DOI:10.13718/j.cnki.xsxb.2015.01.019

基于鲁棒波束成形的 WSNs 可达安全速率研究①

武春岭, 鲁先志, 李贺华

重庆电子工程职业学院 计算机学院,重庆 401331

摘要:针对 WSNs 节点间通信易受非法节点窃听的问题,提出了鲁棒波束成形噪声发送策略来提高节点间的可达安全速率. 假设协作干扰节点只知道其到窃听节点的部分信道状态信息,在最差信道条件下通过优化协作干扰节点的噪声输入协方差矩阵来最大化系统的可达安全速率. 为求解此非凸的最大最小化问题,首先通过数学等价转化将该非凸问题转化为半定规划问题,然后设计了一维搜索算法来计算节点间的最优可达安全速率. 最后,通过仿真验证了所提算法的有效性.

关 键 词:无线传感器网络;可达安全速率;协作干扰;非凸优化;鲁棒波束成形

中图分类号:TP393 **文献标志码**:A **文章编号**:1000-5471(2015)1-0107-06

近年来,无线传感器网络(Wireless Sensor Networks, WSNs)凭借其强大的数据获取和处理能力在军事、救灾、环境、医疗、工业等领域得到了广泛的应用. 然而无线信道的广播特性使得 WSNs 中节点间的无线通信既容易受到自然界噪声的干扰,又容易受到人为对信息进行的攻击、篡改或者窃听[1]. 传统上认为安全的 WSNs 节点间通信的加密算法也随着计算机性能的提高和解密算法的快速出现变得不那么安全[2]. 因此,可以确保通信绝对安全的基于信息理论的物理层安全技术引起了广大学者的广泛关注.

文献[3]中定义了绝对安全的条件:窃听节点接收到的信号与发送节点发送的消息之间的互信息为零. Wyner 在文献[3]证明了在有窃听节点存在的情况下,发送节点与窃听节点间信道是发送节点与目的节点间的信道的退化信道时,发送节点与目的节点不依赖密钥可以做到绝对安全通信. 文献[4]中把安全容量定义为在窃听节点不能译出任何发送节点发送的消息的前提下,通信节点间所能达到的最大可达安全速率. 文献[5]和[6]分析了 WSNs 中通信节点都为多天线时的多输入多输出(Multiple Input Multiple Output, MIMO)信道的安全容量. 文献[7]证明了协作干扰策略有助于 WSNs 中发送节点与目的节点间安全通信性能的提高. 然而,协作干扰节点可以通过目的节点的反馈获得其到目的节点的准确信道状态信息,却很难获得其到窃听节点的准确信道状态信息.

本文假设协作干扰节点不知道它到目的节点的准确信道状态信息,只知道它到窃听节点的部分信道状态信息和信道误差范围,在这种情况下,采用最差性能最优的准则对协作干扰节点进行鲁棒波束成形设计,从而实现系统的可达安全速率最大化. 此时,由于信道误差的不确定性,最大化最差信道情况下的可达安全速率是一个非凸最大最小化问题,很难直接求解. 本文通过一些数学等价转化将该非凸优化问题转化为容易求解的半定规划问题,然后设计了计算最优可达安全速率的一维搜索算法. 最后,通过仿真验证说明本文所提协作干扰节点鲁棒波束成形噪声发送策略,可以显著提高 WSNs 节点间的可达安全速率.

1 系统模型及问题描述

本文研究的系统模型如图 1 所示,包括发送节点(Alice),目的节点(Bob),窃听节点(Eve)和协作干扰

① 收稿日期:2014-01-08

作者简介:武春岭(1975-),男,河南西平人,硕士,副教授,主要从事信息安全及网格技术研究.

节点(Jamming)，其中发送节点、目的节点和窃听节点都配置单根天线，协作干扰节点配置 $N_t > 1$ 根天线. 发送节点与目的节点间的信道表示为 h_0，发送节点与窃听节点间的信道表示为 g_0，协作干扰节点与目的节点、窃听节点间的信道分别表示为 $\mathbf{h} \in \mathbb{C}^{1\times N_t}$ 和 $\mathbf{g} \in \mathbb{C}^{1\times N_t}$. 发送节点发送的信号为 $\sqrt{P_s}x$，其中 P_s 为发送节点的发送功率，x 为发送的符号且 $E\{|x|^2\}=1$. 协作干扰节点发送与消息信号相互独立的噪声信号 $\mathbf{s}$，其中 $\mathbf{s} \sim CN(0, P_j\Sigma)$，$P_j$ 为协作干扰节点的发送功率，Σ 为功率归一化后的噪声输入协方差矩阵，即 $\Sigma \succeq 0$ 且 $\mathrm{Tr}(\Sigma) \leqslant 1$. 因此，目的节点和窃听节点接收到的信号可以分别数学表示为

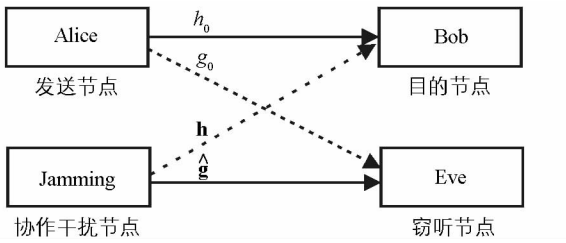

图1 系统模型

$$y_b = \sqrt{P_s}h_0x + \mathbf{hs} + n_b \tag{1}$$

$$y_e = \sqrt{P_s}g_0x + \mathbf{gs} + n_e \tag{2}$$

其中，n_b 和 n_e 分别为目的节点 Bob 和窃听节点 Eve 端的加性高斯白噪声. 在不失一般性的前提下为简单起见，假设 $E\{|n_b|^2\} = E\{|n_e|^2\} = N_0$.

协作干扰节点可以通过目的节点信息反馈的方式获取其到目的节点的准确信道矩阵 $\mathbf{h}$，然而窃听节点不会反馈信道状态信息到协作干扰节点，因此其只能通过信道估计的方式估计其到窃听节点的部分信道矩阵 $\hat{\mathbf{g}}$，信道误差矩阵可以定义为[7]

$$\Delta\mathbf{g} = \mathbf{g} - \hat{\mathbf{g}} \tag{3}$$

其中，$\mathbf{g}$ 为协作干扰节点到窃听节点的准确信道矩阵，假设估计的信道误差矩阵满足边界约束条件 $\beta = \{\Delta g : \|\Delta g\|^2 \leqslant \varepsilon^2\}$.

根据文献[3]，窃听信道的可达安全速率表示为发送节点与目的节点间互信息与发送节点与窃听节点间互信息的差值. 因此，存在协作干扰节点窃听信道的可达安全速率可以数学描述如下

$$R = [I(x; y_b) - I(x; y_e)]^+ \tag{4}$$

其中，$[x]^+ = \max\{0, x\}$.

最差情况最优化的方法是近年来鲁棒波束形成的一个重要发展方向. 由于真实的信道误差矩阵属于一个集合，该方法对这个集合中的最差情况进行优化，因此在集合中其他信道误差情况下所得到的结果都不会差于这个优化结果. 因此，对于所有的信道误差可能，最差情况方法得到波束形成算法的性能都不会太差，从而实现鲁棒性的目的. 本文研究最差情况下的可达安全速率最大化问题，首先通过信道误差矩阵 $\Delta\mathbf{g}$ 在确定的误差范围内变化求得可达安全速率的最小值(即最差情况)，然后通过优化噪声输入协方差矩阵 Σ 使得可达安全速率最大化. 因此，最差情况下可达安全速率最大化的优化问题可数学表述为

$$\begin{aligned} R_{opt} = &\max_{\Sigma}\min_{\Delta\mathbf{g}\in\beta} R(\Sigma, \Delta\mathbf{g}) \\ &\text{s.t. } \Sigma \succeq 0 \\ &\mathrm{Tr}(\Sigma) \leqslant 1 \end{aligned} \tag{5}$$

其中，$\gamma_0 = \dfrac{P_s}{N_0}$，$\gamma_j = \dfrac{P_j}{N_0}$，

$$R(\Sigma, \Delta\mathbf{g}) = \log\left(1 + \frac{\gamma_0 |h_0|^2}{\gamma_j \mathbf{h}\Sigma\mathbf{h}^\dagger + 1}\right) - \log\left(1 + \frac{\gamma_0 |g_0|^2}{\gamma_j (\hat{\mathbf{g}} + \Delta\mathbf{g})\Sigma(\hat{\mathbf{g}} + \Delta\mathbf{g})^\dagger + 1}\right)$$

优化问题的目标函数 $R(\Sigma, \Delta\mathbf{g})$ 为2个对数函数的差且信道误差矩阵 Δ 的数目有无穷多个，因而此优化问题是一个非凸优化问题[8]. 非凸优化问题在数学上很难直接求解，为求解此非凸问题，我们首先利用数学中 S-procedure 引理将非凸优化问题转化为容易求解的半定规划问题，然后通过一维搜索算法求得问题的最优解.

2　问题求解及算法设计

考虑对数函数的单调性，当 $\gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}$ 为常值 z 时，很明显公式描述的最大化最差情况下的可达安全速率等价于表达式 $(\hat{\mathbf{g}}+\Delta\mathbf{g})\sum(\hat{\mathbf{g}}+\Delta\mathbf{g})^{\dagger}$ 的最大最小化问题，此问题便于求解. 因此，非凸问题的求解可以分两步完成：第一步假设 $z=\gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}$ 为常数，求解对应的等价问题；第二步利用一维搜索算法根据 z 的变化搜索最优解. 下面我们首先令 $\gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}=z$ 为常数，此时优化问题等价于

$$\begin{aligned} F(z)=\max_{\Sigma}\min_{\Delta\mathbf{g}\in\beta}(\hat{\mathbf{g}}+\Delta\mathbf{g})\sum(\hat{\mathbf{g}}+\Delta\mathbf{g})^{\dagger} \\ \text{s. t. } \Sigma\geqslant 0 \\ \mathrm{Tr}(\Sigma)\leqslant 1 \\ \gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}=z \end{aligned} \tag{6}$$

此时，优化问题中的目标函数是一个包含无穷多个信道误差矩阵 $\Delta\mathbf{g}$ 的非凸优化问题，仍然无法直接求解. 为此，我们推导出下面的等价定理 1.

定理 1　非凸优化问题等价于下面的半定规划问题.

$$\begin{aligned} F(z)=\max_{\Sigma,\mu,\varphi}\mathrm{Tr}(\Sigma\hat{\mathbf{g}}^{\mathrm{H}}\hat{\mathbf{g}})-\varphi-\mu\varepsilon^{2} \\ \text{s. t. }\begin{bmatrix}\mu\mathbf{I}_{N_h}+\Sigma & \Sigma\hat{\mathbf{g}}^{H}\\ \hat{\mathbf{g}}\Sigma & \varphi\end{bmatrix}\geqslant 0 \\ \Sigma\geqslant 0 \\ \mathrm{Tr}(\Sigma)\leqslant 1 \\ \gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}=z \end{aligned} \tag{7}$$

证　引入辅助变量 v，优化问题可以等价转化为

$$\begin{aligned} \max_{\Sigma,v} v \\ \text{s. t. }(\hat{\mathbf{g}}+\Delta\mathbf{g})\sum(\hat{\mathbf{g}}+\Delta\mathbf{g})^{H}\geqslant v,\ \forall\Delta\mathbf{g}:\ \|\Delta\mathbf{g}\|^{2}\leqslant\varepsilon^{2} \\ \Sigma\geqslant 0 \\ \mathrm{Tr}(\Sigma)\leqslant 1 \\ \gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger}=z \end{aligned} \tag{8}$$

问题(8) 的第一个约束项可以表示为

$$\Delta\mathbf{g}\Sigma\Delta\mathbf{g}^{H}+2\mathrm{Re}(\hat{\mathbf{g}}\Sigma\Delta\mathbf{g}^{H})+\hat{\mathbf{g}}\Sigma\mathbf{g}^{H}-v\geqslant 0 \tag{9}$$

根据信道误差矩阵满足边界约束条件，得

$$\forall\Delta\mathbf{g}:\ -\Delta\mathbf{g}\Delta\mathbf{g}^{H}+\varepsilon^{2}\geqslant 0 \tag{10}$$

根据文献[9] 中的 S-procedure 定理，和成立当且仅当存在 $\mu\geqslant 0$，使得下面的表达式成立

$$\begin{bmatrix}\mu\mathbf{I}_{N_h}+\Sigma & \Sigma\hat{\mathbf{g}}^{\mathrm{H}}\\ \hat{\mathbf{g}}\Sigma & \hat{\mathbf{g}}\Sigma\hat{\mathbf{g}}^{\mathrm{H}}-\mu\varepsilon^{2}-v\end{bmatrix}\geqslant 0 \tag{11}$$

令 $\varphi=\hat{\mathbf{g}}\Sigma\hat{\mathbf{g}}^{\mathrm{H}}-\mu\varepsilon^{2}-v$，其中 $\varphi\geqslant 0$，此时优化问题可以表示为

$$\begin{aligned} \max_{\Sigma,\mu,\varphi}\hat{\mathbf{g}}\Sigma\hat{\mathbf{g}}^{\mathrm{H}}-\mu\varepsilon^{2}-\varphi \\ \text{s. t. }\begin{bmatrix}\mu\mathbf{I}_{N_h}+\Sigma & \Sigma\hat{\mathbf{g}}^{H}\\ \hat{\mathbf{g}}\Sigma & \varphi\end{bmatrix}\geqslant 0 \\ \Sigma\geqslant 0 \end{aligned} \tag{12}$$

$$\mathrm{Tr}(\Sigma) \leqslant 1$$
$$\gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger} = z$$

证毕.

优化问题(7)是由凸目标函数和一些线性矩阵不等式约束项构成的半定规划问题[10]. 半定规划问题为凸优化问题,因此此问题的最优噪声输入协方差矩阵 Σ^* 很容易通过经典的半定规划求解方法,比如内点法求解. 同时也可以使用 Matlab 工具箱 CVX 直接求解.

定理1是在假设 $\gamma_j \mathbf{h}\Sigma\mathbf{h}^{\dagger} = z$ 为常数的前提下得到的,下面计算 z 的取值范围,从而可以通过 z 在取值范围内的变化,连续调用定理1求出系统的最大可达安全速率. 因为 $\mathbf{h}\Sigma\mathbf{h}^{\dagger} \leqslant \|\mathbf{h}\|^2 \lambda_{\max}(\Sigma) \leqslant \|\mathbf{h}\|^2 \mathrm{Tr}(\Sigma) \leqslant \|\mathbf{h}\|^2$,并且不等式取得等号的条件是 $\Sigma = \dfrac{\mathbf{h}^{\dagger}\mathbf{h}}{\|\mathbf{h}\|^2}$ 成立. 因此,z 的取值范围为

$$0 \leqslant z \leqslant \gamma_j \|\mathbf{h}\|^2 \tag{13}$$

根据定理1和(13)式,最差情况下最大化可达安全速率的优化问题(5)等价于下面的优化问题(14)

$$R_{opt} = \max_{z} \log\left(1 + \frac{\gamma_0 |h_0|^2}{z+1}\right) - \log\left(1 + \frac{\gamma_0 |g_0|^2}{\gamma_j F(z) + 1}\right) \tag{14}$$
$$\text{s.t. } 0 \leqslant z \leqslant \gamma_j \|\mathbf{h}\|^2$$

根据对数函数的单调性以及文献[11]可知优化问题(14)的目标函数是关于 z 的凹函数,同时约束项是关于 z 的线性函数,因此该优化问题为容易求解的凸优化问题.

根据上文的分析和推导,本文提出了求解原优化问题(5)的一维搜索算法.

算法1(一维搜索算法)

步骤1:初始化 $z = 0$,迭代步长 λ;

步骤2:对于给定的 z,根据定理1求解 $F(z)$;

步骤3:把 z 和 $F(z)$ 代入式求得 $R_{opt}(z)$;

步骤4:更新 $z \Leftarrow z + \lambda$ 并返回步骤2,直到 $\gamma_{cj} \|\mathbf{h}\|^2 - z \leqslant \delta$;

步骤5:最优解 $R_{opt} = \max\limits_{z \in [0:\ \lambda:\ \gamma_j \|\mathbf{h}\|^2]} R_{opt}(z)$.

该算法分为5步:步骤1为初始化参数 z 和 λ,其中 λ 为迭代步长,控制着参数 z 的更新精度;步骤2主要根据给定的 z 和定理1,利用CVX求解最优的 $F(z)$;步骤3根据步骤2得到的 $F(z)$,利用公式求得给定 z 情况下最大的可达安全速率 $R_{opt}(z)$;步骤4主要是更新 z 的值以及判断算法是否收敛,收敛的判断标准是 $\gamma_{cj} \|\mathbf{h}\|^2 - z \leqslant \delta$,其中 δ 为控制收敛精度非常小的正常数,如果判断算法未收敛,则跳到步骤2继续迭代,反之收敛则跳转到步骤5;步骤5主要是从步骤3中产生的 $R_{opt}(z)$ 中选出最大的可达安全速率 R_{opt}.

3 仿真结果

本节设计了仿真实验来验证本文提出的鲁棒波束成形噪声发送策略的良好性能. 本文考虑 WSNs 节点间的窃听模型为高斯窃听信道,协作干扰节点的天线数 $N_t = 2$. 假设发送节点到窃听节点的窃听链路比到目的节点的目的链路质量好,例如 $h_0 = 0.62 + 0.90i$,$g_0 = 1.12 - 1.23i$,此时若无协作干扰者节点的辅助,WSNs 节点间是无法进行安全通信的,即可达安全速率为0. 除此之外,假设信道矩阵由服从0均值单位方差的复高斯随机变量组成,噪声方差 $N_0 = 1$.

图2为可达安全速率取值与变量 z 的关系图. z 的定义域由公式(13)确定. 仿真中设置发送节点的发送功率 $P_s = 10$ dB,协作干扰节点的发送功率 $P_j = 10$ dB. 针对某一确定的信道误差 ε^2,通过算法1计算出 $R_{opt}(z)$,从而观察变量 z 对 $R_{opt}(z)$ 的影响. 从仿真结果中可以看出,可达安全速率 $R_{opt}(z)$ 是关于 z 的凹函数,对应每个 ε^2 都存在唯一最大可达安全速率.

图3为协作干扰节点鲁棒波束成形噪声发送策略的性能仿真结果. 仿真中设置发送功率 P_s 的变化范围为[0, 20 dB],协作干扰节点的发送功率 $P_j = 10$ dB. 从仿真结果中可以看出,当固定发送节点的发送功率和协作干扰节点的发送功率相同时,信道误差 ε^2 越大,WSNs 节点间的可达安全速率就越低. 另一方面,系统的可达安全速率会随着发送节点发送功率的增加而变大. 同时,从仿真结果中可以看出,当窃听链路好

于目的链路时，文献[6]所提的不采用协作干扰节点策略所对应的可达安全速率为 0，即无法实现安全通信.

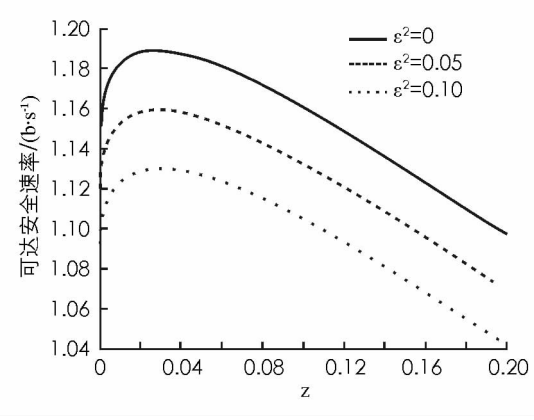

图 2　z 对可达安全速率的影响

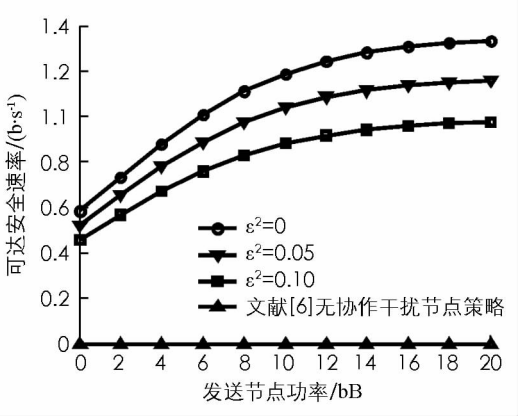

图 3　发送节点功率对可达安全速率的影响

本文所提鲁棒波束设计方法与文献[7]提出的非鲁棒波束设计方法的性能对比结果如图 4 所示. 仿真中设置发送功率 $P_s = 10$ dB，协作干扰节点的发送功率 $P_j = 10$ dB，信道误差 ε^2 的变化范围为[0，0.1]. 可达安全速率的上界是信道误差为 $\varepsilon^2 = 0$ 时系统的最大可达安全速率. 从仿真结果中可以看出，在信道误差为 0 时，本文所提鲁棒波束设计方法和文献[7]所提的非鲁棒设计方法都可以达到可达安全速率的上界. 但随着信道误差 ε^2 的变大，两种设计方法所能实现的可达安全速率都会减小，但文献[7]所提的非鲁棒设计方法对应的可达安全速率降低的非常迅速，而本文所提的鲁棒设计方法所对应的可达安全速率降低得非常缓慢. 同时，这一现象随着信道误差 ε^2 的变大显得更加明显，例如在 $\varepsilon^2 = 0.05$ 时，本文所提鲁棒波束设计方法所能实现的可达安全速率为 1.12 bit/s/Hz，文献[7]所能实现的可达安全速率为 0.95 bit/s/Hz，二者差值为 0.17 bit/s/Hz，但当 ε^2 增加到 0.1 时，二者的差值已经变为 0.3 bit/s/Hz. 因此，从仿真结果中我们可以看出，本文所提的鲁棒波束设计方法具有很强的鲁棒性，在信道误差非常大的情况下依然可以实现良好的安全性能.

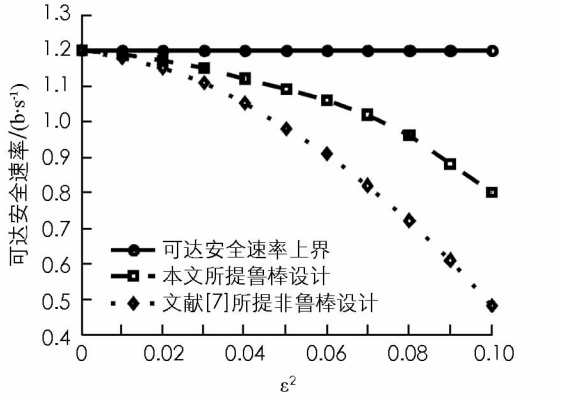

图 4　信道误差 ε^2 对可达安全速率的影响

4　结　　语

通过协作干扰节点发送噪声的方式可以提高 WSNs 节点间的可达安全速率. 当协作干扰节点只知道其到窃听节点的部分信道状态信息和信道误差范围的情况下，本文采用最差情况下最大化系统的可达安全速率为设计准则，得到最优的噪声输入协方差矩阵. 此优化问题是一个很难直接求解非凸优化问题，本文首先通过一些数学等价转化将该非凸优化问题转化为半定规划问题，然后设计了一维搜索算法来计算最大的可达安全速率. 最后，通过仿真说明本文提出的协作干扰节点鲁棒波束成形噪声发送策略，可以明显提高 WSNs 节点间通信的可达安全速率.

参考文献：

[1] ZIOPOULOS M. A Survey on Jamming Attacks and Countermeasures in WSNs [J]. IEEE Communications Surveys & Tutorials, 2009, 11(4): 42－56.

[2] HEALY, NEWE M T, LEWIS E. Security for Wireless Sensor Networks: A Review [C]. Perpignan: IEEE Sensors Applications Symposium, 2009: 80－85.

[3] WYNER A. The Wire-Tap Channel [J]. Bell Systems Technical Journal, 1975, 54(8): 1355－1387.

[4] CSISZÁR I, KÖRNER J. Broadcast Channels With Confidential Messages [J]. IEEE Trans Inf Theory, 1978, 24(3):

339－348.
[5] Al-SAKIB K P. Security in Wireless Sensor Networks: Issues and Challenges [C]. Phoenix Park: The 8th International Conference on Advanced Communication Technology, 2006: 1043－1048.
[6] ISLAM M R. Secrecy Capacity Analysis in a Cooperative MIMO Based Wireless Sensor Network [C]. Fhaka: International Conference on in Computer and Information Technology , 2011: 595－600.
[7] ROHOKALE V M, PRASAD N R. Cooperative Jamming for Physical Layer Security in Wireless Sensor Networks [C]. Taipei: International Symposium in Wireless Personal Multimedia Communications, 2012: 458－462.
[8] BOYD S, VANDENBERGHE L. Convex Optimization [M]. New York: Cambridge Univ. Press, 2004: 127－146
[9] BJÖRNSON E, ZHENG G. Robust Monotonic Optimization Framework for Multicell MISO Systems [J]. IEEE Transactions on Signal Processing, 2012, 60(5): 2508－2523.
[10] JIAHENG W, PALOMAR D P. Worst-Case Robust MIMO Transmission with Imperfect Channel Knowledge [J]. IEEE Transactions on Signal Processing, 2009, 57(8): 3086－3100.
[11] ZHENG G, WONG K K, OTTERSTEN B. Robust Cognitive Beamforming with Bounded Channel Uncertainties [J]. IEEE Transactions on Signal Processing, 2009, 57(12): 4871－4881.

On Achievable Secrecy Rate in WSNs Based on Robust Beamforming

WU Chun-ling, LU Xian-zhi, LI He-hua
College of Computer, Chongqing College of Electronic Engineering, Chongqing 401331, China

Abstract: Aiming at the problem that wireless communication between nodes is vulnerable to eavesdropping in WSNs, robust beamforming has been designed to realize noise transmitting strategy in the cooperative jamming node, which can improve the achievable secrecy rate. Under the worst channel case, the achievable secrecy rate is maximized by optimizing the noise input covariance matrix of the cooperative jamming node. To tackle this challenging non-convex max-min optimization issue, we have first transferred this non-convex optimization problem into an equivalent semi-definite programming problem, and then proposed a one-dimensional algorithm to calculate the optimal achievable secrecy rate. Simulation results verify the effectiveness of the proposed approach.

Key words: wireless sensor networks (WSNs); achievable secrecy rate; cooperative jamming; non-convex optimization; robust beamforming

责任编辑 夏 娟