(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 106230552 B
(45)授权公告日 2019.04.23

(21)申请号 201610600089.4

(22)申请日 2016.07.27

(65)同一申请的已公布的文献号
申请公布号 CN 106230552 A

(43)申请公布日 2016.12.14

(73)专利权人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号

(72)发明人 刘炜炘 刘军 宋晓诗 叶宁 耿蓉

(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 李在川

(51)Int.Cl.
H04L 1/00(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 105119645 A,2015.12.02,
CN 105657698 A,2016.06.08,
CN 104469755 A,2015.03.25,
CN 1889367 A,2007.01.03,
CN 102724026 A,2012.10.10,
CN 101753149 A,2010.06.23,
US 2015188662 A1,2015.07.02,
王亚东,黄开枝,吉江, 钟州.部分信道特征下的物理层安全编码方法.《计算机应用研究》.2012,第29卷(第9期),
王亚东.等效信道特征下的物理层安全编码.《中国优秀硕士学位论文全文数据库 信息科技辑》.2013,(第06期),
Qiang Li, Wing-Kin Ma.Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise.《2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)》.2011,

审查员 温丽丽

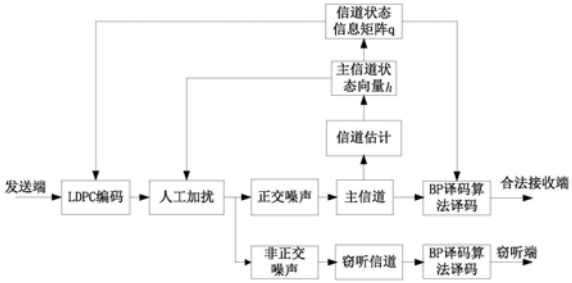
权利要求书1页 说明书7页 附图2页

(54)发明名称

星地链路中结合人工加扰和LDPC安全编码的信息传输方法

(57)摘要

星地链路中结合人工加扰和LDPC安全编码的信息传输方法,属于卫星通信技术领域;该方法包括:步骤1:计算主信道的状态向量;步骤2:计算主信道状态信息矩阵;步骤3:对待发送信息进行LDPC编码;步骤4:构建与主信道正交的人工噪声z;步骤5:计算使私密中断概率达到最小的待发送信息的发送权重;步骤6:连续发送编码后的待发送信息,同时采用多天线发射的方式发送人工噪声;步骤7:接收端采用BP译码算法译码;本发明在信息传输过程中,将信道状态信息引入LDPC编码中,保证通信的安全性和可靠性;采用基于信道状态信息的编码方法,避免传统加密算法运用在卫星通信过程中存在的问题;降低卫星保密通信的复杂度。



CN 106230552 B

1.星地链路中结合人工加扰和LDPC安全编码的信息传输方法,包括如下步骤:

步骤1:计算主信道的状态向量h,主信道为星地通信中合法信道;

步骤2:对主信道状态向量h的幅度向量进行循环移位N-1次,将得到的N-1个向量与主信道状态向量h的幅度向量一起构成N×N维主信道状态信息矩阵q;

步骤3:利用主信道状态信息矩阵q对待发送信息进行LDPC编码;

步骤4:构建与主信道正交的人工噪声z;

步骤5:计算使私密中断概率p_{so}达到最小的待发送信息的发送权重w;

步骤6:发送端以功率$||w||^2$连续发送编码后的待发送信息,同时采用多天线发射的方式发送人工噪声;

步骤7:接收端接收发送端发送的信息,并采用BP译码算法对信息进行译码;

其特征在于:步骤3具体包括:

步骤3-1:利用信道状态信息矩阵q生成校验矩阵H';

步骤3-1-1:确定LDPC编码的码率k/n,其中k为待发送信息S的序列长度,n为编码后待发送信号的序列长度;

步骤3-1-2:构造μ×n维矩阵H_1,n为μ的ω_r倍,且ω_r大于1,采用LDPC编码方法对H_1赋值;

步骤3-1-3:对矩阵H_1进行随机行列变换得到矩阵H_2,H_3,…,H_d,其中d=n-k/μ;

步骤3-1-4:将矩阵H_1到H_d级联得到(n-k)×n维初始校验矩阵$H=[H_1,H_2,\cdots,H_d]^T$;

步骤3-1-5:生成(n-k)×n维估计矩阵D,D中元素均为1;

步骤3-1-6:将信道状态信息矩阵q嵌入D中,得到D';

步骤3-1-7:计算校验矩阵H':

H'=mod(D'•*H)

其中,mod为模二运算;

步骤3-2:使用PEG算法对校验矩阵H'去小环,得到去小环后的校验矩阵H";

步骤3-3:使用去小环后的校验矩阵H"对待发送信息S进行编码。

2.根据权利要求1所述的星地链路中结合人工加扰和LDPC安全编码的信息传输方法,其特征在于:所述步骤5,具体步骤为:

步骤5-1:设定发射总功率P;

步骤5-2:计算人工噪声的协方差矩阵Σ';

步骤5-3:根据不等式约束计算待发送信息的发送权重w,使私密中断概率p_{so}达到最小,即:

$p_{so}=\min\ p(SNR_E>\gamma_E)$

不等式约束如下:$||w||^2+Tr(\Sigma')\leq P$,$SNR_B\geq\gamma_B$,其中,$SNR_E$为窃听端信噪比,$SNR_B$为合法接收端信噪比,Tr(•)表示求矩阵迹,$||w||^2$是待发送信息的发送功率,$\gamma_E$为窃听端误码率最小阈值对应的信噪比,$\gamma_B$为合法接收端误码率最大阈值对应的信噪比。

星地链路中结合人工加扰和LDPC安全编码的信息传输方法

技术领域

[0001] 本发明属于卫星通信技术领域，具体涉及星地链路中结合人工加扰和LDPC安全编码的信息传输方法。

背景技术

[0002] 相比于地面无线通信，轨道公开、具有大范围广播特性的卫星通信更易受到窃听、截获等安全威胁。现有的应对手段主要是对数据进行加密处理，在通信协议栈的上层来保障安全，加密处理存在的主要问题如下：(1)破解概率高。由于卫星处理能力有限，难以处理复杂的加密算法，随着计算机的快速发展及云计算、超算等新概念的出现，基于大数运算的传统加密算法面临严峻的挑战；(2)密分难度大。链路长延时、非持续连通的特性使得节点之间难以建立起信任关系，依靠在线信任授权机构的密钥分发管理面临诸多问题；(3)条件要求高。传统加密方法复杂度高，对系统的软硬件都有较高要求，难以适应卫星节点能力有限的特点。且复杂的处理过程还会增加时延，在卫星这种长时延网络中，愈发影响业务的实时性；(4)误码影响大。通常的保密方法是对信息进行序列处理，当序列存在少量错误，可能引起整个序列的错误，进而恶化误码性能，链路误码率高的特点严重影响通信的可用性和可靠性。基于密码学的传统防窃听方案无论在网络结构上、算法复杂度还是安全级别上，都难以满足卫星通信安全需求。

[0003] 不同于密钥技术方案，物理层安全技术主要利用信号与信道的物理特性，在信息论角度实现保密通信。物理层安全是以Wyner提出的窃听信道模型为基础，当合法信道质量高于窃听信道的质量时存在安全容量，实现安全传输。因此物理层安全编码的安全性源于信道质量上的差异，实现安全编码的关键就是将信道上的差异转化为合法接收端相对窃听端误码率上的差异，即要求合法接收端译码后的误码率尽可能小，保证传输的可靠性，同时希望窃听端误码率尽可能接近0.5，实现安全性。安全编码技术由于可提供传输可靠性和安全性，能够在卫星通信中得以充分的利用。物理层安全编码以直观易用的误码率作为安全测度，其目的就是尽可能减小安全间隙。从应用的角度来看，物理层安全技术具有易实现、易维护等优点，新型信道编码等的广泛应用为物理层安全技术研究提供了广阔的空间。

[0004] 为实现星地链路通信安全，需要相应的物理层技术配合，保障通信的可靠性，防止第三方窃听。设计一种安全的通信保障方案至关重要。

[0005] 目前已有的物理层安全策略大多用于地面无线通信，比如在建立衰落信道物理层安全传输模型的基础之上，分析不同衰落幅度下私密信息的译码错误概率，最终给出了与信道衰落幅度特征相匹配的私密信息隐藏位置选取规则，并结合私密信息置乱将译码残余比特错误扩散到整个码字中，进一步提高窃听者对私密信息的译码错误概率。类似地，以信道匹配为基础的快衰落信道LDPC保密编码，在瑞利衰落信道下，首先根据主信道的衰落系数对私密信息比特进行交织处理，再将私密信息放在主信道衰落系数绝对值低的位置，实现私密信息位置的隐藏。相比于地面通信，卫星通信信道具有更复杂的通信环境，现有的地面通信物理层安全策略应用在卫星通信中会存在很多问题，包括没有充分考虑通信的物理

信道的互易性、唯一性等特性，链路的长时延、卫星通信信道的复杂成分等，因此无法适用于卫星安全通信。

发明内容

[0006] 针对上述现有技术存在的不足，本发明提供星地链路中结合人工加扰和LDPC安全编码的信息传输方法。

[0007] 本发明的技术方案：

[0008] 星地链路中结合人工加扰和LDPC安全编码的信息传输方法，其中，LDPC为低密度奇偶校验码(LowDensityParityCheckCode，LDPC)，包括如下步骤：

[0009] 步骤1：计算主信道的信道状态向量$\hat{h}$，主信道为星地通信中合法信道；

[0010] 步骤2：对主信道状态向量$\hat{h}$的幅度向量进行循环移位N-1次，将得到的N-1个向量与主信道状态向量$\hat{h}$的幅度向量一起构成N×N维主信道状态信息矩阵q；

[0011] 步骤3：利用主信道状态信息矩阵q对待发送信息进行LDPC编码：

[0012] 步骤3-1：利用主信道状态信息矩阵q生成校验矩阵H'；

[0013] 步骤3-1-1：确定LDPC编码的码率k/n，其中k为待发送信息S的序列长度，n为编码后待发送信号的序列长度；

[0014] 步骤3-1-2：构造μ×n维矩阵H_1，n为μ的ω_r倍，且ω_r大于1，采用LDPC编码方法对H_1赋值；

[0015] 步骤3-1-3：对矩阵H_1进行随机行列变换得到矩阵H_2，H_3，…，H_d，其中d＝n-k/μ；

[0016] 步骤3-1-4：将矩阵H_1到H_d级联得到(n-k)×n维初始校验矩阵H＝$[H_1,H_2,\cdots,H_d]^T$；

[0017] 步骤3-1-5：生成(n-k)×n维估计矩阵D，D中元素均为1；

[0018] 步骤3-1-6：将主信道状态信息矩阵q嵌入D中，得到D'；

[0019] 步骤3-1-7：计算校验矩阵H'：

[0020] H'＝mod(D'•*H)

[0021] 其中，mod为模二运算；

[0022] 步骤3-2：使用渐进边增长(Progressive Edge-Growth，PEG)算法对校验矩阵H'去小环，得到去小环后的校验矩阵H"；

[0023] 步骤3-3：使用去小环后的校验矩阵H"对待发送信息进行编码；

[0024] 步骤4：构建与主信道正交的人工噪声z；

[0025] 步骤5：计算使私密中断概率p_{so}达到最小的待发送信息S'的发送权重w：

[0026] 步骤5-1：设定发射总功率P；

[0027] 步骤5-2：计算人工噪声的协方差矩阵Σ'；

[0028] 步骤5-3：根据不等式约束计算待发送信息的发送权重w，使私密中断概率p_{so}达到最小，即：

[0029] p_{so}＝minp(SNR_E＞γ_E)

[0030] 不等式约束如下：$||w||^2$+Tr(Σ')≤P，SNR_B≥γ_B；其中，SNR_E为窃听端信噪比，SNR_B为合法接收端信噪比，Tr(•)表示求矩阵迹，$||w||^2$是待发送信息的发送功率，γ_E为窃听端误码率最小阈值对应的信噪比，γ_B为合法接收端误码率最大阈值对应的信噪比；

[0031] 步骤6：发送端以功率$||w||^2$连续发送编码后的待发送信息，同时采用多天线发射

的方式发送人工噪声；

[0032] 步骤7：接收端接收发送端发送的信息，并采用BP译码算法对信息进行译码。

[0033] 本发明星地链路中结合人工加扰和LDPC安全编码的信息传输方法，具有如下优点：

[0034] 1、针对卫星通信过程中，由于信道的开放性以及大范围广播导致信息易被窃听的问题，在信息传输过程中加入人工噪声，降低窃听端的信道质量，确保安全容量的存在；将信道状态引入LDPC编码中，实现物理层安全编码，保证通信的安全性和可靠性。

[0035] 2、传统加密方法的密钥分发基于可信第三方，但是卫星通信链路长延时、非持续连通的特性使得节点之间难以建立起信任关系，使密钥分发过程难以实现；采用基于信道状态信息的编码方法，信道状态信息仅通过发送端和合法接收端便能够获得，避免传统加密算法运用在卫星通信过程中存在的问题。

[0036] 3、降低卫星保密通信的复杂度，以及由于复杂度所增加的信息处理时延。由于卫星通信的资源受限，区别于复杂度高的传统加密算法，使用物理层技术解决通信安全问题，从方法上降低计算复杂度，同时由于LDPC的译码复杂度低、能够实现并行译码，降低了收发端硬件设备编译码的复杂度，适合硬件实现。

附图说明

[0037] 图1为本发明一种实施方式的物理层安全间隙示意图；

[0038] 图2为本发明一种实施方式的星地链路中结合人工加扰和LDPC安全编码的信息传输方法流程图；

[0039] 图3为本发明一种实施方式的LDPC安全编码流程图。

具体实施方式

[0040] 下面结合附图对本发明的一种实施方式作详细说明。

[0041] 如图1所示，为误码率(Bit ErrorRatio，BER)随信噪比(Signal-Noise Ratio，SNR)变化的曲线图，当SNR不低于门限$SNR_{B,min}$时，误码率可以以很高的概率被纠正，$P_{e,\min}^{B}$为对应BER的上限值。当SNR不高于门限$SNR_{E,max}$时，相对应的BER在0.5左右，$P_{e,\max}^{E}$为BER的下限值。对于安全编码而言，若合法接收端的SNR大于$SNR_{B,min}$，则编码可以保证合法接收端以低误码率恢复私密信息，以实现可靠传输，则将SNR大于$SNR_{B,min}$区域称为可靠区。若窃听端的SNR小于$SNR_{E,max}$，对应窃听端的误码率在0.5左右，几乎不能窃听到任何私密信息，则将SNR小于$SNR_{E,max}$的区域称为安全区。安全间隙定义为$SNR_{B,min}$与$SNR_{E,max}$的差值，它表示在该安全编码方式下所需要的合法接收端相对于窃听端最小信噪比的优势。安全间隙越小，所要求的合法接收端相对于窃听端的信噪比优势越小。理想状态为安全间隙为0，即当合法通信双方满足可靠通信条件时，窃听信道质量(窃听端的信噪比)只要比合法信道质量(合法接收端信噪比)稍差一点就无法还原发送信息。

[0042] 根据安全间隙的理论，实现安全编码的方法主要分为两方面：(1)误码率维度上，降低高信噪比区域内的误码率，同时提高低信噪比区域内的误码率；(2)信噪比维度上，降低窃听信道信噪比，使窃听端处于安全区，同时提高合法信道信噪比，使合法用户处于可靠

区。

[0043] 本实施方式中采用LDPC编码技术与人工加扰技术相结合的方法:在误码率维度上利用LDPC编码,保证合法通信双方的可靠传输,同时在在编码信号中加入信道状态信息,窃听端由于未知合法信道的信道状态信息,会出现高误码率;在信噪比维度上是采用人工加扰的方法,降低窃听端的信噪比,使得窃听端处于安全区,也进一步保证窃听端误码率的要求,最终实现物理层安全传输。

[0044] 具体的,如图2所示,星地链路中结合人工加扰和LDPC安全编码的信息传输方法,包括如下步骤:

[0045] 步骤1:计算主信道的信道状态向量$\hat{h}$,主信道为星地通信中合法信道;本实施方式采用如下方法计算主信道状态向量:

[0046] 步骤1-1:生成训练序列X,本实施方式中,X为伪随机序列(Pseudo-Noise Code,PN);

[0047] 步骤1-2:将训练序列X通过主信道发送给接收端,由于主信道状态和噪声的影响,接收端接收到序列Y;

[0048] 步骤1-3:计算主信道状态向量$\hat{h}$,具体方法为:

[0049] 步骤1-3-1:使用最小二乘(Least Squares,LS)准则进行信道估计,得到信道最小二乘估计值:

[0050] $$\widehat{H}_{LS} = X_P^{-1} Y \qquad (1)$$

[0051] 其中,X_p为训练矩阵,训练矩阵中每列为通过主信道中各个子信道发送的训练序列;

[0052] 步骤1-3-2:使用线性最小均方差误差(Linear Minimum Mean Square Error,LMMSE)准则进行信道估计,得到信道线性最小均方误差估计值:

[0053] $$\widehat{H}_{LMMSE} = R_{HH}(R_{HH} + \delta_n^2 (X^T X)^{-1})^{-1} \widehat{H}_{LS} \qquad (2)$$

[0054] 其中,信道状态向量的自相关矩阵$R_{HH}=h_p h_p^H$,h_p^H为h_p的共轭转置,$h_p=F^{-1}(X^{-1}Y)$,F^{-1}为傅里叶反变换,δ_n^2为主信道方差;

[0055] 步骤1-3-3:主信道状态向量$\hat{h}$为:

[0056] $$\hat{h} = F^{-1} \widehat{H}_{LMMSE} \qquad (3)$$

[0057] 本实施方式中得到的$\hat{h}=\left[1.2e^{j0.6} \quad 0.8e^{j2.4} \quad 1.0e^{j1.7} \quad 0.5e^{j0.7} \quad 2.1e^{j4.1} \quad 1.7e^{j2.5} \quad 0.2e^{j0.9} \quad 0.7e^{j2.8}\right]$;

[0058] 步骤2:对主信道状态向量$\hat{h}$的幅度向量进行循环移位N-1次,将得到的N-1个向量与主信道状态向量$\hat{h}$的幅度向量一起构成N×N维主信道状态信息矩阵q;

[0059] 本实施方式中，信道状态信息矩阵 $\boldsymbol{q}=\begin{bmatrix}1.2 & 0.8 & 1.0 & 0.5 & 2.1 & 1.7 & 0.2 & 0.7\\ 0.7 & 1.2 & 0.8 & 1.0 & 0.5 & 2.1 & 1.7 & 0.2\\ 0.2 & 0.7 & 1.2 & 0.8 & 1.0 & 0.5 & 2.1 & 1.7\\ 1.7 & 0.2 & 0.7 & 1.2 & 0.8 & 1.0 & 0.5 & 2.1\\ 2.1 & 1.7 & 0.2 & 0.7 & 1.2 & 0.8 & 1.0 & 0.5\\ 0.5 & 2.1 & 1.7 & 0.2 & 0.7 & 1.2 & 0.8 & 1.0\\ 1.0 & 0.5 & 2.1 & 1.7 & 0.2 & 0.7 & 1.2 & 0.8\\ 0.8 & 1.0 & 0.5 & 2.1 & 1.7 & 0.2 & 0.7 & 1.2\end{bmatrix}$

[0060] 将所有小数进行向下取整，得到：

[0061] $\boldsymbol{q}=\begin{bmatrix}1 & 0 & 1 & 0 & 2 & 1 & 0 & 0\\ 0 & 1 & 0 & 1 & 0 & 2 & 1 & 0\\ 0 & 0 & 1 & 0 & 1 & 0 & 2 & 1\\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 2\\ 2 & 1 & 0 & 0 & 1 & 0 & 1 & 0\\ 0 & 2 & 1 & 0 & 0 & 1 & 0 & 1\\ 1 & 0 & 2 & 1 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 2 & 1 & 0 & 0 & 1\end{bmatrix}$

[0062] 步骤3：如图3所示，利用信道状态信息矩阵q对待发送信息进行LDPC编码：

[0063] 步骤3-1：利用信道状态信息矩阵q生成校验矩阵H'；

[0064] 步骤3-1-1：确定LDPC编码的码率k/n，其中k为待发送信息S的序列长度，n为编码后待发送信号的序列长度；本实施方式中，k＝5，n＝20，码率＝5/20＝0.25；

[0065] 步骤3-1-2：构造μ×n维矩阵H_1，n为μ的ω_r倍，且ω_r大于1，矩阵H_1的第i行中1列到iω_r列的值为1，其余元素的值为0，1采用如下公式生成：

[0066] $1=(i-1)\,\omega_r+1 \quad (4)$

[0067] 本实施方式中，构造5*20矩阵H_1：

[0068] $H_1=\begin{bmatrix}1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1\end{bmatrix}$

[0069] 步骤3-1-3：对矩阵H_1进行随机行列变换得到矩阵H_2，H_3，…，H_d，其中d＝n-k/μ；

[0070] $H_2=\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}$；

[0071] $H_3=\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1\end{bmatrix}$；

[0072] 步骤3-1-4:将矩阵H_1到H_d级联得到(n-k)×n维初始校验矩阵$H=[H_1,H_2,\cdots,H_d]^T$;

[0073] 步骤3-1-5:生成(n-k)×n维估计矩阵D,D中元素均为1;

[0074] 步骤3-1-6:将信道状态信息矩阵q嵌入D中,得到D',具体的:

[0075] (1)当q的维数N为偶数,将D中第$\lfloor (n-k)/2 \rfloor - \lfloor N/2 \rfloor +1$行到第$\lfloor (n-k)/2 \rfloor + \lfloor N/2 \rfloor$行,第$\lfloor n/2 \rfloor - \lfloor N/2 \rfloor +1$列到第$\lfloor n/2 \rfloor + \lfloor N/2 \rfloor$列之间的元素替换为q;

[0076] (2)当q的维数N为奇数,将D中第$\lfloor (n-k)/2 \rfloor - \lfloor N/2 \rfloor +1$行到第$\lfloor (n-k)/2 \rfloor + \lfloor N/2 \rfloor +1$行,第$\lfloor n/2 \rfloor - \lfloor N/2 \rfloor +1$列到第$\lfloor n/2 \rfloor + \lfloor N/2 \rfloor +1$列之间的元素替换为q;

[0077] 本实施例中,嵌入信道状态信息矩阵q后的估计矩阵D'为:

[0078] $$\boldsymbol{D}'=\begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&0&1&0&2&1&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&1&0&1&0&2&1&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&1&0&1&0&2&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&0&0&1&0&1&0&2&1&1&1&1&1&1\\
1&1&1&1&1&1&2&1&0&0&1&0&1&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&2&1&0&0&1&0&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&0&2&1&0&0&1&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&1&0&2&1&0&0&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{bmatrix}$$

[0079] 步骤3-1-7:计算包含信道状态信息的校验矩阵H',计算公式为:

[0080] $H'=\mathrm{mod}(D'*H)$ (5)

[0081] 其中,mod为模二运算。

[0082] 步骤3-2:采用PEG算法消除围长为4和6的环,得到去小环后的校验矩阵H";

[0083] 步骤3-3:使用校验矩阵对待发送信息进行编码;

[0084] 步骤3-3-1:将校验矩阵H"进行行变换,得到H"=[Q|I]的形式,其中I为n-k阶单位矩阵,Q为(n-k)×k维矩阵;

[0085] 步骤3-3-2:对Q进行转置得到Q^T,并使用Q^T构建k×n维生成矩阵$G=[I'|Q^T]$,其中,I'为k阶单位矩阵:

[0086] $$\boldsymbol{G}=\begin{bmatrix}
1&0&0&0&0&1&0&0&1&1&0&0&1&0&0&0&1&1&0&1\\
0&1&0&0&0&0&1&0&0&1&0&1&1&1&0&0&0&0&0&1\\
0&0&1&0&0&1&1&1&0&1&1&0&1&1&0&0&0&0&0&1\\
0&0&0&1&0&0&0&1&0&0&1&1&0&0&1&1&0&0&0&1\\
0&0&0&0&1&1&0&0&1&0&1&0&1&1&1&1&0&1&1&0
\end{bmatrix}$$

[0087] 步骤3-3-3:将待发送信息与生成矩阵G相乘,得到编码后的待发送信息S';

[0088] 本实施方式中,待发送信息为S=[0 1 1 1 0];

[0089] $$S'=S\times G=[0\ \ 1\ \ 1\ \ 1\ \ 0]\begin{bmatrix}1&0&0&0&0&1&0&0&1&1&0&0&1&0&0&0&1&1&0&1\\0&1&0&0&0&0&1&0&0&1&0&1&1&1&0&0&0&0&0&1\\0&0&1&0&0&1&1&1&0&1&1&0&1&1&0&0&0&0&0&1\\0&0&0&1&0&0&0&1&0&0&1&1&0&0&1&1&0&0&0&1\\0&0&0&0&1&1&0&0&1&0&1&0&1&1&1&1&0&1&1&0\end{bmatrix}$$

$$=[0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1]$$

[0090] 步骤4:构建与主信道正交的人工噪声z,即$\hat{h}^H\cdot z=0$;

[0091] 步骤5:计算使私密中断概率p_{so}达到最小的待发送信息S'的发送权重w;

[0092] 步骤5-1:设定发射总功率P;

[0093] 步骤5-2:计算人工噪声的协方差矩阵Σ';

[0094] 步骤5-3:根据不等式约束计算待发送信息的发送权重w,使私密中断概率p_{so}达到最小,即:

[0095] $p_{so}=\min p(SNR_E>\gamma_E)$ (6)

[0096] 不等式约束如下:$||w||^2+Tr(\Sigma')\leq P$,$SNR_B\geq\gamma_B$,其中,$SNR_E$为窃听端信噪比,$SNR_B$为合法接收端信噪比,Tr(•)表示求矩阵迹,$||w||^2$是待发送信息的发送功率,$\gamma_E$为窃听端误码率最小阈值对应的信噪比,$\gamma_B$为合法接收端误码率最大阈值对应的信噪比。

[0097] 其中,合法接收端噪比为:

[0098] $$SNR_B(w,\sum')=E[|h^HwS'|^2]/E[|h^Hz|^2+\delta_b^2]=w^TR_hw/(Tr(\sum'R_h)+\delta_b^2) \quad (7)$$

[0099] 其中:Tr(•)表示求矩阵迹;w是待发送信息S'的发送权重;δ_b^2为主信道高斯白噪声n_b的方差;$R_h=hh^H$,h为主信道的理想信道状态向量,因为$\hat{h}$存在估计误差Δh,即$\hat{h}=h+\Delta h$,假设h和Δh相互独立,Δh中元素相互独立且服从均值为零,方差为δ_{Δ,N_i}的正态分布,其中$1\leq i\leq N_A$,N_A为发送端天线的个数,则合法接收端信噪比可写为:

[0100] $$SNR_B(w,\sum')=\frac{w^TR_hw}{Tr(\sum'R_h)+Tr(Diag(\delta_{\Delta,1},\cdots,\delta_{\Delta,j},\cdots,\delta_{\Delta,N_A})R_h)+\delta_b^2} \quad (8)$$

[0101] 其中:Diag(•)表示除对角线元素外其他元素均为0;

[0102] 窃听端信噪比为:

[0103] $$SNR_E(w,\sum')=E[|g^HwS'|^2]/E[|g^Hz|^2+\delta_e^2]=w^TR_sw/(Tr(\sum'R_g)+\delta_e^2) \quad (9)$$

[0104] $R_s=S'S'^T$,$R_g=gg^H$,g为窃听信道的信道状态向量,该情况下认为发送端能够获知窃听端瞬时信道,如果仅能够获取窃听端信道的相关矩阵,则$R_g=E\{gg^H\}=\overline{g}\overline{g}^H+C_g$,其中$\overline{g}$和$C_g$分别为g的平均值和协方差;$\delta_e^2$为窃听信道高斯白噪声$n_e$的方差;

[0105] 步骤6:发送端以功率$||w||^2$连续发射编码后的待发送信息,同时采用多天线发射的方式发送人工噪声;

[0106] 主信道和窃听端的信道模型为:

[0107] $Y_b=h^HwS'+h^Hz+n_b=h^HwS'+n_b$

[0108] $Y_e=g^HwS'+g^Hz+n_e$

[0109] 其中,Y_b和Y_e分别为主信道和窃听信道接收到的信号;

[0110] 步骤7:接收端接收发送端发送的信息,并采用BP译码算法对信息进行译码。

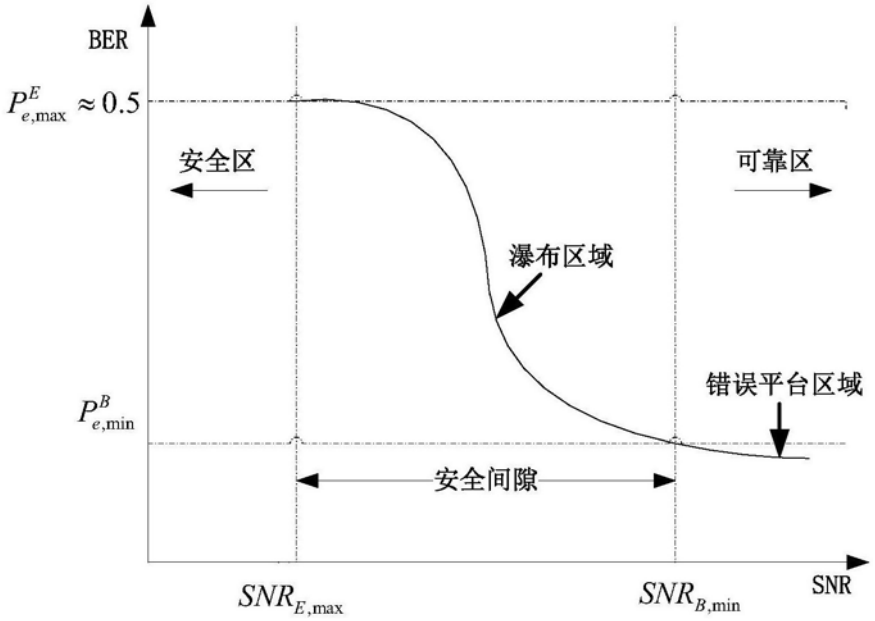

BER
$P^{E}_{e,\max} \approx 0.5$
安全区
可靠区
瀑布区域
错误平台区域
$P^{B}_{e,\min}$
安全间隙
$SNR_{E,\max}$
$SNR_{B,\min}$
SNR

图1

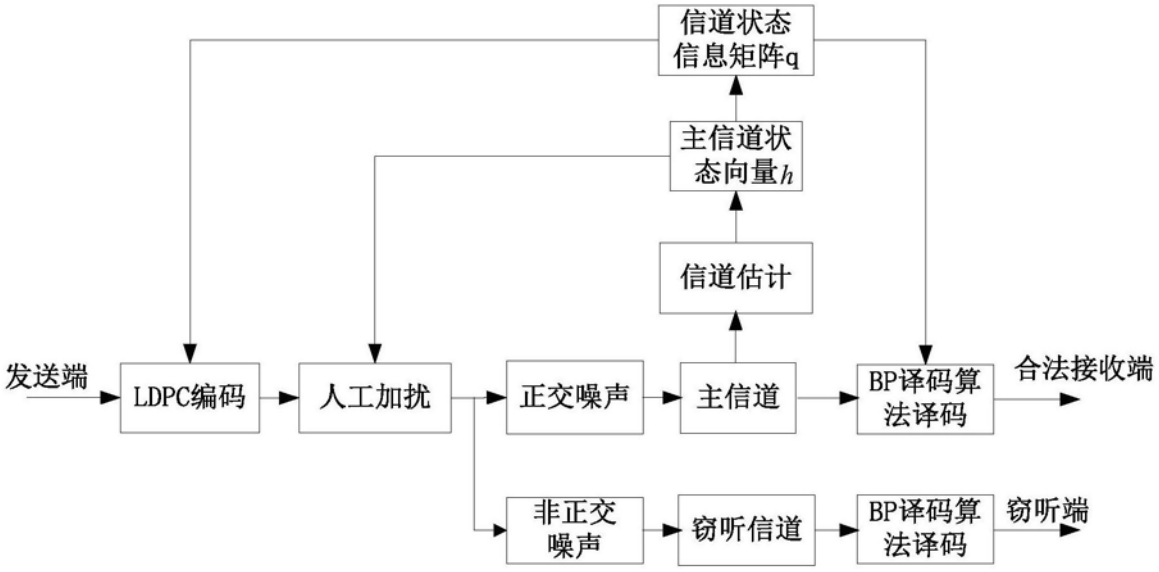

信道状态信息矩阵q
主信道状态向量h
信道估计
发送端
LDPC编码
人工加扰
正交噪声
主信道
BP译码算法译码
合法接收端
非正交噪声
窃听信道
BP译码算法译码
窃听端

图2

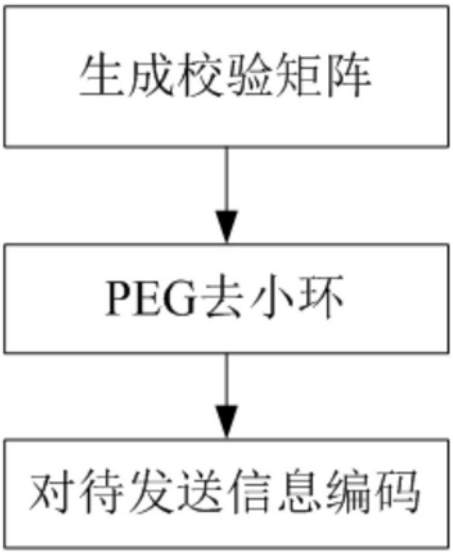


图3