DOI:10.16515/j.cnki.32-1722/n.2018.02.0004

全双工网络的友好干扰协作机制和功率分配

罗荣华[1],雷 俊[2],胡国兵[3]

(1.金陵科技学院网络与通信工程学院,江苏 南京 211169;2.南京熊猫汉达科技有限公司,江苏 南京 210094;
3.金陵科技学院电子与信息工程学院,江苏 南京 211169)

摘 要:在无线全双工中继网络中,假设中继节点是不可信任的,为了改善合法用户的物理层安全性能,利用友好干扰节点向中继节点发射干扰信号进行协作,且为了获得帮助,合法用户需向干扰节点支付一定的费用。基于此协作干扰机制,讨论了如何对友好干扰节点进行有效的功率分配,从而使得合法用户获得的效用达到最优。理论分析和仿真结果表明,由于中继节点采用了全双工技术,且利用友好干扰节点进行协作,并在此基础上进行最优功率分配,合法用户的物理层安全性能可得到有效提高。

关键词:全双工;物理层安全;友好干扰节点;协作干扰机制;功率分配

中图分类号:TN92 **文献标识码**:A **文章编号**:1672-755X(2018)02-0015-04

Friendly Jamming Cooperative Scheme and Power Allocation in Full-Duplex Network

LUO Rong-hua[1], LEI Jun[2], HU Guo-bing[1]

(1. Jingling Institute of Technology, Nanjing 211169, China;
2. Nanjing Panda Handa Technology Company Limited, Nanjing 210094, China)

Abstract: In wireless full-duplex relay network, the relay node is assumed to be untrusted. In order to enhance the physical layer security of legitimate user, the friendly jammers are proposed to transmit interference signals to the untrusted relay node for cooperation. The legitimate user must pay the costs to friendly jammers for gaining help. Based on this cooperative jamming scheme, the power allocation problem of friendly jammers for maximizing the physical layer security of legitimate users was discussed. Theoretical analysis and simulation results show that when the relay nodes adopt full duplex technology and cooperate with the friendly jammers, and the optimal power allocation is also carried out according to the scheme, the physical layer security of the legitimate users can be effectively improved.

Key words: full-duplex; physical layer security; friendly jammers; cooperative jamming scheme; power allocation

近年来,物理层安全(Physical Layer Security)通信正得到越来越多的关注[1-3],而全双工(Full-Duplex)技术由于能够有效提高频谱效率也成为当前研究的热点[4-6]。显然,若无线通信系统采用全双工技术,且考虑物理层安全通信,无疑可提高系统的有效性和可靠性,同时将面临更多的机遇和挑战。

收稿日期:2018-04-06

基金项目:江苏省自然科学基金资助项目(BK20161104);江苏省高校自然科学研究面上项目(16KJB510011);金陵科技学院校级科研基金(jit-2016-jlxm-24);金陵科技学院博士科研启动基金(jit-b-201409)

作者简介:罗荣华(1980—),女,湖北荆门人,讲师,博士,主要从事物理层安全通信、RF供电通信技术、认知无线电及协作中继通信等研究。

现阶段，基于全双工技术的物理层安全通信通常考虑存在恶意监听用户时，目的节点或基站采用全双工技术，如文献[7－8]所示。此外，还有学者研究了无线网络中存在恶意监听用户并采用全双工技术，形成博弈论的机制对物理层安全性的影响[9]。此外，文献[10]考虑全双工中继网络中，存在恶意监听者，为了改善合法用户的物理层安全性能，提出了友好协作干扰机制。文献[11]经过证明发现在半双工中继网络中，非信任中继节点存在恶意监听的情况时，合法用户的保密速率为 0，若考虑全双工非信任中继时，其保密速率是否也为 0 呢？本文对此问题进行了探索，给出了肯定答案。同时，为了改善合法用户的物理层安全性能，提出了友好干扰协作机制，并在此基础上进行了最优的功率分配。

1 系统模型

本文采用的无线通信网络如图 1 所示，中继节点分别采用两个天线同时同频段进行发送和接收。源节点、中继节点和干扰节点发射的功率分别为 p_S、p_R 和 $p_{J,l}$。首先讨论无友好干扰节点帮助时，在中继节点处，接收的信号可表示为：

$$r[i]=h_{SR}x[i]+h_{LI}t[i]+n_R[i] \tag{1}$$

$x[i]$和 $t[i]$分别表示源节点和中继节点发射的信号。在目的节点处接收到的信号表示为：

$$y[i]=h_{RD}t[i]+n_D[i] \tag{2}$$

其中，$n_R[i]$和 $n_D[i]$分别表示节点处的加性高斯白噪声(Additive White Gaussian Noise，AWGN)，其服从均值为 0、方差为 σ^2 的高斯分布。中继节点采用放大转发(Amplify and Forward，AF)方式，放大因子 β 为：

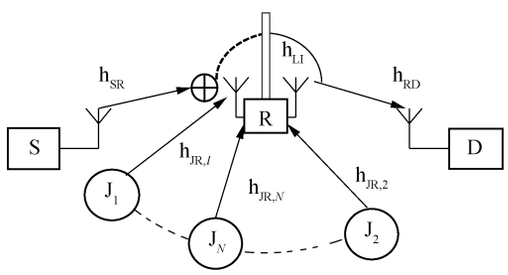

图 1 无线全双工中继网络模型

$$\beta=\sqrt{\frac{p_R}{p_S|h_{SR}|^2+p_R|h_{LI}|^2+\sigma^2}} \tag{3}$$

由于 $r[i]$和 $t[i]$存在如下关系：

$$t[i]=\beta r[i-\tau] \tag{4}$$

其中，$\tau\geqslant 1$，表示延迟的符号数。经过计算，得到中继节点和目的节点处获得的速率：

$$R_E=\log_2\left(1+\frac{p_S|h_{SR}|^2}{p_R|h_{LI}|^2+\sigma^2}\right) \tag{5}$$

$$R_D=\log_2\left(1+\frac{p_S|h_{SR}|^2}{p_R|h_{LI}|^2+\sigma^2+\dfrac{\sigma^2}{\beta^2|h_{RD}|^2}}\right) \tag{6}$$

从公式(5)和(6)对比中，可以得到：

$$R_D<R_E \tag{7}$$

这说明，在没有友好干扰节点的帮助下，合法用户的保密速率为 0[11]。

假设，在友好干扰节点的帮助下，中继节点和目的节点处接收到的 SINR(Signal to Interference plus Noise Ratio)为：

$$\gamma_R=\frac{p_S|h_{SR}|^2}{p_R|h_{LI}|^2+\sum_{l=1}^{N}p_{J,l}|h_{JR,l}|^2+\sigma^2} \tag{8}$$

$$\gamma_D=\frac{p_S|h_{SR}|^2}{p_R|h_{LI}|^2+\sigma^2+\dfrac{\sigma^2}{\beta^2|h_{RD}|^2}} \tag{9}$$

比较公式(8)和(9)可知，若要保密速率大于 0，则需要满足以下关系式：

$$\sum_{l=1}^{N}p_{J,l}|h_{JR,l}|^2>\frac{1}{\beta^2|h_{RD}|^2} \tag{10}$$

2　算法描述

为了使得友好干扰节点有动力向合法用户提供帮助，合法用户需要付给干扰节点相应的费用，由此我们形成如下最优化问题：

$$\max U = \alpha R_{\mathrm{S}} - \sum_{l=1}^{N} c_l p_{\mathrm{J},l} \quad \text{s.t.} \quad R_{\mathrm{S}} > 0$$
$$0 \leqslant p_{\mathrm{J},l} \leqslant p_{\max} \quad \text{fixed} \quad p_{\mathrm{S}}, p_{\mathrm{R}} \tag{11}$$

其中，$R_{\mathrm{S}} = R_{\mathrm{D}} - R_{\mathrm{E}}$，$c_l$ 表示不同友好干扰节点向合法用户收取费用所定的单位功率价格，$\alpha > 0$ 表示单位速率增益因子，$p_{\max}$ 表示节点发射的最大功率，p_{S} 和 p_{R} 均为固定功率。对上述问题进行求解，可对目标函数 U 求一阶导数，设 $A_1 = p_{\mathrm{R}}^2 \mid h_{\mathrm{LI}} \mid^2 \mid h_{\mathrm{RD}} \mid^2 + \sigma^2 \left(p_{\mathrm{S}} \mid h_{\mathrm{SR}} \mid^2 + p_{\mathrm{R}} \mid h_{\mathrm{LI}} \mid^2 + \sigma^2 + \sum_{l=1}^{N} \mid h_{\mathrm{JR},l} \mid^2 p_{\mathrm{J},l} \right) + p_{\mathrm{R}} \mid h_{\mathrm{RD}} \mid \sigma^2$，$A_2 = p_{\mathrm{R}} \mid h_{\mathrm{LI}} \mid^2 + \sigma^2 + \sum_{l=1}^{N} \mid h_{\mathrm{JR},l} \mid^2 p_{\mathrm{J},l}$，当 $\dfrac{\partial U}{\partial p_{\mathrm{J},l}} = 0$ 时，经过推导可求得：

$$\lambda_1 p_{\mathrm{J},l}^4 + \lambda_2 p_{\mathrm{J},l}^3 + \lambda_3 p_{\mathrm{J},l}^2 + \lambda_4 p_{\mathrm{J},l} + \lambda_5 = 0 \tag{12}$$

其中，λ_n，$n = 1,2,3,4,5$ 分别是由 A_1，A_2，p_{S}，p_{R}，$\sum_{\substack{k \neq l \\ k=1}}^{N} p_{\mathrm{J},k}$ 等参量所组成。此四阶多项式方程求解较为困难，而我们所关心的主要是 $p_{\mathrm{J},l}$ 与哪些参数有关，所以 $p_{\mathrm{J},l}$ 可简单表示如下：

$$p_{\mathrm{J},l}^* = p_{\mathrm{J},l}^* \left(A_1, A_2, p_{\mathrm{S}}, p_{\mathrm{R}}, \sum_{N} p_{\mathrm{J},k}^*, \lambda_l \right) \tag{13}$$

考虑到约束条件，$p_{\mathrm{J},l\_opt} = \min\{\max\{p_{\mathrm{J},k}^*, 0\}, p_{\max}\}$。

3　仿真结果及性能分析

本文基于 Matlab 软件平台进行蒙特卡罗仿真。假设源节点、中继节点和目的节点所处的坐标位置分别为(−1,0)、(0,0)、(1,0)。而其它参数设置为 $p_{\max}=10$，$\alpha=1$，$\sigma^2=0.01$，$h_{ij} \sim CN(0, d_{ij}^{-\tau})$，$\tau=2$，$p_{\mathrm{S}}=p_{\mathrm{R}}=10$ mW。

从图 2 可以看出，友好干扰节点越接近中继节点，中继节点窃听到的信息量越少，合法用户则可获得更高的效用。从图 3 可知，随着单位功率价格的提高，合法用户向友好中继节点买入的功率越小，最后趋近于 0。

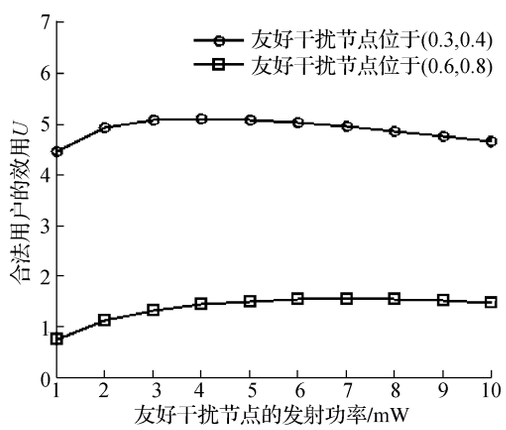

图 2　合法用户的效用 V_{S} 发射功率

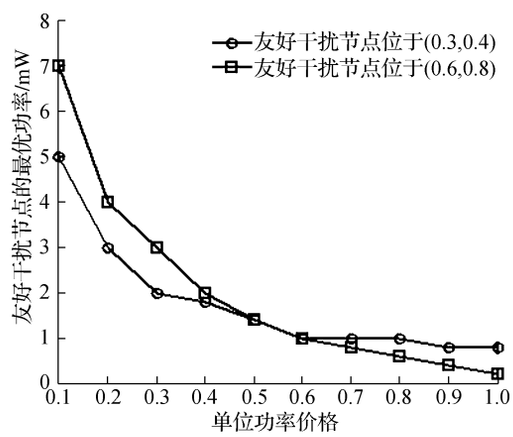

图 3　友好干扰节点的最优功率 V_{S} 单位功率价格

从图 4 可知，若中继节点采用全双工技术，由于需要同时进行发送和接收，其所窃听到的信息量较半双工大，为了使得合法用户的收益最大，其所需要的干扰功率比采用半双工技术要大。在图 5 中，全双工中继网络的保密性能明显优于半双工中继网络。这是因为与半双工相比，全双工技术能够获得较大的频

谱效率，因而合法用户的保密速率明显大于半双工，相应的其收益也较大。

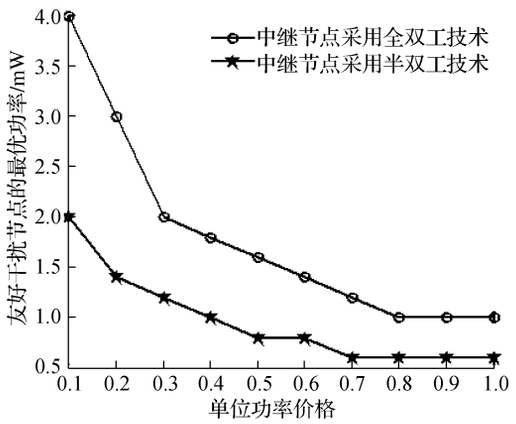

图 4 友好干扰节点的最优功率 V_S 单位功率价格

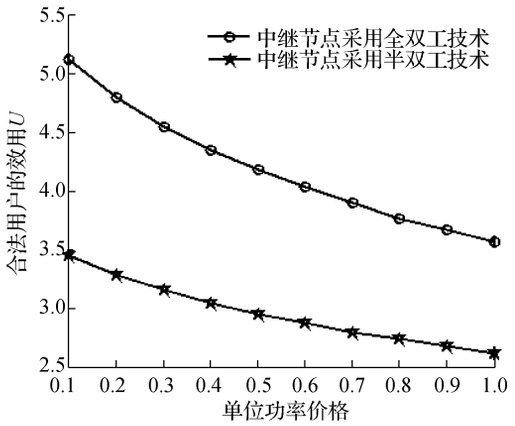

图 5 合法用户的效用 V_S 单位功率价格

4 结 语

本文讨论无线通信网络中，存在非信任全双工中继节点，为了改善合法用户的保密性能，提出友好干扰协作机制，并通过对干扰节点的功率进行有效分配，使合法用户的保密性能得到最优。并通过理论分析和仿真结果证明，与没有友好干扰节点的帮助相比，合法用户获得了更高的保密性能，且因为非信任中继节点采用了全双工技术，使得合法用户的保密速率明显优于半双工技术。

参考文献：

[1] 杨斌. 无线通信物理层安全技术研究[J]. 信息网络安全，2012(6)：76－79

[2] Zhang H J，Xing H，Cheng J L，et al. Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming[J]. IEEE Transactions on Industrial Informatics，2016，12(5)：1714－1725

[3] Zhao J，Lu Z M，Wen X M，et al. Resource management based on security satisfaction ratio with fairness-aware in two-way relay networks[J]. International Journal of Distributed Sensor Networks，2015，6(11)：1－5

[4] Meulen E C. Three-terminal communication channels[J]. Advances in Applied Probability，1997，3：120－154

[5] Cover T M，Gamal A E. Capacity theorems for the relay channel[J]. IEEE Transactions on Information Theory，1979，25(5)：572－584

[6] Wang L，Tian F，Svensson T，et al. Exploiting full duplex for device-to-device communications in heterogeneous networks[J]. IEEE Communication Magazine，2015，53(5)：146－152

[7] Zheng G，Krikids I，Li J，et al. Improving physical layer secrecy using full-duplex jamming receivers[J]. IEEE Transactions on Signal Processing，2013，61(20)：4962－4974

[8] Zhu F C，Gao F F，Yao M L，et al. Joint information- and jamming- beamforming for physical layer security with full duplex base station[J]. IEEE Transactions on Signal Processing，2014，62(24)：6391－6401

[9] Tang X，Ren P Y，Han Z. Combating full-duplex active eavesdropper：a game-theoretic perspective [C]//IEEE ICC 2016 Communication and Information Systems Security Symposium. Kuala Lumpur：IEEE Press，2016：1－6

[10] Li X R，Dai H N. Friendly-jamming：An anti-eavesdropping scheme in wireless networks [C]//2017 IEEE 18th International Symposium on A World of Wireless，Mobile and Multimedia Networks (WoWMoM). Macau：IEEE Press，2017：1－3

[11] He X，Yener A. Cooperation with untrusted relay：a secrecy perspective[J]. IEEE Transactions on Information Theory，2010，56(8)：3807－3827

（责任编辑：湛 江）