基于混合信号的放大转发中继系统的物理层安全传输

杨 斌,王文杰,殷勤业
(西安交通大学电子与信息工程学院,陕西西安 710049)

摘 要: 中继系统可以增强物理层安全算法的系统性能,这种系统一般包含两阶段的通信过程:从信源到中继节点,在从中继节点到目的节点.通常来说,第一阶段的信息传输缺乏保护,如果窃听者距离信源节点比较近的话,系统性能就无法保证了.该文提出了一种基于混合信号的三阶段的传输方法确保整个传输过程中的保密性能,这样,当窃听者接近信源节点的时候,仍可以保证系统的安全性能.这种方法的优化解是一个复杂的非凸优化问题,该文中建议了一种低复杂度的次优解来解决其中的优化问题.理论分析以及方针结果证明,该方法可以有效确保系统的全过程的安全性能.

关键词: 无线通信; 物理层安全; 中继通信
中图分类号: TN929.5 **文献标识码:** A **文章编号:** 0372-2112 (2016)02-0268-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.02.004

Secure Wireless Communication for AF Relay System with Hybrid Signals

YANG Bin, WANG Wen-jie, YIN Qin-ye
(*School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi* 710049, *China*)

Abstract: Relay system can improve the secrecy of a wireless communication with physical layer security algorithms. Most of these algorithms include two stages: during the first stage, the source node sends coded messages to the relays, and during the second stage, the relays forward the received messages to the destination node. Usually, there is no protection during the first stage, thus most of the secrecy analysis is based on the assumption that there is no direct channel between the source and the eavesdropper. In a practical system, when the eavesdropper is located near the source, the secrecy rate of all these algorithms is down to zero. In this paper, a novel three-stage algorithm with hybrid signals is proposed, which can offer full protection on a relay system. The algorithm results in a non-convex optimal problem, and a sub-optimal solution with low computational complexity is proposed. The theoretical analysis and simulation results show that the proposed scheme can achieve much better secrecy performance than traditional algorithms when the eavesdropper is near the source node.

Key words: wireless communication; physical layer security; relay network

1 引言

由于无线通信介质的开放性,安全性一直是无线通信系统需要解决的难题.近年来,随着无线通信技术的发展,物理层安全技术逐渐引起了更多的重视[1~25].这个领域早期的工作[1~3]中证明,当窃听者信道质量比主信道差的时候,通过一定的编码方式,可以保密传输信息.为了造成主信道和窃听信道的差异,通常考虑的方法是人工干扰[4]或多天线[5].在通讯双方没有配备多天线的时候,额外的系统节点或者中继节点是可以帮助系统获得更好的安全性能的[6~25].这些协助节点可以帮助合法用户形成分布式波束,增强接收端的信号,以达到提高系统保密容量的目的[7~15];额外的节点还可以产生干扰信号,影响窃听者的性能,进而增强系统的保密性能[19~24];或者还可以将两种方式结合起来[16~18].在中继系统中,保密通讯的方式通常有三种:放大转发(AF)模式,解码转发(DF)模式,以及协作干扰(CJ)模式.不论是何种模式,中继通讯通常都包含两个阶段:在第一阶段发送端将信息发送给中继节点,第二阶段中继节点再将信号发送给目的节点.第一阶段由于只有一个发信节点,各个中继节点都需要接收信

收稿日期:2014-07-07;修回日期:2014-12-20;责任编辑:马兰英
基金项目:国家自然科学基金(No.61172092)

号,很难对于这个阶段进行保密.

有很多研究已经考虑对于中继通信的全过程进行保护. 文献[16,17]考虑引入多天线的节点对于第一阶段进行协作干扰保护;目的节点也是可以作为干扰源的,在收到信号的时候,目的节点是可以减去自己前面发出的干扰的,这也就对第一阶段传输产生的保护作用[13];如果源节点和目的节点都配备有多天线的话,第一阶段的保护可以通过波束形成的方式来完成[14];在更复杂的模型中,以上两种方式是可以结合起来的[18];如果节点间可以提前共享干扰信号,不让窃听者知晓,第一阶段的保护就比较容易了[23]. 以上这些方法,都不大适合于各个节点都是单天线的系统.

本文提出了一种新的协作干扰方法,对于中继通信的所有阶段提供完整的保护. 该方法不论窃听者位于系统的任何位置,都可以让系统获得有效的安全性能,而且不附带任何前提假设. 该方法的通信过程分为三个阶段:第一阶段,由各个中继节点以互相独立的方式向信源节点发送干扰信号;第二阶段,信源节点将自己要发送的信息和接收到的干扰信号相加混合起来发给中继节点;第三阶段,中继节点将接收到的信号加上各自第一阶段发出的干扰信号发给接收节点,合理设计发送调整系数,可以在接收节点处将全部干扰信号消除掉,只保留有用信号. 对于窃听者来说,第一阶段收到的干扰信号,由于信道的不同,各个中继的独立信号经过信道传输后在窃听者处叠加产生的随机信号,是和在发送者处产生的随机信号不同的,所以,窃听者无法知道发送者到底收到了什么样的干扰信号. 这样,在第二阶段,窃听者得到发送者的混合信号后,也就无法将信号与干扰有效分离. 至于第三阶段,中继节点实际上将干扰信号的零空间对准了接收者,而窃听者则不在这个零空间内,同样会受到干扰. 如此,这三个阶段的通信过程都受到了人工干扰的保护,也就能确保系统的整体性能了.

本文的方法和以往的工作的不同点在于:之前的相关研究工作,参与协作的节点都要发送相关的信号,这些信号必须有一个安全的通道进行传输,这在实际中很难做到. 本文的方法,协作节点没有信息的交互,各自发送独立的干扰信号,彼此只需要在时间上保持同步,确保干扰信号在目的节点上的叠加. 本文的方法主要是受文献[25]中方法的启发,但是文献[25]中的协作节点不作为中继使用,而本文模型中,源节点和目的节点间没有直接的通信信道,两者的模型不同. 本文建议的方法,在中继总功率限制条件下,会导致一个非凸的优化问题. 文中提出了一种低运算复杂度的次优算法获得中继节点间的优化功率分配方案.

本文公式用粗体小写字母代表向量,粗体大写字母代表矩阵,$\boldsymbol{x}^{\mathrm{H}}$ 代表 $\boldsymbol{x}$ 的共轭转置,°代表哈达玛乘积.

2　系统模型

系统模型如图1所示,在合法用户 A 和 B 之间没有直接的信道通路,A 希望能通过中继节点 $R_i, i=1\cdots N$ 来传递保密信息给 B. 系统中存在一个窃听者,他可以监听系统中所有节点发出的信号. 系统中所有的节点都只配备一根天线.

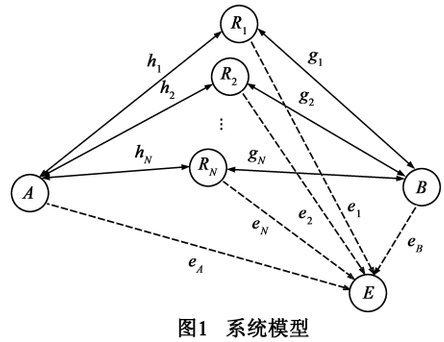

图1　系统模型

建议算法分为三个阶段. 在第一阶段,N 个中继节点同步向用户 A 发送独立的随机信号,用户 A 收到的信号就是

$$v_A = \boldsymbol{h}^{\mathrm{T}}\boldsymbol{v}_R + n_A \tag{1}$$

其中 n_A 是第一阶段系统接收机噪声,$\boldsymbol{h} \triangleq [h_1, h_2, \cdots, h_N]^{\mathrm{T}}$ 是复信道增益向量,$\boldsymbol{v}_R \triangleq [v_1, v_2, \cdots, v_N]^{\mathrm{T}}$ 是中继发出的随机符号向量,服从复高斯分布. 所有中继节点发出的总功率就是

$$P_{R1} = \sum_{i=1}^{N} \sigma_i^2, \text{where } \sigma_i^2 = E(|v_i|^2), i = 1\cdots N \tag{2}$$

第二阶段,用户 A 把上阶段收到的干扰信号和自身需要发送的信号加起来发出. 发送的信号是

$$x_A = \sqrt{\alpha}s + \sqrt{\beta}v_A \tag{3}$$

这里 α 和 β 是功率分配因子,s 是待发送的有用信号,服从单位方差复高斯分布. 这一阶段,各个中继节点收到的信号就是

$$\boldsymbol{y}_R = \boldsymbol{h}x_A + \boldsymbol{n}_R \tag{4}$$

其中 $\boldsymbol{n}_R \triangleq [n_1, n_2, \cdots, n_N]^{\mathrm{T}}$ 和 $\boldsymbol{y}_R \triangleq [y_1, y_2, \cdots, y_N]^{\mathrm{T}}$ 分别是中继节点的接收噪声和收到的信号. 这一阶段用户 A 的发射功率是

$$P_A = \alpha + \beta|v_A|^2 \tag{5}$$

第三阶段,中继节点应用 AF 方式将各自收到的信号转发出去. 同时各个中继节点也重复第一阶段各自发送的干扰信号,用以在用户 B 处形成干扰零陷. 中继节点的发送信号是

$$\boldsymbol{x}_R = \boldsymbol{\lambda} \circ \boldsymbol{y}_R + \boldsymbol{w} \circ \boldsymbol{v}_R \tag{6}$$

其中 $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \cdots, \lambda_N]^{\mathrm{T}}$ 是波束形成系数,$\boldsymbol{w} = [w_1, w_2, \cdots, w_N]^{\mathrm{T}}$ 是干扰消除系数.

在接收端,用户 B 收到的信号就是

$$\begin{aligned} y &= \boldsymbol{g}^{\mathrm{T}}\boldsymbol{x}_R + n_B \\ &= \sqrt{\alpha}ts + \sqrt{\beta}t(\boldsymbol{h}^{\mathrm{T}}\boldsymbol{v}_R) + \boldsymbol{g}^{\mathrm{T}}(\boldsymbol{w}\circ\boldsymbol{v}_R) \\ &+ \sqrt{\beta}tn_A + \boldsymbol{g}^{\mathrm{T}}(\lambda\circ\boldsymbol{n}_R) + n_B \end{aligned} \tag{7}$$

其中

$$t \triangleq \boldsymbol{g}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{h}) \tag{8}$$

$\boldsymbol{w}$ 用来消除接收端的干扰,那么就有

$$\sqrt{\beta}t(\boldsymbol{h}^{\mathrm{T}}\boldsymbol{v}_R) + \boldsymbol{g}^{\mathrm{T}}(\boldsymbol{w}\circ\boldsymbol{v}_R) = 0 \tag{9}$$

解方程可以得到

$$w_i = -\sqrt{\beta}t\frac{h_i}{g_i}, i = 1,2,\cdots,N \tag{10}$$

这样用户 B 的接收信号就是

$$y = \sqrt{\alpha}ts + \sqrt{\beta}tn_A + \boldsymbol{g}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{n}_R) + n_B \tag{11}$$

此时,中继节点总发射功率就是

$$\sum_{i=1}^{N} E(|x_i|^2) = \boldsymbol{\lambda}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{\lambda} \tag{12}$$

其中

$$\begin{aligned} A \triangleq \operatorname{diag}\{&\alpha|h_i|^2 + (\beta|h_i|^2+1)\sigma_n^2 + \beta|h_i|^2\Big(\sum_{j=1}^{N}|h_j|^2 p_j\Big)\} \\ &+ \beta\Big(\sum_{i=1}^{N}\frac{|h_i|^2}{|g_i|^2}p_i\Big)\operatorname{mtx}\{g_i h_i g_j^* h_j^*\} - \beta\operatorname{mtx}\Big\{g_i h_i g_j^* h_j^*\frac{|h_j|^2}{|g_j|^2}p_j\Big\} \\ &- \beta\operatorname{mtx}\Big\{g_i^* h_i^* g_j h_j\frac{|h_j|^2}{|g_j|^2}p_j\Big\} \end{aligned} \tag{13}$$

其中 $\operatorname{diag}\{x_i\}$ 是以 x_i 为对角元素的对角矩阵,$\operatorname{mtx}\{x_{ij}\}$ 是以 x_{ij} 为元素的矩阵.

窃听者各个阶段接收到的信号是

$$y_{E1} = \boldsymbol{e}^{\mathrm{T}}\boldsymbol{v}_R + n_{E1} \tag{14}$$

$$\begin{aligned} y_{E2} &= e_A x_A + n_{E2} \\ &= \sqrt{\alpha}e_A s + \sqrt{\beta}e_A\boldsymbol{h}^{\mathrm{T}}\boldsymbol{v}_R + \sqrt{\beta}e_A n_A + n_{E2} \end{aligned} \tag{15}$$

$$\begin{aligned} y_{E3} &= \sqrt{\alpha}t_e s + \sqrt{\beta}t_e(\boldsymbol{h}^{\mathrm{T}}\boldsymbol{v}_R) + \boldsymbol{e}^{\mathrm{T}}(\boldsymbol{w}\circ\boldsymbol{v}_R) \\ &+ \sqrt{\beta}t_e n_A + \boldsymbol{e}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{n}_R) + n_{E3} \end{aligned} \tag{16}$$

其中 $\boldsymbol{e} \triangleq [e_1, e_2, \cdots, e_N]^{\mathrm{T}}$ 是窃听者和中继节点之间的信道向量,

$$t_e \triangleq \boldsymbol{e}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{h}) \tag{17}$$

e_A 和 e_B 分别代表窃听者到用户 A、B 之间的信道增益,n_{E1}、n_{E2} 和 n_{E3} 分别是各个阶段窃听者的接收噪声.

在本文中,所有的噪声信号都服从方差为 σ_n^2 的复高斯分布.

3 保密性能分析

对于高斯信道来说,系统的保密速率是合法用户的互信息和窃听者互信息的差. 本文所述系统的合法用户的互信息是

$$I(y;s) = \frac{1}{3}\log\left(1 + \frac{\alpha|t|^2}{(\beta|t|^2 + \mathbf{1}^{\mathrm{T}}|\boldsymbol{\lambda}\circ\boldsymbol{g}|^2 + 1)\sigma_n^2}\right) \tag{18}$$

其中 $\mathbf{1} \triangleq [1,1,\cdots,1]^{\mathrm{T}}$.

对于窃听者来说,系统可以等效看做是一个单入多出(SIMO)的系统,其接收信号就可以重新表达为

$$\boldsymbol{y}_E = \sqrt{\alpha}\boldsymbol{h}_E s + \boldsymbol{i}_E{}^{\mathrm{T}}\boldsymbol{v}_R + \boldsymbol{n}_E \tag{19}$$

其中

$$\boldsymbol{y}_E = [y_{E1}, y_{E2}, y_{E3}]^{\mathrm{T}} \tag{20}$$

$$\boldsymbol{h}_E = [0, e_A, t_e]^{\mathrm{T}} \tag{21}$$

$$\boldsymbol{i}_E = [e, \sqrt{\beta}e_A h, \sqrt{\beta}t_e\boldsymbol{h} + \boldsymbol{w}\circ\boldsymbol{e}]^{\mathrm{T}} \tag{22}$$

$$\boldsymbol{n}_E = [n_{E1}, \sqrt{\beta}e_A n_A + n_{E2}, \sqrt{\beta}t_e n_A + \boldsymbol{e}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{n}_R) + n_{E3}]^{\mathrm{T}} \tag{23}$$

其中干扰部分并不互相独立,本文通过对接收信号的干扰"白化"来计算其互信息. 定义干扰和噪声的互相关矩阵为

$$\boldsymbol{Q} = E((\boldsymbol{i}_E{}^{\mathrm{T}}\boldsymbol{v}_R + \boldsymbol{n}_E)(\boldsymbol{v}_R{}^{H}\boldsymbol{i}_E{}^{*} + \boldsymbol{n}_E{}^{H})) \tag{24}$$

其中 $E(x)$ 代表随机变量 x 的数学期望. 将式(19)两边乘以 $Q^{-1/2}$,这样

$$\boldsymbol{y}'_E = \boldsymbol{Q}^{-1/2}\boldsymbol{y}_E = \boldsymbol{Q}^{-1/2}\sqrt{\alpha}\boldsymbol{h}_E s + \boldsymbol{n}'_E \tag{25}$$

可以看出,$\boldsymbol{n}'_E = \boldsymbol{Q}^{-1/2}(\boldsymbol{i}_E{}^{\mathrm{T}}\boldsymbol{v}_R + \boldsymbol{n}_E)$ 是空间上的"白噪声". 这样窃听者的互信息就是

$$\begin{aligned} I(\boldsymbol{y}_E;s) &= \frac{1}{3}\log|\boldsymbol{I} + \alpha\boldsymbol{Q}^{-1/2}\boldsymbol{h}_E\boldsymbol{h}_E{}^{\mathrm{H}}(\boldsymbol{Q}^{-1/2})^{\mathrm{H}}| \\ &= \frac{1}{3}(\log|\alpha\boldsymbol{h}_E\boldsymbol{h}_E{}^{\mathrm{H}} + \boldsymbol{Q}| - \log|\boldsymbol{Q}|) \end{aligned} \tag{26}$$

这样系统的保密速率就是

$$R_s = [I(y;s) - I(\boldsymbol{y}_E;s)]^{+} \tag{27}$$

其中 $[x]^{+} = \max(0,x)$.

如果我们限制中继节点的总功率,以及源节点的发射功率的话,问题就是,在这样的功率限制下,如何调节 α、β、$\boldsymbol{p}$ 和 $\boldsymbol{\lambda}$ 使得保密速率 R_s 最大:

$$\begin{aligned} \max_{\alpha,\beta,p,\lambda}\quad & R_s \\ \text{s.t.}\quad & \boldsymbol{p}^{\mathrm{T}}1 = P_0 \\ & \boldsymbol{\lambda}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{\lambda} = P_0 \\ & \alpha + \beta|v_A|^2 = P_A \end{aligned} \tag{28}$$

考虑到 R_s 的数学表达形式,我们可以看出 R_s 并非一个凸函数,也就无法用比较简洁的方式求得最优解. 在这种情况下,我们可以对于该优化问题增加部分约束,或者简化一些形式,来取得一个次优解. 通常来说,这种次优解也是可以接受的.

4 总功率约束下的次优解

我们引入的第一个条件是零空间条件. 在第三阶段,我们可以设定将信号的零空间对准窃听者.

$$t_e = \boldsymbol{e}^{\mathrm{T}}(\boldsymbol{\lambda}\circ\boldsymbol{h}) = 0 \tag{29}$$

这样就可以确保窃听者在第三阶段无法收到任何有用信息.

引入的第二个附加条件是高功率假设. 在建议方案中,合法用户和窃听者之间的差异主要由各个中继节点发出的干扰信号造成,由于合法用户和窃听者收到的人工干扰信号不同,窃听者就无法完全去除人工干扰信号. 当各中继节点发射的总发射功率足够高的时候,对于窃听者来说,起主要作用的是干扰而不是噪声,可以忽略接收噪声的影响.

引入了零空间和高功率两个附加条件后,窃听者的接收信号就可以重新表达为

$$\boldsymbol{y}_E=\sqrt{\alpha}\boldsymbol{h}_E s+\boldsymbol{i}_E{}^{\mathrm{T}}\boldsymbol{v}_R \tag{30}$$

其中

$$\boldsymbol{y}_E=[y_{E1},y_{E2},y_{E3}]^{\mathrm{T}} \tag{31}$$

$$\boldsymbol{h}_E=[0,e_A,0]^{\mathrm{T}} \tag{32}$$

$$\boldsymbol{i}_E=[\boldsymbol{e},\sqrt{\beta}e_A\boldsymbol{h},\boldsymbol{w}\circ\boldsymbol{e}]^{\mathrm{T}} \tag{33}$$

窃听者的互信息就是

$$\begin{aligned}I(\boldsymbol{y}_E;s)&=\frac{1}{3}(\log|\alpha\boldsymbol{h}_E\boldsymbol{h}_E{}^{\mathrm{H}}+\boldsymbol{Q}|-\log|\boldsymbol{Q}|)\\&=\frac{1}{3}\log\left(1+\frac{\alpha|e_A|^2|\boldsymbol{Q}_2|}{|\boldsymbol{Q}|^2}\right)\end{aligned} \tag{34}$$

其中

$$\begin{aligned}\boldsymbol{Q}&=E(\boldsymbol{i}_E{}^{\mathrm{T}}\boldsymbol{v}_R\boldsymbol{v}_R{}^{\mathrm{H}}\boldsymbol{i}_E{}^{*}))\\&=\begin{bmatrix}q_{11}&q_{12}&q_{13}\\q_{21}&q_{22}&q_{23}\\q_{31}&q_{32}&q_{33}\end{bmatrix}\end{aligned} \tag{35}$$

$\boldsymbol{Q}$ 的各个元素是

$$q_{11}=\boldsymbol{p}^{\mathrm{T}}|\boldsymbol{e}|^2 \tag{36}$$

$$q_{22}=\beta|e_A|^2\boldsymbol{p}^{\mathrm{T}}|\boldsymbol{h}|^2 \tag{37}$$

$$q_{33}=\beta|t|^2\boldsymbol{p}^{\mathrm{T}}|\boldsymbol{Be}|^2 \tag{38}$$

$$q_{12}=q_{21}^{*}=\sqrt{\beta}e_A^{*}\boldsymbol{p}^{\mathrm{T}}(\boldsymbol{e}\circ\boldsymbol{h}^{*}) \tag{40}$$

$$q_{13}=q_{31}^{*}=-\sqrt{\beta}t\boldsymbol{p}^{\mathrm{T}}(\boldsymbol{e}\circ(\boldsymbol{Be})^{*}) \tag{41}$$

$$q_{23}=q_{32}^{*}=-\beta t^{*}e_A\boldsymbol{p}^{\mathrm{T}}(\boldsymbol{h}\circ(\boldsymbol{Be})^{*}) \tag{41}$$

其中,我们定义

$$\boldsymbol{B}\triangleq\mathrm{diag}\left\{\frac{h_i}{g_i}\right\} \tag{42}$$

$$\boldsymbol{Q}_2=\begin{bmatrix}q_{11}&q_{13}\\q_{31}&q_{33}\end{bmatrix} \tag{43}$$

于是,经过推导,可以得到

$$|\boldsymbol{Q}|=\beta^2|e_A|^2|t|^2\sum_{i>j>k}\alpha_{ijk}P_iP_jP_k \tag{44}$$

$$|\boldsymbol{Q}_2|=\beta|t|^2\sum_{i>j}\mu_{ij}P_iP_j \tag{45}$$

其中

$$\alpha_{ijk}=\left|e_jh_ih_k\left(\frac{e_i}{g_i}-\frac{e_k}{g_k}\right)-e_ih_jh_k\left(\frac{e_j}{g_j}-\frac{e_k}{g_k}\right)-e_kh_ih_j\left(\frac{e_i}{g_i}-\frac{e_j}{g_j}\right)\right|^2 \tag{46}$$

$$\mu_{ij}=|e_ie_j|^2\left|\frac{h_i}{g_i}-\frac{h_j}{g_j}\right|^2 \tag{47}$$

这样,窃听者的互信息就是

$$\begin{aligned}I(\boldsymbol{y}_E;s)&=\frac{1}{3}\log\left(1+\frac{\alpha|e_A|^2|\boldsymbol{Q}_2|}{|\boldsymbol{Q}|}\right)\\&=\frac{1}{3}\log\left(1+\frac{\alpha}{\beta}f(p)\right)\end{aligned} \tag{48}$$

其中

$$f(\boldsymbol{p})=\frac{\sum_{i>j}\mu_{ij}P_iP_j}{\sum_{i>j>k}\alpha_{ijk}P_iP_jP_k} \tag{49}$$

附加了两个条件后的系统的保密速率就是

$$\begin{aligned}R_s'&=[I(y;s)-I(\boldsymbol{y}_E;s)]^{+}\\&=\frac{1}{3}\log\left(1+\frac{\alpha|t|^2}{(\beta|t|^2+u+1)\sigma_n^2}\right)\\&\quad-\frac{1}{3}\log\left(1+\frac{\alpha}{\beta}f(p)\right)\end{aligned} \tag{50}$$

其中 $u\triangleq\sum_{i=1}^{N}|g_i\lambda_i|^2$.

这里,我们再引入一个假设:上式的第一项中,$u\sigma_n^2$ 代表的是各个中继节点接收的噪声经过信道传输后在接收节点处的功率. 各个中继节点的噪声互不相关,所以接收节点处的和功率就是各噪声功率的代数和. 由于这些噪声无法形成相干叠加,如果发送节点的功率比较大的时候,这些噪声就相对比较小,这一项在最终结果中不起主要作用. 所以,我们在优化中忽略这一项的影响,即认为 $\boldsymbol{\lambda}$ 的变化不会影响到 u 的数值. 这样,在最终表达式中,和 $\boldsymbol{\lambda}$ 相关的就只有波束形成参数 t,这样,优化过程就得到了简化.

以上就是我们引入的三个条件,此时的保密传输速率的表达式已经比较简单了,可以用迭代的方式取得优化解.

如果我们把 $f(\boldsymbol{p})$ 整体当做一个变量的话,R_s' 是关于 $f(\boldsymbol{p})$ 的单调减函数. 我们就可以单独先对 $f(\boldsymbol{p})$ 做优化,求得其最小值. 另外,在高信噪比下,很容易满足 $\alpha|t|^2>(\beta|t|^2+u+1)\sigma_n^2$,也就是接收端的信噪比大于 0dB. 此时,$R_s'$ 是关于 $|t|^2$ 的单调增函数,要想获得更高的保密速率,$|t|^2$ 也应该取得其最大值.

这一点的物理意义非常清楚,$|t|^2$ 代表有效信息的波束形成增益,也就是需要有效信息波束形成的功率最大. $|t|^2$ 的限制条件与 α 和 β 相关,所以,采用交替优化的方法来获得 R_s' 的最大值.

将问题式(28)转化为三个子问题进行处理:首先是求解 p 的优化解,问题描述如下

$$\begin{aligned}&\min_{\boldsymbol{p}}\quad f(\boldsymbol{p})\\&\text{s.t.}\quad \boldsymbol{p}^{\mathrm{T}}\boldsymbol{1}=P_0\end{aligned} \tag{51}$$

$f(\boldsymbol{p})$不是凸函数,我们考虑采用其局部最小值代替全局最小值来求解. 为了使多数情况下,求得的局部最小值就是全局最小值,先对于目标函数进行一次大数量的随机搜索. 也就是随机在可行域中产生一些可行点,找到函数值最小的那一个可行点,再以这个可行点为初始点,利用牛顿法进行迭代,得到一个优化解.

第二个子问题就是在固定其他参数的情况下,对于 $\boldsymbol{\lambda}$ 的优化,问题描述如下

$$\begin{aligned} &\max_{\boldsymbol{\lambda}} && |t|^2 \\ &\text{s.t.} && \boldsymbol{\lambda}^{\mathrm{H}} A\lambda = P_0 \end{aligned} \tag{52}$$

这个问题可以用拉格朗日乘数法解决. 目标函数$|t|^2$可以重写为

$$|t|^2 = \boldsymbol{\lambda}^{\mathrm{H}} \boldsymbol{R} \boldsymbol{\lambda} \tag{53}$$

其中 $\boldsymbol{R} \triangleq mtx\{g_i h_i g_j^* h_j^*\}$. 利用拉格朗日乘数法可以得到

$$\boldsymbol{R\lambda} = \rho \boldsymbol{A\lambda} \tag{54}$$

其中ρ是拉格朗日乘数. 这里,$\boldsymbol{R}$不满秩,$\boldsymbol{A}$满秩. 且由于节点总发射功率总大于零,可以知道$\boldsymbol{A}$是正定的矩阵. 这样,可以得到

$$\boldsymbol{A}^{-1}\boldsymbol{R\lambda} = \rho \boldsymbol{\lambda} \tag{55}$$

也就是说,$\boldsymbol{\lambda}$的最优值应当是$\boldsymbol{A}^{-1}\boldsymbol{R}$的某一个特征向量,而$\rho$是$\boldsymbol{A}^{-1}\boldsymbol{R}$的特征值,$\boldsymbol{A}^{-1}\boldsymbol{R}$最大特征值对应的特征向量就是要求得的优化系数$\boldsymbol{\lambda}_o$.

第三个子问题是在固定其他参数的情况下,对于α的优化. 问题描述如下

$$\begin{aligned} &\max_{\alpha,\beta} && R_s' \\ &\text{s.t.} && \alpha + \beta |v_A|^2 = P_A \end{aligned} \tag{56}$$

可以用求导解方程的方法求得,具体的闭式解由于篇幅所限,就不列出了.

总体优化算法就如下:

(1)用随机选择的方法确定初始的功率分配$\boldsymbol{p}_m$,然后,按照牛顿法计算问题(51)的解$\boldsymbol{p}_o$.

(2)$n=1$,确定α的初始值$\alpha_n = P_a/2$,$\alpha_{n-1}=0$.

(3)while $\alpha_n \neq \alpha_{n-1}$ do.

(a)$n=n+1$.

(b)根据α_{n-1}计算问题(52)的解$\boldsymbol{\lambda}_n$.

(c)根据$\boldsymbol{\lambda}_n$计算问题(56)的解α_n.

(4)end while.

(5)此时的α_n和$\boldsymbol{\lambda}_n$就是最终的优化解.

该算法在多数情况下,尤其是高功率的时候(这也是更实用的情况),和最优解差距不大,附加条件分析如下:

第一个条件零空间假设. 通常来说,在第三阶段不泄露信息给窃听者,就是最优的选择. 但是,当窃听者和目的节点的信道向量处于同一方向或者接近,即$\boldsymbol{g}=\rho\boldsymbol{e}$,其中$\rho>1$. 根据建议算法,目的节点也处于信号的零空间,信息无法传递给目的节点,也就是保密传输速率为零,算法失效. 事实上,这种情况下,虽然干扰在窃听者处也被消除了,但由于目的节点的信道状况好于窃听者,系统仍可以进行保密传输. 当然,这种失效的可能性并不大,而且随着中继节点数量的增加,窃听者的信道向量和目的节点相同的可能性会非常小.

第二个条件是高功率假设. 对于实用系统来说,这是一个合理的条件. 只有当系统发射功率比较低的时候,次优算法才会距离最优解比较远.

第三个条件是假设中继的接收噪声被转发后,受分布式波束形成系数影响较小. 该条件通常来说是合理的,只有当个别的中继节点第一阶段链路很弱,第二阶段链路很强,该节点的接收噪声相对就比较大. 如果总发射功率较小,此时,中继噪声功率和波束形成系数的关联很强,次优解就不好了. 通常来说,中继节点的链路质量太差,就不会考虑使用这个中继,所以,这种情况也不会经常碰到.

建议算法的第一步$f(\boldsymbol{p})$的优化(51),采用了一种非最优的算法. 该算法先进行了一次随机搜索,起始点落入局部最优点的附近的可能性并不大. 多数情况下,该算法得到的就是最优解.

综合来看,实际系统中,本论文建议的优化算法会非常接近最优解.

5 仿真

仿真结果都在 LOS 信道模型下进行,仿真模型如图 2 所示. 信源节点和目的节点延水平轴向排列,相互距离 100m. 四个中继节点在源和目的节点的中点处垂直对称分布,上下距离水平轴的距离分别是 10m 和 20m. 移动窃听者的时候,是沿着水平轴从源节点向目的节点移动. 固定窃听者位置的时候,在图中所示的叉号的位置,也就是水平轴上距离源节点 60m 的位置. 在整个系统中,不考虑从源节点到目的节点的直达信道,系统中的噪声功率为$\sigma_n^2 = -60$dBm. 系统中任何两个节点间的复信道增益都表示为$h = d^{-c/2}\mathrm{e}^{j\theta}$,其中$d$是节点

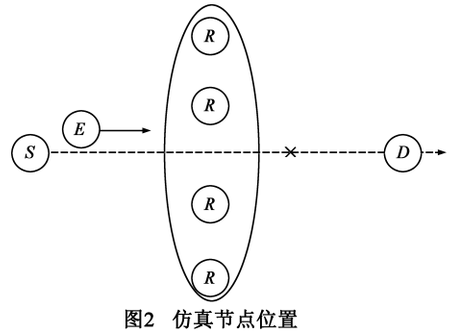

图2 仿真节点位置

间的距离,c 是路损参数,设置为 $c=3.5$,θ 是随机分布的相位,服从[0,2π)区间上的均匀分布. 所有仿真都做了 1000 次,求出其平均值.

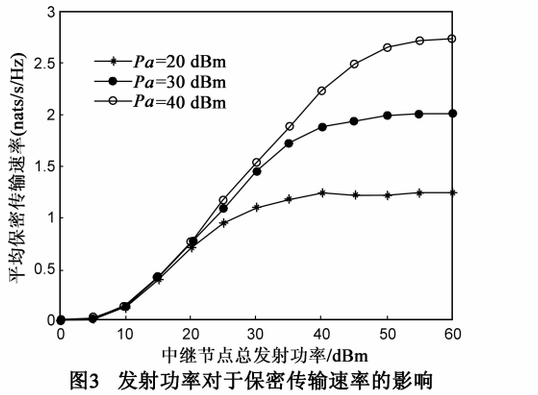

图3　发射功率对于保密传输速率的影响

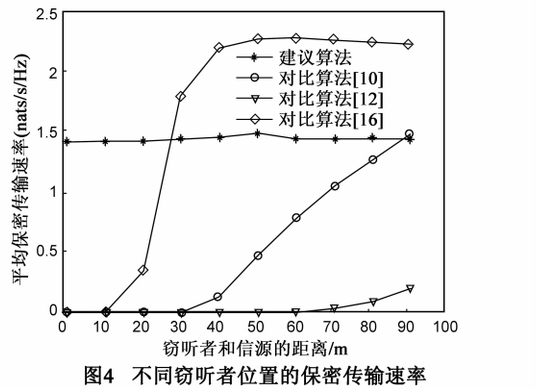

图4　不同窃听者位置的保密传输速率

图 3 显示的是固定窃听者位置的时候,功率和保密传输速率的关系. 可以看出,中继节点的总输出功率增大到一定程度,就不会对系统性能产生大的影响了. 而源节点的输出功率则对保密传输速率影响比较大,源节点功率越大,保密传输速率就越大. 所以,在设计系统的时候,中继节点的总功率控制到一定程度就可以了,更多的需要采用高功率的源节点来提升系统性能.

当窃听者沿着横轴运动的时候,固定 $P_a=P_0=30$dBm,其结果如图 4 所示. 可以看出,窃听者的位置对于建议算法的平均保密传输速率的影响并不大. 我们把建议算法和文献[10,12]和文献[16]中的算法做了对比,几个算法的功率约束相同. 对比算法在窃听者接近源节点的时候,保密速率非常低,甚至为零. 在近源区域内,建议算法的性能远好于对比算法. 由于建议算法的信号中混合了干扰信号,一部分功率并没有用来传输信号. 在远离源节点的地方,建议算法的保密传输速率相对比较低.

6　总结

本文提出了一种新的 AF 中继系统保密通信方法. 该方法有利于在整个通信过程中保护通信数据的安全,与传统方法相比,在窃听者贴近信源节点的时候,本文提出的方法有很大的优势. 这对于实际系统来说非常重要,因为保密的要求不是最佳情况下的性能,而是在最差情况下确保性能,这才能让人放心使用. 这种方法的本质是直接在信息中加入干扰,再在接收节点处消除这部分干扰. 通过信道空间的不相关性,确保窃听者无法获得有效的信息. 该方法并不限于本文的应用场景,可以应用于其他通信系统模型.

参考文献

[1] Wyner AD, The wire-tap channel[J]. Bell Syst Tech J, 1975,54(8):1355 – 1387.

[2] Csiszár I, Kørner J, Broadcast channels with confidential messages[J]. IEEE Trans IT,1978,24(3):339 – 348.

[3] Leung-Yan-Cheong SK, Hellman ME. The gaussian wire-tap channel[J]. IEEE Trans IT,1978,24(4):451 – 456.

[4] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. IEEE Trans WC,2008,7(6):2180 – 2189.

[5] Khisti A, Wornell G. Secure transmission with multiple antennas II: The MIMOME siretap channel[J]. IEEE Trans IT,2010,56(11):5515 – 5532.

[6] Lai L, Gamal HE. The relay-eavesdropper channel: cooperation for secrecy[J]. IEEE Trans IT, 2008, 54(9): 4005 – 4019.

[7] Ekrem E, Ulukus S. Secrecy in cooperative relay broadcast channels[J]. IEEE Trans IT,2011,57(1):137 – 155.

[8] Zhang J, Gursoy MC. Collaborative relay beamforming for secure broadcasting[A]. Proc IEEE Wireless Commun Netw Conf. (WCNC)[C]. Princeton, IEEE, 2010. 1 – 6.

[9] Zhang J, Gursoy MC. Relay beamforming strategies for physical-layer security[A]. Proc 44th Annu Conf Inform Sci Syst. (CISS)[C]. Sydney, IEEE, 2010. 1 – 6.

[10] Dong L, Han Z, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Trans Signal Process,2010,58(3):1875 – 1888.

[11] Yang Y, Li Q, et al. Cooperative secure beamforming for AF relay networks with multiple eavesdroppers[J]. IEEE Signal Proc Letters,2013,20(1):35 – 38.

[12] Long H, Xiang W, et al. Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems [J]. IEEE Trans IFS,2013,8(1):229 – 238.

[13] Wang HM, Yin Q, et al. Distributed beamforming for physical-layer security of two-way relay networks[J]. IEEE Trans SP,2012,60(7):3532 – 3545.

[14] Mo J, Tao M, et al. Secure beamforming for MIMO two-way transmission with an untrusted relay[A]. Proc IEEE Wireless Commun Netw Conf. (WCNC)[C]. Shanghai,

IEEE,2013. 4180 – 4185.
[15] Li J,Petropulu AP,et al. On cooperative relaying schemes for wireless physical layer security[J]. IEEE Trans SP, 2011,59(10):4985 – 4997.
[16] Wang HM,Luo M,et al. Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper´s CSI[J]. IEEE Signal Proc Letters,2013,20(1):39 – 42.
[17] Wang HM,Yin Q,et al. Joint null-space beamforming and jamming to secure AF relay systems with individual power constraint[A]. Acoustics, Speech and Signal Proc. (ICASSP),2013 IEEE International Conference on[C]. Vancouver,IEEE,2013. 2911 – 2914.
[18] Wang HM,Luo M,et al. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks[J]. IEEE Trans IFS,2013,8(12):2007 – 2020.
[19] Zheng G,Choo LC,et al. Optimal cooperative jamming to enhance physical layer security using relays[J]. IEEE Trans SP,2011,59(3):1317 – 1322.
[20] Dong L,Yousefi´zadeh H,et al. Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper[A]. Communications (ICC),2011 IEEE International Conference on[C]. Kyoto, IEEE, 2011. 1 – 5.
[21] Tang L,Gong X,et al. Secure wireless communications via cooperative relaying and jamming[A]. GC'11 workshop on physical-layer security[C]. Houston, IEEE, 2011. 849 – 853.
[22] Tang X,Liu R,et al. Interference assisted secret communication[J]. IEEE Trans IT,2011,57(5):3153 – 3167.
[23] Liu Y,Li J,et al. Destination assisted cooperative jamming for wireless physical-layer security[J]. IEEE Trans IFS, 2013,8(4):682 – 694.
[24] Park KH,Wang T,et al. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming[J]. IEEE J Select Areas Commun, 2013, 31(9):1741 – 1750.
[25] Yang B,Wang W,et al. Destination assisted secret wireless communication with cooperative helpers[J]. IEEE Signal Proc. Letters,2013,20(11):1030 – 1033.
[26] Foschini GJ,Chizhik D,et al. Analysis and performance of some basic spacetime architectures[J]. IEEE J Select Areas Commun,2013,21(1):303 – 320.
[27] Boyd S, Vandenberghe L, Convex Optimization[M]. Combridge University Press,2004.

作者简介

杨 斌 男,1977 年出生,西安交通大学电子与信息工程学院博士生,研究方向为物理层安全.
E-mail:yabby_yb@hotmail.com

王文杰 男,1971 年出生,西安交通大学电子与信息工程学院教授,研究方向为阵列信号处理,传感器网络,物理层安全.
E-mail:wjwang@xjtu.edu.cn

殷勤业 男,1950 年出生,西安交通大学电子与信息工程学院教授,研究方向为时空谱估计,阵列信号处理.