物理层安全中的最优中继选择及协同干扰策略

赵耀环,谢梦非,尚 勇
(北京大学信息科学技术学院,北京 100871)

摘 要: 本文提出了一种以协同干扰为基础,结合了最优中继选择和功率分配的物理层安全方案.该方案针对分布式天线的场景,从中间节点中选择一个最佳的节点作为中继,剩余的其他节点作为协同干扰节点.中继节点使用放大转发策略.本文同时提出了协同干扰节点的波束成形算法.另外,我们还推导出了中继节点和协同干扰节点之间的功率分配的闭式解.最后,本文还给出了相关的仿真结果,证实了新提出的方案比传统方案能获得更高的安全容量.

关键词: 物理层安全; 中继选择; 协同干扰; 功率分配
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112 (2015)04-0791-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.04.023

Cooperative Jamming with Optimal Relay Selection and Power Allocation for Physical Layer Security

ZHAO Yao-huan, XIE Meng-fei, SHANG Yong
(*School of Electronic Engineering and Computer Science, Peking University, Beijing* 100871, *China*)

Abstract: In this paper, a scheme of cooperative jamming with optimal relay selection and power allocation is proposed. The proposed scheme selects one node from the intermediate nodes as relay and the rest nodes as friendly jammers. The relay operates in amplify-and-forward (AF) strategy. Jammer weights are derived to null the jamming signals at the destination and relay node and maximize the jamming signal at the eavesdropper. Furthermore, a closed-form optimal solution of power allocation between the selected relay and cooperative jammers is derived. Numerical simulation results show that the proposed scheme can outperform the conventional schemes at the same power consumption.

Key words: physical layer security; relay selection; cooperative jamming; power allocation

1 引言

在现代通信中,信息安全已经成为了一个越来越受重视的一个重要方面.在20世纪70年代,Wyner发现了一种不依赖于传统的加密算法的可以达到"绝对安全"的新型安全机制[1].这种机制是在通信中的物理层实现的,利用了无线信道天然存在的物理特性.随后,文献[2,3]更加深入地研究了高斯窃听信道中的安全问题.最近,文献[4,5]研究了无线衰落信道下的物理层安全问题.

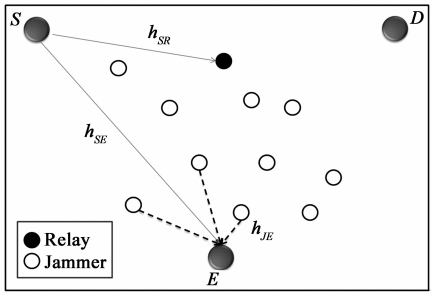
在存在窃听者的情况下,无线信道的安全性可以由安全容量来评价.安全容量定义为窃听者无法得到任何有用信息的最大通信速率.显然,当合法通信信道比窃听信道还差时,安全容量为零[1].为了解决这一问题,文献[6~10]提出了协同中继与协同干扰的多种方案.在文献[6]中,Krikidis等人提出了在一种最优中继选择(Optimal Selection, OS)的方法.该方法从辅助节点中选出最优的中继节点来最大化安全容量.随后,在文献[7]中,Krikidis等人又提出了最优中继与干扰(Optimal Selection and Jamming, OSJ)的方法.该方法在每个阶段选择一对节点,一个作为中继另一个作为协同干扰节点.最近,J Chen等人在一个双向中继的系统中分析了OSJ方法[10].另外,在协同中继的波束成形方面也有很多先前的工作.如Dong等人研究了多中继情形下的最优中继波束成形算法(Optimal Relay Beamforming, ORB)[9],该算法包括两种情况,分别是在解码转发或放大转发两种策略下最大化接收节点的接收功率的中继波束成形算法,以及所有辅助节点作为协同干扰节点时最大化窃听节点的干扰功率的干扰波束成形算法.

本文考察了一种包含了多个中间辅助节点的单向中继网络,提出了一种结合了最优中继选择和协同干扰波束成形的方案.

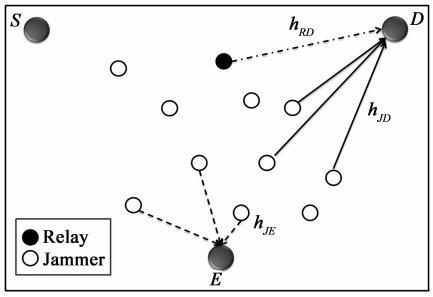
收稿日期:2013-10-30;修回日期:2014-05-16;责任编辑:李勇锋

2 系统模型

本文考虑的系统模型如图1所示,系统中包含一个发射节点 S,一个接收节点 D,一个窃听节点 E 以及 K 个中间辅助节点.假设所有节点工作在半双工模式,即节点不能同时发送和接受消息,整个通信过程可以分成两个阶段.



(*a*) 第一阶段



(*b*) 第二阶段

图1 系统模型

在第一阶段,S 将需要发送的信息发送至中继节点 R,同时这些信息也有可能被窃听节点 E 截获.协同干扰节点向外发送人工噪声干扰.

在第二阶段,中继节点 R 向接收节点 D 转发消息.干扰节点同样向外发送干扰信号.

本文假设网络中的所有节点之间的信道为缓变平衰落的 Rayleigh 信道,信道衰落的方差为 $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$,其中 $d_{i,j}$ 表示节点 i 和节点 j 之间的距离.β 表示信道的路径损耗指数.假设 S-D 之间的通信链路已被遮挡($h_{SD} \approx 0$).$\boldsymbol{h}_{JR}$ 表示 N 个干扰节点与中继节点 R 之间的信道矢量,$\boldsymbol{h}_{JE}$ 表示 N 个干扰节点与窃听节点 E 之间的信道矢量,其中 $N = K - 1$ 表示协同干扰节点的个数.另外,本文还假设每个节点处都有零均值单位方差的加性高斯白噪声.P_S,P_{in} 和 P_R 分别代表发射节点的功率,辅助节点的总功率限制以及中继节点 R 的发射功率.

在第一阶段中,S 发送信息符号 x,中继节点 R 和窃听节点 E 接收到的信号分别为:

$$r = \sqrt{P_S} h_{SR} x + \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 z + n_R \tag{1}$$

$$e_1 = \sqrt{P_S} h_{SE} x + \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_1 z + n_{e1}$$

其中 n_R 和 n_{e1} 分别表示 R 和 E 处的功率归一化的高斯白噪声,$\boldsymbol{w}_1$ 表示在第一阶段分配给 N 个协同中继节点的波束成形矢量,z 表示干扰节点发出的人工噪声信号,其功率也已归一化.

在第二阶段,中继节点 R 以放大转发的方式工作.其传输信号为

$$t = \alpha \sqrt{P_R} r \tag{2}$$

其中

$$\alpha = \frac{1}{\sqrt{1 + P_S \left| h_{SR} \right|^2 + \left| \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2}} \tag{3}$$

在第二阶段,D 和 E 接收到的信号为

$$y = \sqrt{P_R} h_{RD} \alpha r + \boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{w}_2 z + n_d$$

$$e_2 = \sqrt{P_R} h_{RE} \alpha r + \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_2 z + n_{e2} \tag{4}$$

其中,n_d 和 n_{e2} 分别表示 D 和 E 处的高斯白噪声信号,$\boldsymbol{w}_2$ 表示在第二阶段中的协同干扰波束成形矢量.

根据式(1)和式(4),S 与 D 之间的链路的信干噪比(SINR)可以写为

$$\Gamma_{SD} = \frac{P_R P_S \left| h_{SR} \right|^2 \left| h_{RD} \right|^2 \alpha^2}{\alpha^2 P_R \left| h_{RD} \right|^2 \left| \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2 + P_R \left| h_{RD} \right|^2 \alpha^2 + \left| \boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{w}_2 \right|^2 + 1} \tag{5}$$

在本文中,假设窃听节点可以采用最大比合并的方式从两个阶段提取的信号 e_1 和 e_2 中提取信息,则窃听节点 E 的 SINR 可以表示为

$$\Gamma_E = \frac{\bar{P}_S \left| h_{SE} \right|^2}{\left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2 + 1} + \frac{\alpha^2 P_S P_R \left| h_{SR} \right|^2 \left| h_{RE} \right|^2}{P_R \alpha^2 \left| h_{RE} \right|^2 \left| \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2 + P_R \left| h_{RE} \right|^2 \alpha^2 + \left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_2 \right|^2 + 1} \tag{6}$$

最后,根据文献[10],S 与 D 之间的安全容量定义为

$$C_S = \max\left\{ \frac{1}{2} \log_2(1 + \Gamma_{SD}) - \frac{1}{2} \log_2(1 + \Gamma_E), 0 \right\} \tag{7}$$

我们需要从 K 个辅助节点构成的集合中选择一个最优的中继节点 R,并且优化波束成形矢量 $\boldsymbol{w}_1$ 和 $\boldsymbol{w}_2$ 以及中继节点的发射功率 P_R.

3 方案描述

3.1 最优中继选择与干扰波束成形(Optimal Relay Selection with Cooperative Jammers,OS-CJ)

OS-CJ 从辅助节点中选出一个中继节点 R,剩余的节点全部作为友好干扰节点.中继节点的功率固定为 $P_R = 0.5 P_{\text{in}}$,即中继功率设置为总功率的一半.本节的目标是选出最优的中继 R,并且优化 $\boldsymbol{w}_1$ 和 $\boldsymbol{w}_2$ 的权值来最大化安全容量.

在第一阶段,$\boldsymbol{w}_1$ 需要在保证对中继节点 R 完全没有干扰的情况下,尽量最大化对窃听节点的干扰功率,同时还需要满足功率约束条件.

这个优化问题可以建立成如下所示的数学模型:

$$\arg\max_{\boldsymbol{w}_1} \left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2 \quad \text{s.t.} \quad \begin{cases} \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 = 0 \\ \boldsymbol{w}_1^{\mathrm{H}} \boldsymbol{w}_1 = P_{\mathrm{in}} \end{cases} \tag{8}$$

在文献[9]中给出了式(8)的解:

$$\boldsymbol{w}_1 = \mu_1 \| \boldsymbol{h}_{JR} \|^2 \boldsymbol{h}_{JE}^* - \mu_1 (\boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{h}_{JE}^*) \boldsymbol{h}_{JR}^* \tag{9}$$

其中 $\| \cdot \|$ 表示矢量的二阶范数,μ_1 为标量,值为:

$$\mu_1 = \sqrt{\frac{P_{\mathrm{in}}}{\| \boldsymbol{h}_{JR} \|^4 \| \boldsymbol{h}_{JE} \|^2 - \| \boldsymbol{h}_{JR} \|^2 \left| \boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{h}_{JE}^* \right|^2}} \tag{10}$$

在第二阶段,与第一阶段相似的是,$\boldsymbol{w}_2$ 也需要在保证对接收节点 D 无干扰的情况下最大化对窃听节点的干扰功率.此问题可以建模为:

$$\arg\max_{\boldsymbol{w}_2} \left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_2 \right|^2 \quad \text{s.t.} \quad \begin{cases} \boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{w}_2 = 0 \\ \boldsymbol{w}_2^{\mathrm{H}} \boldsymbol{w}_2 = P_{\mathrm{in}} - P_R \end{cases} \tag{11}$$

其解可以写为

$$\boldsymbol{w}_2 = \mu_2 \| \boldsymbol{h}_{JD} \|^2 \boldsymbol{h}_{JE}^* - \mu_2 (\boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{h}_{JE}^*) \boldsymbol{h}_{JD}^* \tag{12}$$

其中 μ_2 值为

$$\mu_2 = \sqrt{\frac{P_{\mathrm{in}} - P_R}{\| \boldsymbol{h}_{JD} \|^4 \| \boldsymbol{h}_{JE} \|^2 - \| \boldsymbol{h}_{JD} \|^2 \left| \boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{h}_{JE}^* \right|^2}} \tag{13}$$

在满足两个约束 $\boldsymbol{h}_{JR}^{\mathrm{T}} \boldsymbol{w}_1 = 0$, $\boldsymbol{h}_{JD}^{\mathrm{T}} \boldsymbol{w}_2 = 0$ 的条件下,S-D 链路与 S-E 链路的 SINR 可以重写为:

$$\Gamma_{SD} = \frac{P_R P_S \left| h_{SR} \right|^2 \left| h_{RD} \right|^2 \alpha^2}{P_R \left| h_{RD} \right|^2 \alpha^2 + 1} \tag{14}$$

$$\Gamma_E = \frac{P_S \left| h_{SE} \right|^2}{\left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_1 \right|^2 + 1} + \frac{\alpha^2 P_S P_R \left| h_{SR} \right|^2 \left| h_{RE} \right|^2}{P_R \left| h_{RE} \right|^2 \alpha^2 + \left| \boldsymbol{h}_{JE}^{\mathrm{T}} \boldsymbol{w}_2 \right|^2 + 1} \tag{15}$$

其中

$$\alpha = \frac{1}{\sqrt{1 + P_S \left| h_{SR} \right|^2}} \tag{16}$$

之后可以选择最优中继节点为

$$\arg\max_R \frac{1 + \Gamma_{SD}}{1 + \Gamma_E} \tag{17}$$

3.2 最优功率分配(Optimal Selection and Power Allocation with Cooperative Jamming,OS-PA-CJ)

OS-PA-CJ 在 OS-CJ 的基础上增加了最优功率分配的考虑.最优功率选择问题可以建模如下:

$$\arg\max_{R, P_R} \frac{1 + \Gamma_{SD}}{1 + \Gamma_E} \tag{18}$$

当选择好一个中继节点 R 之后,目标函数就可以写成一个 P_R 的单变量函数.式(18)可以重写为:

$$f(P_R) = \frac{1 + \Gamma_{SD}}{1 + \Gamma_E} = \frac{1 + \dfrac{P_R A}{P_R B + 1}}{C + \dfrac{P_R D}{P_R E + F}} \tag{19}$$

其中 $A \sim F$ 均为与 P_R 无关的标量,在优化过程中可以视作常量.对 $f(P_R)$取导数,可以得到

$$f'(P_R) = \frac{aP_R^2 + bP_R + c}{dP_R^2 + eP_R + f} \tag{20}$$

其中 a-f 同样为与 P_R 无关的系数.令 $f'(P_R) = 0$,可以得到最优的中继功率

$$\tilde{P}_R = \frac{-\sqrt{\Delta} - af + cd}{ae - bd} \tag{21}$$

其中

$$\Delta = a^2 f^2 - abef - 2acdf + ace^2 + b^2 df - bcde + c^2 d^2 \tag{22}$$

通常,$\tilde{P}_R$ 的值都在 0 与 P_{in}之间.当 R 与 P_{in}都固定时,安全容量与 P_R 的关系是一个凸函数,在 $\tilde{P}_R$ 处取得最大值.当 $\tilde{P}_R < 0$ 时,说明此时安全容量为 0,当 $\tilde{P}_R > P_{\mathrm{in}}$时,最优的中继节点功率即为 P_{in}.

4 性能分析

在本节中,我们对提出的模型进行了数值仿真.仿真场景由一个源节点 S,一个目的节点 D,一个窃听节点 E 和 $K = 10$ 个辅助节点组成.所有的节点都分布在 1 × 1 的正方形区域内,其中 S、D、E 分别位于(0,0),(1,1)和(0.5,0).为了简化问题,我们假设发送功率 P_S 与辅助节点的总功率限制 P_{in}相等,信道的路径损耗指数设为 $\beta = 3$.

我们对本文提出的方案与现存的方案(OS,OSJ 和 ORB)进行了性能对比.为了公平,我们假设在不同方案中中间节点的总功率限制 P_{in}相等.对于 OS 和 ORB,在第一阶段没有功率消耗,因此中继节点的功率为 $P_R = 2P_{\mathrm{in}}$.对于 OSJ,功率限制为 $P_R + 2P_J = 2P_{\mathrm{in}}$.

不同方案的性能仿真结果如图 2 所示,从图 2 中可以看出,在相同的功率限制情况下,本文的方案 OS-CJ 和 OS-PA-CJ 比传统方案 OS 和 OSJ 性能更优.当 $P_S >$ 10dB 时,OS 方案下的安全速率 C_s 几乎达到最大值.当 $P_S >$ 25dB 时,OSJ 方案的安全速率也不再提高.而 OS-CJ 和 OS-PA-CJ 的安全速率仍然保持线性增加.可见,本文提出的方案显著提高了安全容量.

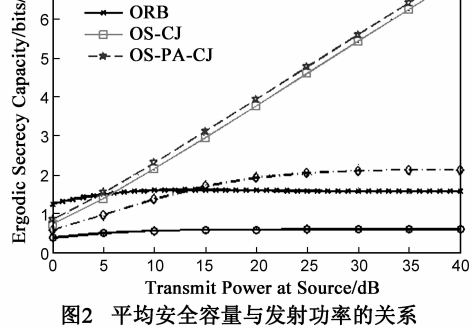


图2　平均安全容量与发射功率的关系

很显然,辅助节点的分布对于性能有显著影响.为了得到更普遍的结果,我们通过对辅助节点进行随机位置撒点,进行了 1000 次蒙特卡罗仿真得到平均安全速率.图 3 显示了在此情况下的五种方案的性能仿真.可以看出,OS-CJ 和 OS-PA-CJ 方案仍然明显优于其他方案.

图 4 显示了平均安全速率随辅助节点数目变化曲线(P_S = 10dB).可以看出,随着中间节点数目增加,所有方案的性能有所提高.特别的,当辅助节点数目增加到 16 时,OSJ 方案的平均安全速率性能十分接近 OS-CJ.然而,当中间节点数目增大到一定情况时,平均安全速率的增长变得非常缓慢.因此,当辅助节点数目较大时再增加节点数目对性能的提升是有限的.所以,在实际中需要综合考虑性能增益和节点数目增加带来的复杂度增加,选择合适的辅助节点数目.

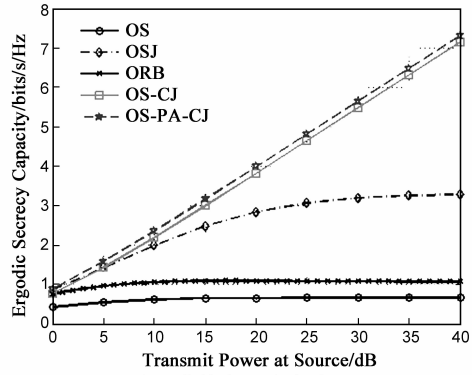


图3 蒙特卡罗仿真结果

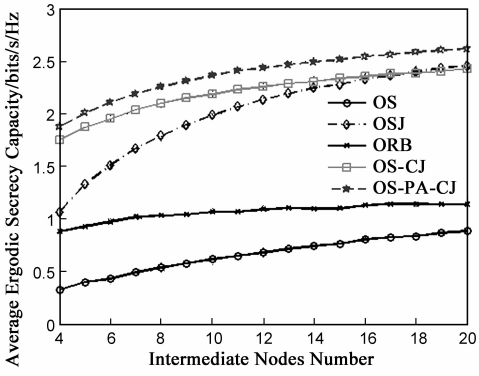


图4 平均安全容量与节点数量的关系

5 结束语

本文针对含有多个辅助节点的无线网络模型,提出了一种新型的最优中继选择及协同干扰的策略.该策略从辅助节点中选出一个最优的节点作为中继节点,并将剩余的辅助节点作为协同干扰节点.友好干扰节点进行了波束成形来消除对目的节点和中继节点的干扰,并且最大化对窃听者的干扰.另外,本文推导出了干扰节点和中继节点之间的最优功率分配的闭式解.通过在相同功率限制下,对不同的节点分布模型进行数值仿真,验证了本文提出的方案在所有场景下比现有方案都有明显的性能提升.另外,本文研究了中间节点数目对系统性能的影响,结果分析发现安全容量随着中间节点数增加而提高,但随着数目增大,提高的速率变缓.

参考文献

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

[2] I Csiszar, et al. Broadcast channels with confidential messages [J]. IEEE Transactions on Information Theory, 1978, 24(3): 339 – 348.

[3] S K Leung-Yan-Cheong, et al. The Gaussian wiretap channel [J]. IEEE Trans Inf Theory, 1978, 24(4): 451 – 456.

[4] Y Liang, et al. Secure communication over fading channels[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2470 – 2492.

[5] P K Gopala, et al. On the secrecy capacity of fading channels [J]. IEEE Trans Inf Theory, 2008, 54(10): 4687 – 4698.

[6] I Krikidis. Opportunistic relay selection for cooperative networks with secrecy constraints [J]. IET Commun, 2010, 4 (15): 1787 – 1791.

[7] I Krikidis, et al. Relay selection for secure cooperative networks with jamming[J]. IEEE Transactions on Wireless Communications, 2009, 8(10): 5003 – 5011.

[8] B Rankov, et al. Achievable rate regions for the two way relay channel[A]. Proceedings of IEEE International Symposium on Information Theory[C]. Seattle: IEEE, 2006. 1668 – 1672.

[9] L Dong, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875 – 1888.

[10] J Chen, et al. Joint relay and jammer selection for secure two-way relay networks [J]. IEEE Transactions On Information Forensic and Security, 2012, 7(1): 310 – 320.

作者简介

赵耀环 男,1989 年 11 月出生于河北省石家庄市,现为北京大学信息科学技术学院硕士生.

E-mail: blazingring@pku.edu.cn

尚 勇 男,1970 年 12 月出生于陕西省西安市,2000 年在西安电子科技大学获得工学博士学位,现为北京大学信息科学技术学院副教授.

E-mail: shangyong@pku.edu.cn