AB,2}^H\mathbf{W}_2\bar{\mathbf{x}}(n)+\cdots+\mathbf{h}_{AB,L}^H\mathbf{W}_L\bar{\mathbf{x}}(n)$$
$$=(\mathbf{h}_{AB,1}^H\mathbf{W}_1+\mathbf{h}_{AB,2}^H\mathbf{W}_2+\cdots+\mathbf{h}_{AB,L}^H\mathbf{W}_L)\bar{\mathbf{x}}(n) \quad (5)$$

[0051] 为了能从$y_{Bob}(n)$中恢复原始符号矢量$\bar{\mathbf{x}}(n)$，一种简单的方法是使Alice生成的随机权值系数矩阵序列满足下述线性约束

[0052]
$$\mathbf{h}_{AB,1}^H\mathbf{W}_1+\mathbf{h}_{AB,2}^H\mathbf{W}_2+\cdots+\mathbf{h}_{AB,L}^H\mathbf{W}_L$$
$$=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|] \quad (6)$$

[0053] 其中，$||h_{AB,1}||$表示信道矢量$h_{AB,1}$的2-范式。$\lambda_1,\lambda_2,\cdots,\lambda_L$为一组公开的实系数。由于实际中，我们无法保证信道系数$||h_{AB,1}||,||h_{AB,2}||,\cdots,||h_{AB,L}||$之间具有明显的差异，因此需要附加$\lambda_1,\lambda_2,\cdots,\lambda_L$去保证Bob能够正确解调。

[0054] (6)式对应的一种简单权值系数矩阵的生成算法如下：先随机生成L-1个权值系数矩阵$W_1,W_2,\cdots,W_{L-1}$，再通过(6)式约束求解最后一个矩阵W_L。设

$[\phi_1,\phi_2,\cdots,\phi_L]=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]-\sum_{l=1}^{L-1}\mathbf{h}_{AB,l}^H\mathbf{W}_l$，那么$\mathbf{h}_{AB,L}^H\mathbf{W}_L=[\phi_1,\phi_2,\cdots,\phi_L]$。

算法 1 权值系数矩阵生成算法（此处以生成$\mathbf{W}_L$的最后一行为例）

1. 随机生成前$L-1$个权值系数矩阵$\mathbf{W}_1,\mathbf{W}_2,\cdots,\mathbf{W}_{L-1}$；
2. 对于$\mathbf{W}_L$，随机生成权值$w_{j,l}^{(L)},1\le j\le J-1,1\le l\le L$；

[0055]
3. 权值$w_{J,l}^{(L)}=(\phi_l-\sum_{j=1}^{J-1}h_{A_jB,L}^*w_{j,l}^{(L)})/h_{A_JB,L}^*$；、$w_{j,l}^{(L)}$表示权值系数矩阵中第$j$行、第$l$列的元素；其中$[\phi_1,\phi_2,\cdots,\phi_L]=[\lambda_1\|\mathbf{h}_{AB,1}\|,\lambda_2\|\mathbf{h}_{AB,2}\|,\cdots,\lambda_L\|\mathbf{h}_{AB,L}\|]-\sum_{l=1}^{L-1}\mathbf{h}_{AB,l}^H\mathbf{W}_l$，则$\mathbf{h}_{AB,L}^H\mathbf{W}_L=[\phi_1,\phi_2,\cdots,\phi_L]$；$h_{A_jB,L}^*$表示信道矢量$\mathbf{h}_{AB,L}$的第$j$个分量的复共轭。

[0056] 将(6)式代入(5)式，Bob收到的信号表示为

[0057]
$$y_{Bob}(n)=[\lambda_1\|\mathbf{h}_{AB,1}\|\quad\lambda_2\|\mathbf{h}_{AB,2}\|\quad\cdots\quad\lambda_L\|\mathbf{h}_{AB,L}\|]\bar{\mathbf{x}}(n) \quad (7)$$

[0058] 再将$\bar{\mathbf{x}}(n)=[x(n),x(n+N),\cdots,x[n+(L-1)N]]^T$代入(7)式，有

[0059]
$$y_{Bob}(n)=[\lambda_1\|\mathbf{h}_{AB,1}\| \quad \lambda_2\|\mathbf{h}_{AB,2}\| \quad \cdots \quad \lambda_L\|\mathbf{h}_{AB,L}\|]\begin{bmatrix} x(n) \\ x(n+N) \\ \vdots \\ x[n+(L-1)N] \end{bmatrix}+v_{Bob}(n)$$
$$=\lambda_1\|\mathbf{h}_{AB,1}\|x(n)+\lambda_2\|\mathbf{h}_{AB,2}\|x(n+N)+\cdots+\lambda_L\|\mathbf{h}_{AB,L}\|x[n+(L-1)N]+v_{Bob}(n)$$
$$=\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]+v_{Bob}(n) \tag{8}$$

[0060] 所以,一种扩展的最大似然检测方法如下

[0061]
$$[\tilde{x}(n),\tilde{x}(n+N),\cdots,\tilde{x}[n+(L-1)N]]$$
$$=\arg\min_{\substack{x(n)\\x(n+N)\\\vdots\\x[n+(L-1)N]}}\{|y_{Bob}(n)-\sum_{l=1}^{L}\lambda_l\|\mathbf{h}_{AB,l}\|x[n+(l-1)N]|^2\} \tag{9}$$

[0062] 图2是用MUSIC-like算法破解现有随机加权方案的性能曲线图。Alice有4根发送天线。窃听者Eve分别在不同的窃听天线数量下(m=1,4,6,8)进行窃听,并采用MUSIC-like算法对窃听到的信号进行联合检测。从图中可以看出,当Eve接收天线数小于发送天线数时,BER保持在0.5附近,说明此时随机加权方案依然有效。当接收天线数大于或等于发送天线数时,BER下降。这说明MUSIC-like算法确实可以破解随机加权方案。

[0063] 对方案性能的仿真实验以误码率作为衡量系统安全的性能指标。假设Alice发送天线个数为4(J=4)。Alice到Bob和Eve的信道服从瑞利平坦衰落,在一个数据块(N=8)内保持不变,不同块间独立变化。规整化后,Alice到Bob和Eve的信道矢量(矩阵)中的元素是独立同分布的零均值、单位方差的复Gauss随机变量,并且在一个块内保持不变。Alice总共发送1万个符号,每个信号符号从集合{+1,-1}中等概率产生。

[0064] 图3是本发明的系统接收性能曲线。Alice在不同的L(L=1,2,3,4)情况下发送符号或符号矢量,Bob采用(9)式对接收信号进行恢复。Eve采用两种破解方式:一种是MUSIC-like;另一种是(9)式。当L=1时,本发明方案将退化成一维传输体制下的随机加权方案。

[0065] 从图3可知,随着Alice发送符号矢量的维度(L)增加,Bob的误码率升高。这是因为(9)式中,Bob是从叠加信号矢量中检测出每个符号成分,这种检测方式需要利用系数$\lambda_1||h_{AB,1}||$,$\lambda_2||h_{AB,2}||$,…,$\lambda_L||h_{AB,L}||$之间的差异性。当L增加时,同时也增加了从两个不同符号矢量计算出相同范数的概率。同时发现,无论Eve采用何种检测方法,其误码率都大约维持在0.5左右。所以方案实现了无条件安全。

[0066] 图4是方案在不同的发送天线数量(J=4,6,8)下的性能比较。从图中可以看出,相同的符号矢量维度时,随着发送天线数J的不同,Bob的BER并没有明显的变化。因此,发送天线数J对Bob的误码率影响甚微。类似,如图5所示,块长度(信道的稳定状态)对Bob的误码率影响甚微。

[0067] 本发明中发送的符号序列(x(1),x(2),…)仍旧是常规调制信号,与现有通信系统比较并无二致。$\lambda_1,\lambda_2,...,\lambda_L$均为正数,只在最后一次传输计算随机权值系数矩阵$W_L$时才需要,此时前面L-1次传输已经完成。设发送端的信息序列、信道衰落系数和信道噪声彼此相互独立,考虑到发送端额定功率限制,显然有$\lambda_1^2+\lambda_2^2+\cdots+\lambda_L^2=L$,L表示符号矢量的维度(也

即重复次数)。

[0068] 另一方面,对合法接收者而言,其误码率很大程度取决于$\lambda_1||h_{AB,1}||,\lambda_2||h_{AB,2}||,\ldots,\lambda_L||h_{AB,L}||$之间的差异性,即系数$\lambda_1,\lambda_2,\ldots,\lambda_L$应该让$\lambda_1||h_{AB,1}||,\lambda_2||h_{AB,2}||,\ldots,\lambda_L||h_{AB,L}||$之间的差异足够大。

[0069] 记$d_{m,n}=(\lambda_m||h_{AB,m}||-\lambda_n||h_{AB,n}||)^2$,$1\leqslant m\leqslant L$,$1\leqslant n\leqslant L$,$m\neq n$,表示$\lambda_m||h_{AB,m}||$与$\lambda_n||h_{AB,n}||$之间的差异。$Min(d_{m,n})$表示所有$d_{m,n}$($1\leqslant m\leqslant L$,$1\leqslant n\leqslant L$,$m\neq n$)值中的最小值。本传输方案中,准则是$\lambda_1,\lambda_2,\ldots,\lambda_L$系数应该使$Min(d_{m,n})$最大化。

[0070] $\lambda_1,\lambda_2,\ldots,\lambda_L$的生成算法如下所示。显然,该算法为一个穷举算法,每次循环λ_i递增t(实验中t取0.1)。显然λ_i最小值0.1(不能为0),最大值$\sqrt{L}$。实际应用中,可以根据各种先验知识进一步优化寻优过程。

[0071] $\lambda_1,\lambda_2,\cdots,\lambda_L$的求解过程包括:

[0072] 1)设r=0;步长为t;$\lambda_1,\lambda_2,\cdots,\lambda_L$均初始化为0.1;

[0073] 2)对于λ_s,递增t,然后计算$Min(d_{m,n})$ $1\leqslant s\leqslant L$,其中$d_{m,n}=(\lambda_m||h_{AB,m}||-\lambda_n||h_{AB,n}||)^2$,$1\leqslant m\leqslant L$,$1\leqslant n\leqslant L$,$m\neq n$;$Min(d_{m,n})$是指所有$d_{m,n}$值中的最小值;

[0074] 3)如果$Min(d_{m,n})>r$,则令$r=Min(d_{m,n})$,保存当前对应的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,返回步骤2),直至$\lambda_s=\sqrt{L}$;否则直接返回步骤2),直至$\lambda_s=\sqrt{L}$;重复步骤2)和步骤3),直至$\lambda_1,\lambda_2,\cdots,\lambda_L$的值都达到上限,输出最后保存的$\lambda_1,\lambda_2,\cdots,\lambda_L$值,即为最优值。

[0075] 本发明中,步长设置为0.1,是为了在合适的计算量的前提下,保证计算精度。本发明方案的安全性认证分析如下:

[0076] 1.多窃听者采用MUSIC-like算法

[0077] 假设有M个单天线窃听者,接收条件与合法接收者Bob一样,即每根天线(窃听者)都能正常接收L次传输的N个叠加信号。作为一个整体,则M个窃听者的接收的L次传输的信号可以写成M×N矩阵的形式

[0078]
$$\mathbf{Y}_{Eve}=\begin{bmatrix} y_{Eve_1}(1) & y_{Eve_1}(2) & \cdots & y_{Eve_1}(N) \\ y_{Eve_2}(1) & y_{Eve_2}(2) & \cdots & y_{Eve_2}(N) \\ \vdots & \vdots & \ddots & \vdots \\ y_{Eve_M}(1) & y_{Eve_M}(2) & \cdots & y_{Eve_M}(N) \end{bmatrix} \tag{1}$$

[0079] 式中,$y_{Eve_m}(n),1\leq m\leq M,1\leq n\leq N$表示第m个窃听者将接收的所有L次传输的第n个叠加信号累加而成,$v_{Eve_m}(n)$表示第m个窃听者端的噪声,即

[0080]
$$\begin{aligned} y_{Eve_m}(n)&=y_{Eve_m,1}(n)+y_{Eve_m,2}(n)+\cdots+y_{Eve_m,L}(n) \\ &=\mathbf{h}_{AE_m,1}^H\mathbf{W}_1(n)\bar{\mathbf{x}}(n)+\mathbf{h}_{AE_m,2}^H\mathbf{W}_2(n)\bar{\mathbf{x}}(n)+\cdots+\mathbf{h}_{AE_m,L}^H\mathbf{W}_L(n)\bar{\mathbf{x}}(n)+v_{Eve_m}(n) \\ &=[\mathbf{h}_{AE_m,1}^H \quad \mathbf{h}_{AE_m,2}^H \quad \cdots \quad \mathbf{h}_{AE_m,L}^H]\begin{bmatrix} \mathbf{W}_1(n)\bar{\mathbf{x}}(n) \\ \mathbf{W}_2(n)\bar{\mathbf{x}}(n) \\ \vdots \\ \mathbf{W}_L(n)\bar{\mathbf{x}}(n) \end{bmatrix}+v_{Eve_m}(n) \end{aligned} \tag{2}$$

[0081] 将(2)代入(1)式,有

[0082] $$\mathbf{Y}_{Eve}=\mathbf{H}_{AE}\mathbf{E}(w,\bar{x})+v_{Eve} \tag{3}$$

[0083] 其中

[0084] $$\mathbf{H}_{AE}=\begin{bmatrix}\mathbf{h}_{AE_1,1}^{H} & \mathbf{h}_{AE_1,2}^{H} & \cdots & \mathbf{h}_{AE_1,L}^{H}\\ \mathbf{h}_{AE_2,1}^{H} & \mathbf{h}_{AE_2,2}^{H} & \cdots & \mathbf{h}_{AE_2,L}^{H}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{h}_{AE_M,1}^{H} & \mathbf{h}_{AE_M,2}^{H} & \cdots & \mathbf{h}_{AE_M,L}^{H}\end{bmatrix} \tag{4}$$

[0085] $$\mathbf{E}(w,\bar{x})=\begin{bmatrix}\mathbf{W}_1(1)\bar{\mathbf{x}}(1) & \mathbf{W}_1(2)\bar{\mathbf{x}}(2) & \cdots & \mathbf{W}_1(N)\bar{\mathbf{x}}(N)\\ \mathbf{W}_2(1)\bar{\mathbf{x}}(1) & \mathbf{W}_2(2)\bar{\mathbf{x}}(2) & \cdots & \mathbf{W}_2(N)\bar{\mathbf{x}}(N)\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{W}_L(1)\bar{\mathbf{x}}(1) & \mathbf{W}_L(2)\bar{\mathbf{x}}(2) & \cdots & \mathbf{W}_L(N)\bar{\mathbf{x}}(N)\end{bmatrix} \tag{5}$$

[0086] $\mathbf{W}_1(n)$为J×L的矩阵,设$\mathbf{W}_1(n)$为如下矩阵

[0087] $$\mathbf{W}_l(n)=\begin{bmatrix}w_{1,1}^{l}(n) & w_{1,2}^{l}(n) & \cdots & w_{1,L}^{l}(n)\\ w_{2,1}^{l}(n) & w_{2,2}^{l}(n) & \cdots & w_{2,L}^{l}(n)\\ \vdots & \vdots & \ddots & \vdots\\ w_{J,1}^{l}(n) & w_{J,2}^{l}(n) & \cdots & w_{J,L}^{l}(n)\end{bmatrix} \tag{6}$$

[0088] 对$\mathbf{W}_l(n)\bar{\mathbf{x}}(n)$有

$$\mathbf{W}_l(n)\bar{\mathbf{x}}(n)=\begin{bmatrix}w_{1,1}^{l}(n)\\ w_{2,1}^{l}(n)\\ \vdots\\ w_{J,1}^{l}(n)\end{bmatrix}x(n)+\begin{bmatrix}w_{1,2}^{l}(n)\\ w_{2,2}^{l}(n)\\ \vdots\\ w_{J,2}^{l}(n)\end{bmatrix}x(n+N)+\cdots+\begin{bmatrix}w_{1,L}^{l}(n)\\ w_{2,L}^{l}(n)\\ \vdots\\ w_{J,L}^{l}(n)\end{bmatrix}x[n+(L-1)N]$$

[0089]

$$=\sum_{i=1}^{L}\left\{\begin{bmatrix}w_{1,i}^{l}(n)\\ w_{2,i}^{l}(n)\\ \vdots\\ w_{J,i}^{l}(n)\end{bmatrix}x[n+(i-1)N]\right\} \tag{7}$$

[0090] 为了方便,记$\boldsymbol{\alpha}_{l,i}(n)=\begin{bmatrix}w_{1,i}^{l}(n)\\ w_{2,i}^{l}(n)\\ \vdots\\ w_{J,i}^{l}(n)\end{bmatrix}$,有

[0091] $$\mathbf{W}_l(n)\bar{\mathbf{x}}(n)=\sum_{i=1}^{L}\boldsymbol{\alpha}_{l,i}(n)x[n+(i-1)N] \tag{8}$$

[0092] 将(8)式代入$\mathbf{E}(w,\bar{x})$,整理后得

$$\mathbf{E}(w,\bar{x})=$$

[0093]
$$\sum_{i=1}^{L}\begin{bmatrix}\boldsymbol{\alpha}_{1,i}(1)x[1+(i-1)N] & \boldsymbol{\alpha}_{1,i}(2)x[2+(i-1)N] & \cdots & \boldsymbol{\alpha}_{1,i}(N)x[N+(i-1)N]\\ \boldsymbol{\alpha}_{2,i}(1)x[1+(i-1)N] & \boldsymbol{\alpha}_{2,i}(2)x[2+(i-1)N] & \cdots & \boldsymbol{\alpha}_{2,i}(N)x[N+(i-1)N]\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{\alpha}_{L,i}(1)x[1+(i-1)N] & \boldsymbol{\alpha}_{L,i}(2)x[2+(i-1)N] & \cdots & \boldsymbol{\alpha}_{L,i}(N)x[N+(i-1)N]\end{bmatrix} \quad (9)$$

[0094] 由(6)式有

[0095]
$$\mathbf{h}_{AB,1}^{H}\boldsymbol{\alpha}_{1,i}(n)+\mathbf{h}_{AB,2}^{H}\boldsymbol{\alpha}_{2,i}(n)+\cdots+\mathbf{h}_{AB,L}^{H}\boldsymbol{\alpha}_{L,i}(n)=\lambda_i\left\|\mathbf{h}_{AB,i}\right\| \quad (10)$$

[0096] 为了方便,记$\boldsymbol{\theta}_i(n)=\begin{bmatrix}\boldsymbol{\alpha}_{1,i}(n)\\ \boldsymbol{\alpha}_{2,i}(n)\\ \vdots\\ \boldsymbol{\alpha}_{L,i}(n)\end{bmatrix}$, $\boldsymbol{\delta}_{AB}=\begin{bmatrix}\mathbf{h}_{AB,1}\\ \mathbf{h}_{AB,2}\\ \vdots\\ \mathbf{h}_{AB,L}\end{bmatrix}$,则(10)式可写为

[0097]
$$\boldsymbol{\delta}_{AB}^{H}\boldsymbol{\theta}_i(n)=\lambda_i\left\|\mathbf{h}_{AB,i}\right\| \quad (11)$$

[0098] 我们尝试对$\theta_i(n)x[n+(i-1)N]$进行类似MUSIC-like算法的分解,将传输信号序列分解为子矩阵。

[0099] 由(11)式,有$\boldsymbol{\delta}_{AB}^{H}\left[\boldsymbol{\theta}_i(n)-\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|\right]=0$,则$\left[\boldsymbol{\theta}_i(n)-\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|\right]$在$\boldsymbol{\delta}_{AB}^{H}$的零空间上。因此,$x[n+(i-1)N]\left[\boldsymbol{\theta}_i(n)-\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|\right]$也在$\boldsymbol{\delta}_{AB}^{H}$的零空间上,其可以写为

[0100]
$$x[n+(i-1)N]\left[\boldsymbol{\theta}_i(n)-\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|\right]=\sum_{k=1}^{JL-1}\eta_k[n+(i-1)N]\boldsymbol{\varphi}_k \quad (12)$$

[0101] 其中$(\boldsymbol{\varphi}_1,\ \boldsymbol{\varphi}_2,\ \cdots\ \boldsymbol{\varphi}_{JL-1})$为$\boldsymbol{\delta}_{AB}^{H}$零空间的单位正交基,$\eta_k[n+(i-1)N]$为对应的投影系数(坐标)。有

[0102]
$$\boldsymbol{\theta}_i(n)x[n+(i-1)N]=\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|x[n+(i-1)N]+\sum_{k=1}^{JL-1}\varphi_k\eta_k[n+(i-1)N] \quad (13)$$

[0103] 即

[0104]
$$\begin{bmatrix}\boldsymbol{\alpha}_{1,i}(n)\\ \boldsymbol{\alpha}_{2,i}(n)\\ \vdots\\ \boldsymbol{\alpha}_{L,i}(n)\end{bmatrix}x[n+(i-1)N]=\begin{bmatrix}\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\| & \boldsymbol{\varphi}_1 & \cdots & \boldsymbol{\varphi}_{JL-1}\end{bmatrix}\begin{bmatrix}x[n+(i-1)N]\\ \eta_1[n+(i-1)N]\\ \vdots\\ \eta_{JL-1}[n+(i-1)N]\end{bmatrix} \quad (14)$$

[0105] 显然,对于不同的i值,$\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^2}\lambda_i\left\|\mathbf{h}_{AB,i}\right\|$是不一样的。因此(9)式$\mathbf{E}(w,\bar{x})$无法将传输信号序列类似MUSIC-like算法一样将其单独分离成一行或一列。因此MUSIC-like算法无法破解。

[0106] 2.采用Bob同样的检测方法

[0107] 记$y_{Eve,1}(n)$为任意窃听者的第1次传输的第n个接收信号。如果Eve采用和Bob同样的方式检测信号，类似地，对于每一次传输的第n个接收信号，其累加可以写成

$$y_{Eve}(n)=y_{Eve,1}(n)+y_{Eve,2}(n)+\cdots+y_{Eve,L}(n)$$

$$=\mathbf{h}_{AE,1}^{H}\mathbf{W}_{1}(n)\bar{\mathbf{x}}(n)+\mathbf{h}_{AE,2}^{H}\mathbf{W}_{2}(n)\bar{\mathbf{x}}(n)+\cdots+\mathbf{h}_{AE,L}^{H}\mathbf{W}_{L}(n)\bar{\mathbf{x}}(n)+v_{Eve}(n)$$

[0108]

$$=\sum_{i=1}^{L}\left[\mathbf{h}_{AE,1}^{H},\mathbf{h}_{AE,2}^{H},\cdots,\mathbf{h}_{AE,L}^{H}\right]\begin{bmatrix}\boldsymbol{\alpha}_{1,i}(n)\\ \boldsymbol{\alpha}_{1,i}(n)\\ \vdots\\ \boldsymbol{\alpha}_{1,i}(n)\end{bmatrix}x\left[n+(i-1)N\right]+v_{Eve}(n)$$

[0109] 设$\boldsymbol{\delta}_{AE}=\begin{bmatrix}\mathbf{h}_{AE,1}\\ \mathbf{h}_{AE,2}\\ \vdots\\ \mathbf{h}_{AE,L}\end{bmatrix}$，将(14)式代入上式，显然有

[0110] $$y_{Eve}(n)=\sum_{i=1}^{L}\{\boldsymbol{\delta}_{AE}^{H}\frac{\boldsymbol{\delta}_{AB}}{\left\|\boldsymbol{\delta}_{AB}\right\|^{2}}\lambda_{i}\left\|\mathbf{h}_{AB,i}\right\|x\left[n+(i-1)N\right]+\boldsymbol{\delta}_{AE}^{H}\sum_{k=1}^{JL-1}\boldsymbol{\varphi}_{k}\eta_{k}\left[n+(i-1)N\right]\}+v_{Eve}(n)$$

[0111] 容易发现，由于$\boldsymbol{\delta}_{AE}^{H}$与$\boldsymbol{\varphi}_{k}$是相互独立的两个量，而$\eta_{k}[n+(i-1)N]$在不同的n上是变化的，因此$\boldsymbol{\delta}_{AE}^{H}\sum_{k=1}^{JL-1}\boldsymbol{\varphi}_{k}\eta_{k}\left[n+(i-1)N\right]$的任何变化都会影响到窃听者的接收信号$y_{Eve}(n)$。所以Eve无法求解出传输信号。

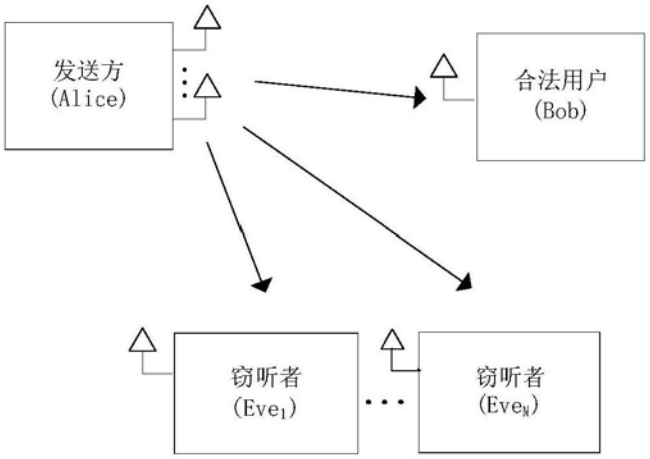

发送方
(Alice)
合法用户
(Bob)
窃听者
(Eve1)
窃听者
(EveM)

图1

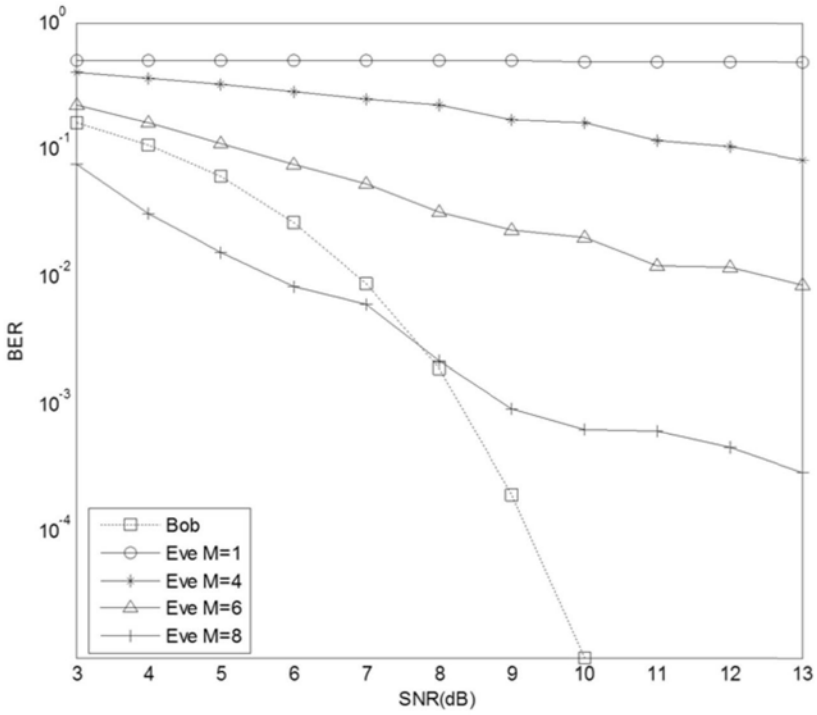

BER
SNR(dB)
Bob
Eve M=1
Eve M=4
Eve M=6
Eve M=8

图2

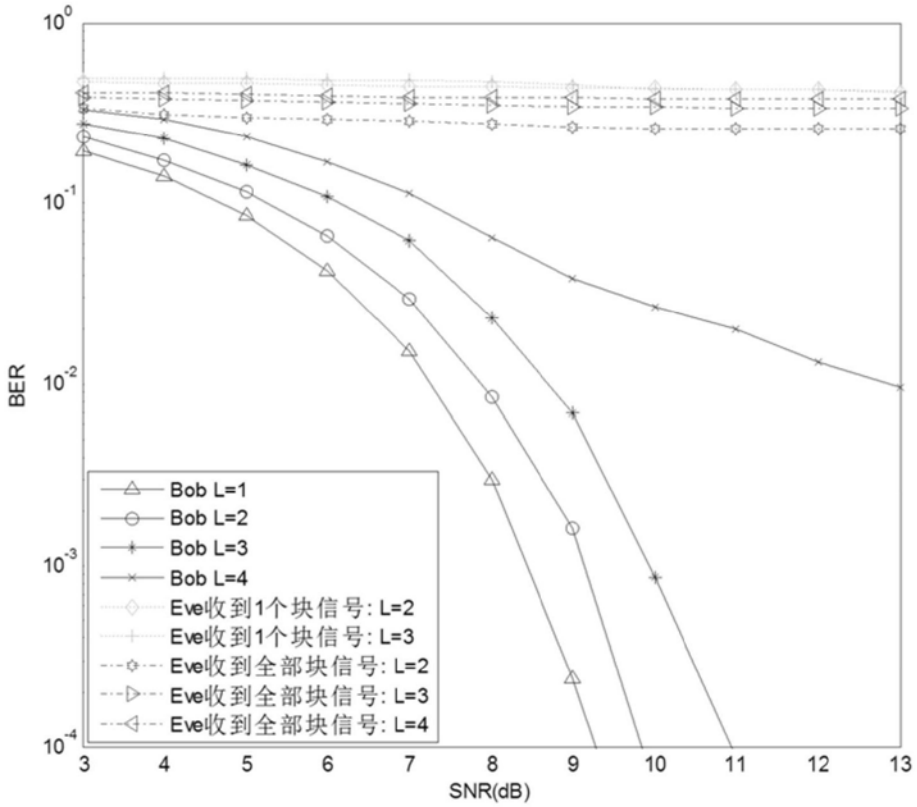

BER
SNR(dB)
Bob L=1
Bob L=2
Bob L=3
Bob L=4
Eve收到1个块信号: L=2
Eve收到1个块信号: L=3
Eve收到全部块信号: L=2
Eve收到全部块信号: L=3
Eve收到全部块信号: L=4

图3

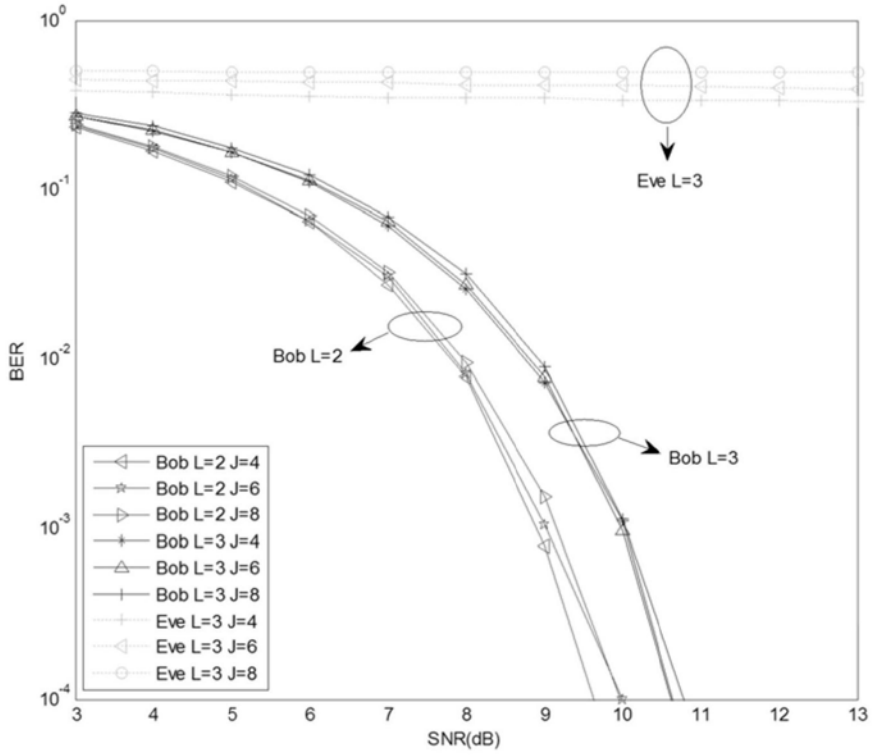

BER
SNR(dB)
Eve L=3
Bob L=2
Bob L=3
Bob L=2 J=4
Bob L=2 J=6
Bob L=2 J=8
Bob L=3 J=4
Bob L=3 J=6
Bob L=3 J=8
Eve L=3 J=4
Eve L=3 J=6
Eve L=3 J=8

图4

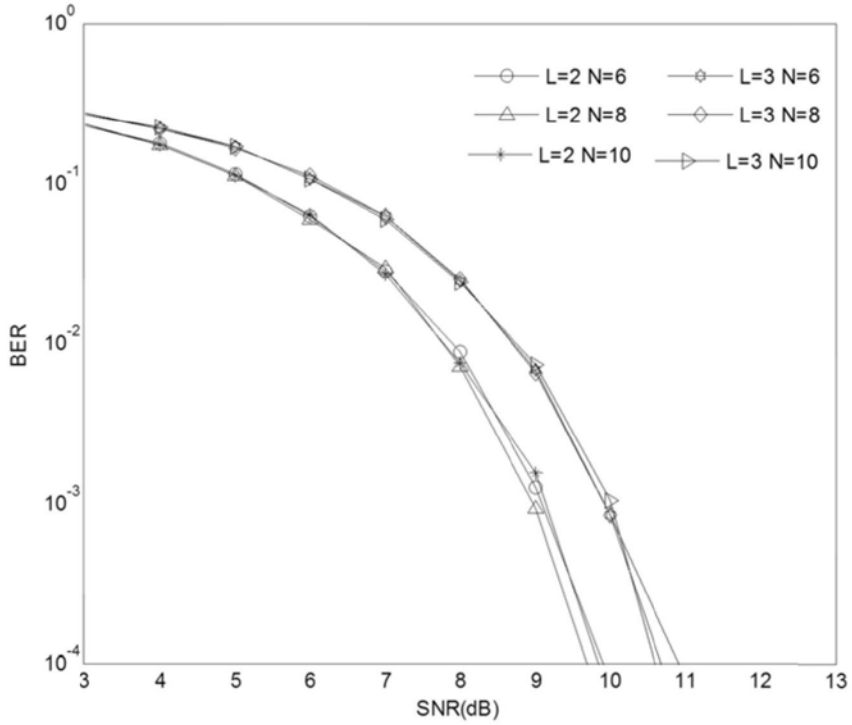

L=2 N=6
L=3 N=6
L=2 N=8
L=3 N=8
L=2 N=10
L=3 N=10
BER
SNR(dB)
10^0
10^-1
10^-2
10^-3
10^-4
3
4
5
6
7
8
9
10
11
12
13

图5