一种基于博弈的联盟组网方法

黄开枝 洪 颖* 罗文宇 林胜斌
(国家数字交换网络工程技术研究中心 郑州 450002)

摘 要：针对缺乏有效联盟收益分配机制，导致发送端拒绝协作，同时发送信号，造成接收端信号重叠，该文提出一种基于博弈的安全联盟组网方法。首先，将协作博弈机制中的收益分摊机制引入安全联盟组网自适应形成方法，建立发送端联盟组网模型。然后，为实现联盟方式组网，基于博弈方法将联盟组网相比非联盟时增加的总安全速率作为可转移的收益函数，平均分配给组网内各个发送端；之后，发送端遍历所有可能形成的联盟组网，得到均摊收益最大的联盟组网方式；最后，发送端自适应形成该联盟组网，无需发送信号或相同需求下窃听信道条件最坏的发送端发信号，其余所有发送端通过发送人工噪声进行协作。仿真分析验证了该方法的公平性和有效性，当发送端功率等于20 mW时，高斯信道下的网络平均安全速率相比初始状态提高1.8 bit/(s·Hz)。

关键词：无线通信；安全速率；合作博弈；人工噪声；联盟组网
中图分类号： TN915.08 **文献标识码**： A **文章编号**：1009-5896(2015)07-1562-07
DOI: 10.11999/JEIT141204

Security Coalition Method Based on Game Theory

Huang Kai-zhi Hong Ying Luo Wen-yu Lin Sheng-bin
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: For the problems of reduced secrecy rate and energy according to noncooperation of selfish relay, this paper presents a security coalition method based on the game theory. Firstly, this paper introduces a benefit-sharing mechanism of cooperative game for the adaptive security coalition method, and models the transmitter coalition. And then this paper makes the increased part of total network secrecy rate compared with the initial as the transferable benefit, and allocates it to all transmitters in the coalition. After that, the transmitters iterate through the average utility under all coalitions, and find the largest benefit coalition. Finally, this coalition of transmitters is formed autonomously, the transmitter which is badly in need of sending signal or the transmitter with the worst eavesdropping channel conditions under the same need sends signal, the rest cooperate by sending artificial noise. Simulations and analyses show the fairness and effectiveness of this method, when sending power is 20 mW, the average network secrecy rate under the Gaussian channel compared with the initial stated is improved by 1.8 bit/(s·Hz).

Key words: Wireless communication; Secrecy rate; Cooperative game; Artificial noise; Coalition group

1 引言

近年来，无线与移动通信已快速发展成为全球范围内用户规模和使用量最大的一种通信方式，各种新型的宽带无线与移动通信技术研究也在全球范围内紧锣密鼓地加速推进，期望能以更快的速度、更大的容量、更低的成本给各类用户提供更丰富的业务。协作通信网络能有效地利用无线网络的广播特性，并且通过中继节点协作得到空间分集增益，提高无线链路的传输速率及传输可靠性，增加系统的覆盖范围和系统的鲁棒性，成为当前的研究热点之一。安全问题是协作通信网络能否给用户提供稳定可靠服务的关键问题，中继节点和协作思路的引入给安全性带来了极大的隐患，同时也为其安全问题研究带来了新的机遇。传统上主要采取直接移植有线通信系统中的方法，在“信息层面”采用信源加密来避免信息泄露。该类方法不仅回避了无线信号本身易被截获的问题，而且在协作通信网络中还面临密码设备管理、密钥管理、密钥分发困难等一系列问题。针对这些问题，近年来兴起的物理层安全技术从无线通信的物理层特点入手，利用无线信道在空时频域的多样性、时变性和私有性，为协作通信网络的安全传输方法设计提供了新的思路，成

2014-09-15 收到，2014-12-04 改回，2015-05-08网络优先出版
国家自然科学基金(61379006)资助课题
*通信作者：洪颖 hongyinghunan@126.com

为近年来无线协作通信安全的研究热点[1−6]。

基于博弈的物理层安全协作技术近年来得到了广泛的研究，通过基于博弈的方法分析获取各个节点间的关系，多个发送端可以形成联盟提高各自的安全速率，从而解决无线网络的安全问题。技术的中心原则是将发送端建模成理性的参与者，建模目标为最大化各自的收益函数。2009 年，文献[7]针对多发送端无线网络，提出了一个基于多发送端协作的分布式联盟博弈理论架构，组网内发送端分时隙协作放大转发信号，通过比较各个发送端的加入是否能够增加组网安全速率收益从而决定协作组网的形成。文献[8]研究了多用户 MISO(Multiple-Input Single-Output)干扰信道的可达安全速率，通过反复算法得到纳什均衡。文献[9]与文献[10]研究用户高斯干扰信道场景下的多个协作和非协作的发送机制，推导出各个机制的可达安全速率，并提出将博弈作为解决问题工具，这样发送端可以寻找到平衡网络安全性能和公平的可控点。2013 年，文献[11]中，各个多天线发送端都希望最大化其安全速率和其他链路安全速率的差距，得到闭合形式的纳什均衡点。文献[12]采用协作博弈解决异构网络中安全速率的提高问题，当用户形成联盟，通过协作波束成形使得窃听方信号无效。文献[13]研究了考虑多用户非协作功率控制博弈，并应用价格函数来提高能量效率和整个网络的总安全速率。但是，现有方法缺乏有效联盟收益分配机制，可能导致发送端拒绝协作，同时发送信号，造成接收端信号重叠的问题出现[14]。因此，有必要在无线协作网络中实施有效的协作联盟收益机制，实现多个发送端之间的协作，保证协作通信网络的稳定和高效[15]。

针对此问题，本文提出了一种基于博弈的联盟组网方法：通信需求最强的发送端发送信号，当所有发送端需求相同时，窃听信道状态信息最差的发送端发送信号，其余发送端在其零空间上发送人工噪声，既避免了多个发送端之间相互干扰，又恶化了窃听端的接收；为实现这一联盟组网，本文使用虚拟货币量化安全速率，基于博弈将协作联盟增加的安全速率增益均分，发送端的收益定义为非协作时的安全速率增益加上联盟组网系统总安全速率增益增加部分的平均值，当网络中某个发送端 T' 临时有强烈信号传输需求时，可以通过增加自身安全速率单位价格，达到分摊收益的最大值；各个发送端通过遍历所有联盟组网方式下的收益，自适应形成收益最大的联盟组网，这时各个发送端的收益达到最大值，不会有节点脱离组网。仿真结果表明：当发送端功率为 2~20 mW 时，基于本文方法下的网络平均安全速率相比初始状态提高 0.4~1.8 bit/(s·Hz)。

2　系统模型与问题提出

如图 1 所示，系统模型包含 N 对发送端-接收端(Alice-Bob)和 L 个窃听方(Eve)，其中 $L<N$，是一个无中继参与的多发送端无线协作网络。定义发送端集合为 $\Omega=\{T_1,T_2,\cdots,T_n\}$，发送端到接收端的主信道特征参数为 $h=1$，发送端到窃听方的窃听信道特征参数为 g，该尺度参数可以作为窃听方到接收端的相关距离的标志。此信道中某个发送端 T_i，$T_i\in\Omega$ 的安全速率为主信道和窃听信道的容量之差。

$$C_i=\left[C_{i,d}-C_{i,e}\right]^+ \tag{1}$$

其中，$C_{i,d}$ 表示发送端到合法接收端的主信道容量，$C_{i,e}$ 表示发送端到窃听端的窃听信道容量。$[\ ]^+$ 表示取正的最大值。

如图 1(a)所示，处于相同频段的 N 个发送端同时发信号，接收端接收的信号相互干扰，其中，T_i 的安全速率为

$$C_{T_i}^{NC}=\left[\log_2\left(1+P_i\Big/\left(\sum_{j\neq i}^{n}P_j+1\right)\right)-\log_2\left(1+g_i^*P_i\Big/\left(\sum_{j\neq i}^{n}P_jg_j+1\right)\right)\right]^+ \tag{2}$$

其中，g_i^* 表示 T_i 的窃听信道增益，g_j 表示其余发送端对应的窃听信道增益，P_i 和 P_j 表示所有发送端发送功率且相等。由于信道的叠加性导致接收端信号相互干扰，系统的安全性不高。

如果发送端互相协作，可以通过人工噪声的协作策略获得安全速率的提升。各个发送端之间通过控制信道交换各自的信道状态信息和发送需求(现有将博弈论应用在物理层安全技术的文献中关于协作双方通信的实现均做此假定)，通过检测感知功率可以判断发送端是否协作干扰。然而，出于自私的意图，一些节点可能会拒绝协作。因此，研究有效的协作联盟收益机制促进多个节点之间的协作，具有非常重要的意义。

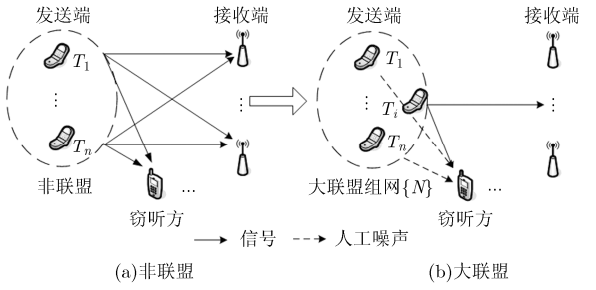

图 1　发送端的非联盟与联盟组网模型

3 基于合作博弈多用户联盟组网自适应形成方法

为实现多个发送端之间的协作，本节将协作博弈机制中的收益分摊机制引入多用户联盟组网自适应形成方法，将联盟组网相比非协作增加的总安全速率收益值均分。首先，得出联盟状态下的系统安全速率；然后，将联盟状态下系统总安全速率相对无协作时的增量作为可转移收益，基于博弈将平均分摊转移到联盟组网内各个发送端；最后，发送端遍历所有可能形成的联盟组网，计算得到均摊收益最大的联盟组网方式 G_*，并按照 G_* 的形成结构自适应形成联盟组网，此时各个发送端的收益值达到最大。

3.1 大联盟组网的安全速率

首先，得出联盟状态下的系统安全速率。用 $\{N\}$ 表示包含所有发送端的大联盟。当 T_i 发送信号时，其余发送端将噪声置于其主信道的零空间上发送，可以在降低窃听信道容量的同时不影响接收端的接收。如图 1(b)所示，所有发送端通过这种协作方式形成一个大联盟组网 $\{N\}$，那么 T_i 的安全速率为

$$C_{T_i}^{\{N\}}=\left[\log_2(1+P_i)-\log_2\left(1+g_iP_i\Big/\left(\sum_{j\neq i}^{N}P_jg_j+1\right)\right)\right]^+ \tag{3}$$

为使 $C_{T_i}^{\{N\}}$ 达到最大，发送信号发送端的窃听信道增益满足 $g_i^*=\arg\max C_{T_i}^{C_K}$，易得 g_i^* 为所有发送端窃听信道增益的最低值，即

$$g_i^*=\min\ g_i,\ \ i\in\{1,2,\cdots,N\} \tag{4}$$

对比式(2)和式(3)得到，$\max\ C_{T_i}^{\{N\}}>\max\ C_{T_i}^{NC}$，通过联盟组网的方式可以提高网络的安全性。

为促进发送端相互协作形成联盟组网，本节根据发送端的相互协作关系构建一个可转移收益协作博弈，将组网总的安全速率相对无协作时的增量作为可转移收益，将其转移到联盟组网内各个发送端。然后，基于博弈将可转移收益平均分摊，保证各个发送端收益配置的均衡和公平，从而实现组网内各个发送端的协作。

3.2 安全速率收益分摊

首先，根据发送端的相互协作关系构建一个可转移收益协作博弈，将组网安全速率相对无协作时的安全速率增量作为可转移收益，为实现收益的转移性，本节使用虚拟货币量化安全速率，用 ρ 表示每单位安全速率货币价格。

$$v(G_i)=D_{T_*}^{G_i}=\rho C_{T_*}^{G_i} \tag{5}$$

其中，$C_{T_*}^{G_i}$ 表示联盟 G_i 内窃听信道增益最低的 T_* 发送信号的安全速率，T_* 可以通过虚拟货币将收益转移给发人工噪声的发送端，各个发送端的收益用 $u_i^{G_i}$ 表示，并满足

$$\sum_{i\in G_i}u_i^{G_i}=v(G_i) \tag{6}$$

其中，$v(G_i)$ 为联盟组网 G_i 的总收益。对于最优联盟内 $\forall\ T_i\in G_*$，都有 $u_i^{G_*}\geq v(i)$，$v(i)$ 表示 T_i 不加入 G_* 时可以得到最大的收益。当发送端在联盟组网 G_* 中获得的收益比非联盟以及加入其他联盟得到的收益多时，它才会愿意加入该联盟。

定义 1 协作博弈 $\langle N,v\rangle$，其中 N 为所有发送端的集合，特征函数 $v(G_i)$ 为每种联盟方式确定的联盟值，如果对于任意两个联盟 $G_j,G_k\subset\{N\}$ 且 $G_j\cap G_k=\varnothing$，如果特征函数 G_j，G_k 满足 $v(G_j\cup G_k)\geq v(G_j)+v(G_k)$，那么该博弈是超可加的。

在可转移收益博弈中，$v(G_j)$ 和 $v(G_k)$ 分别为联盟组网 G_j，G_k 的安全速率。其中，

$$v\left(G_j\right)=\rho C_{T_*}^{G_j}=\rho\left[\log_2\left(1+P_i\Big/\left(\sum_{j\notin G_j}^{N}P_j+1\right)\right)-\log_2\left(1+g_i^*P_i\Big/\left(\sum_{j\neq i}^{N}P_jg_j+1\right)\right)\right]^+ \tag{7}$$

$$v(G_k)=\rho C_{T_*}^{G_k}=\rho\left[\log_2\left(1+P_i\Big/\left(\sum_{j\notin G_k}^{N}P_j+1\right)\right)-\log_2\left(1+g_i^*P_i\Big/\left(\sum_{j\neq i}^{N}P_jg_j+1\right)\right)\right]^+ \tag{8}$$

$$\begin{aligned}v\left(G_j\cup G_k\right)&=\rho C_{T_*}^{G_j\cup G_k}\\&=\rho\left[\log_2\left(1+P_i\Big/\left(\sum_{j\notin G_j\cup G_k}^{N}P_j+1\right)\right)-\log_2\left(1+g_i^*P_i\Big/\left(\sum_{j\neq i}^{N}P_jg_j+1\right)\right)\right]^+\end{aligned} \tag{9}$$

如果满足 $v(G_j\cup G_k)\geq v(G_j)+v(G_k)$，那么联盟组网 G_j 和 G_k 将合并成一个大联盟。通过数学推导，易得发送端任意联盟组网都满足 $v(G_j\cup G_k)\geq v(G_j)+v(G_k)$，该协作博弈下的联盟组网满足超可加性，所以包含所有发送端的大联盟 $\{N\}$ 的安全速率最大，即 $G_*=\{N\}$。

若 N 个发送端不协作时，各个发送端发送各自信号的收益 $v(i)$ 为

$$U_{NC}\left\{D_{T_1}^{NC},D_{T_2}^{NC},\cdots,D_{T_N}^{NC}\right\} \tag{10}$$

其中，$u_i^{NC}=D_{T_i}^{NC}=\rho C_{T_i}^{NC}$，$T_i\in N$。

当 M（$M\leq N$）个发送端形成联盟组网 G_i 时，窃听信道增益最低的 T_* 发送信号，其余发送端发送人

工噪声，此时组网的安全速率收益为

$$D_{T_*}^{G_i} = \max\ D_{T_i}^{G_i},\ T_* \in G_i \tag{11}$$

M 个发送端的收益分摊方案 $\{u_1^{G_i}, u_2^{G_i}, \cdots, u_M^{G_i}\}$ 满足

$$u_1^{G_i} + u_2^{G_i} \cdots + u_M^{G_i} = D_{T_*}^{G_i} \tag{12}$$

相对非协作可以增加的总收益函数为

$$\Delta = D_{T_*}^{G_i} - \sum_{i=1}^{M} D_{T_i}^{NC} \tag{13}$$

在联盟发送端中平均分摊 Δ，$\Delta_i = \Delta / M$。各个发送端通过分摊得到的收益为

$$\begin{aligned} U_{G_i} &= \left\{u_1^{G_i}, u_2^{G_i}, \cdots, u_M^{G_i}\right\} \\ &= \left\{D_{T_1}^{NC} + \left(D_{T_*}^{G_i} - \sum_{i=1}^{M} D_{T_i}^{NC}\right)\Big/ M,\right. \\ &\quad D_{T_2}^{G_i} + \left(D_{T_*}^{G_i} - \sum_{i=1}^{M} D_{T_i}^{NC}\right)\Big/ M, \cdots, \\ &\quad \left. D_{T_m}^{G_i} + \left(D_{T_*}^{G_i} - \sum_{i=1}^{M} D_{T_i}^{NC}\right)\Big/ M\right\} \end{aligned} \tag{14}$$

其中，$u_i^{G_i} = D_{T_*}^{NC} + \Delta / M, T_i \in N$。

3.3 联盟自适应形成步骤

可见，基于协作博弈联盟组网自适应形成方法分两个分阶段：第 1 阶段，发送端遍历所有可能的联盟组网方式，得到分摊收益 Δ / M 最大的联盟组网方式 $\{N\}$；第 2 阶段，发送端按照 $\{N\}$ 的构成，当 $(\Delta / M)_{\{N\}} > 0$ 时，自适应形成联盟组网，窃听信道增益最低的 T_* 发送信号，其余发送端发送人工噪声。

第 1 阶段是寻找最优联盟组网方式：根据联盟组网特征函数值 $v(\{N\})$，各个发送端通过最大收益函数算法计算得到最好的联盟方式 $\{N\}$，具体步骤如表 1 所示。

由定义 1 知道，发送端的协作博弈具有超可加性，所以，最好的联盟组网方式为 $\{N\}$，$M = N$。在所有的联盟组网方式中，由所有发送端组成的大联盟能获得最大收益。

表 1 寻找最优联盟组网步骤

(1)寻找所有可以协作的发送端 $N = \{T_1, T_2, \cdots, T_n\}$；
(2)遍历包含所有发送端的各种可能联盟组网方式；
(3)计算各种联盟组网下的特征函数 $v(G_i)$，从而得到分摊收益 $\Delta / M_{\{G_i\}}$；
(4)找到最好的联盟组网方式 $\{N\}$，$\{N\} = \arg\max\ \Delta / M$。

第 2 阶段是最优大联盟组网自适应形成：发送端从初始的非联盟状态，经过以下步骤自适应形成系统安全速率最大的 $\{N\}$，具体步骤如表 2 所示。

表 2 最优大联盟组网形成步骤

(1)计算最优大联盟组网下各个发送端的收益 $u_i^{C_N}$；
(2)对比大联盟下的收益值 $u_i^{C_N}$ 与非协作的收益值 u_i^{NC}。若 $u_i^{C_N} \ge u_i^{NC}$，则加入大联盟；若 $u_i^{C_N} < u_i^{NC}$，则脱离联盟；
(3)组网内发送端按照协作协议，窃听信道条件最坏的 T_* 发送信号，其余发送端在 T_* 的主信道零空间上发送噪声；
(4)当有新的发送端进入该网络，则回到步骤(1)；否则，回到步骤(3)。

只要 $\Delta > 0$，即满足 $u_i^{C_N} \ge u_i^{NC}$，各个发送端联盟下的收益大于非联盟时的收益，发送端就能形成大联盟组网。即

$$\begin{aligned} \Delta = \rho\Bigg\{&\log_2(1+P_*) - \log_2\left(1+g_*P_*\Big/\left(\sum_{j\ne i^*}^{N} P_j g_j + 1\right)\right) \\ &- \sum_{i=1}^{N}\Bigg[\log_2\left(1+P_i\Big/\left(\sum_{j\ne i}^{N} P_j + 1\right)\right) \\ &- \log_2\left(1+g_iP_i\Big/\left(\sum_{j\ne i}^{N} P_j g_j + 1\right)\right)\Bigg]\Bigg\} > 0 \end{aligned} \tag{15}$$

化简 Δ，得

$$\begin{aligned} \Delta = \rho\Bigg\{&\log_2(1+P_*) - \sum_{i=1}^{N}\log_2\left(1+P_i\Big/\left(\sum_{j\ne i}^{N} P_j + 1\right)\right) \\ &+ \sum_{i=1, i\ne i^*}^{N}\log_2\left(1+g_iP_i\Big/\left(\sum_{j\ne i}^{N} P_j g_j + 1\right)\right)\Bigg\} = \alpha + \beta \end{aligned} \tag{16}$$

其中，$\beta = \sum_{i=1, i\ne i^*}^{N}\log_2\left(1+g_iP_i\Big/\left(\sum_{j\ne i}^{N} P_j g_j + 1\right)\right)$ 恒大于 0，所以只要满足式(17)，即能满足大联盟组网自适应形成算法的条件

$$\begin{aligned} \alpha &= \rho\left\{\log_2(1+P_{i^*}) - \sum_{i=1}^{N}\log_2\left(1+P_i\Big/\left(\sum_{j\ne i}^{N} P_j + 1\right)\right)\right\} \\ &= \rho\left\{\log_2(1+P) - N\log_2\left(1+\frac{P}{(N-1)P+1}\right)\right\} \ge 0 \end{aligned} \tag{17}$$

易得知 α 是关于功率 P 的增函数和关于联盟内发送端数量 N 的减函数。

当 $N \to \infty$ 时，只要功率 P 满足 $\log_2(1+P) - N\log_2\left(1+\dfrac{P}{NP+1}\right) \ge 0$ 时，Δ 恒大于 0，组网内发送端联盟必然形成。即

$$\alpha=\rho\left\{\log_2(1+P_{i^*})-\sum_{i=1}^{N}\log_2\left(1+P_i\Big/\left(\sum_{j\neq i}^{N}P_j+1\right)\right)\right\}$$
$$=\rho\left\{\log_2(1+P)-N\log_2\left(1+\frac{P}{(N-1)P+1}\right)\right\}$$
$$\geq 0(1+P)-\left(1+\frac{P}{NP+1}\right)^N\geq 0 \tag{18}$$

其中，P 为常数，则当 $N\to\infty$ 时，$\dfrac{P}{NP+1}\to 0$，那么根据序列的极限原则

$$\lim_{n\to\infty}(1+P)-\left(1+\frac{P}{NP+1}\right)^N=1+P-e \tag{19}$$

解得 $P>e-1$ 时，Δ 恒大于 0，当同时隙下的发送端功率大于 $e-1$ 时，基于本节的方法，发送端自动形成大联盟组网，窃听信道增益最低的发送端发送信号，组网内其他发送端在其主信道零空间上发送人工噪声，实现了网络的安全。

本文的方法也能解决网络需求公平性的问题，保证各个发送端不同的需求。

4 数值仿真与安全性能分析

为验证本文方法的有效性，对存在窃听方的无线通信网络仿真。假设该网络存在 40 对发送端-接收端，1 个窃听方。网络内每个时隙下的发送端为 $2\sim k(k\leq 4)$ 个。为了计算方便，取量化安全速率的单位 $\rho=1$，ρ 的大小不影响最终结果。窃听信道为高斯随机信道，窃听信道增益 g 取 40 个随机数值，方差为 1。

图 2 给出了网络发送端功率 P 的变化与联盟内发送端个数 k 对各个发送端联盟与非联盟收益差 Δ_i 的影响。可以看到：当发送端功率大于 1.8mW 时，Δ_i 恒大于 0，这时同时隙下的发送端都趋向于协作形成联盟组网，满足理论分析的数值 $P>e-1$。同时观察到，Δ_i 与 k 呈反比，同时隙下的发送端个数越多，基于联盟组网下增加的收益得越少；Δ_i 与 P 呈正比，各个发送端功率越大，基于联盟组网下的收益增加得越多。

为了分析功率变化时组网联盟内不同协作方式对收益的影响，图 3 仿真比较了包含两个发送端的组网在两种联盟协作方式下与非联盟组网的收益情况。其中，T_1 和 T_2 的窃听信道状态信息分别为 $g_1=1.2$，$g_2=0.5$。当窃听信道增益较低的 T_2 发信号、T_1 发干扰时，各个发送端的收益相比原始的非协作组网方式以及 T_1 发信号、T_2 发干扰的组网方式，各个发送端获得收益达到最大，与理论分析相符，并随着功率的增加而增大。

图 4 和图 5 进一步给出了不同窃听信道状态信息条件下，组网联盟内不同协作方式对收益的影响。图 4 中给出了 T_2 的窃听信道状态信息 $g_2=0.5$ 时，g_1 的变化对各个发送端收益的影响，其中各个发送端的功率 P 恒为 5 mW。当 $g_1<g_2$ 时，如图 4，T_1 发信号、T_2 发干扰的联盟方式下的各个发送端的收益达到最大；当 $g_1>g_2$ 时，T_2 发信号、T_1 发干扰的联盟方式下的各个发送端的收益达到最大。只有当窃听信道增益最低的发送端发送信号，其余的发送端发干扰时，各个发送端的收益才能达到最大。其中，T_2 的收益随着另一发送端窃听信道 g_1 的增大而增大。图 5 相对应给出了 $g_1=1.2$ 时，g_2 对发送端收益的影响，与上述结论一样。当 $g_2<g_1$ 时，可以看到 T_2 发信号、T_1 发干扰的联盟方式下的各个发送端的收益达到最大；当 $g_2>g_1$ 时，T_1 发信号、T_2 发干扰的联盟方式下的各个发送端的收益达到最大。

最后，图 6 比较了网络原始状态下与基于本文方法的平均安全速率，可以看到，当发送端功率为 2~20 mW 时，基于本文方法下相同频段的发送端自适应形成联盟组网发送信号，网络平均安全速率相应提高 0.4~1.8 bit/(s·Hz)，与理论分析相符。

3.4 需求公平的实现

当网络中除 T_* 以外的某个发送端 T' 临时有强烈信号传输需求时，这时用 γ 表示 T' 自身单位安全速率的定价，T' 的分摊收益必须大于最优大联盟 T_* 的分摊收益，即

$$\gamma\left(C_{T'}^{\{N\}}-\sum_{i=1}^{n}C_{T_i}^{NC}\right)\Big/n>\rho\left(C_{T_*}^{\{N\}}-\sum_{i=1}^{n}C_{T_i}^{NC}\right)\Big/n \tag{20}$$

其中 $C_{T'}^{\{N\}}$ 表示 T' 发信号，其余发送端发干扰时的安全速率，$C_{T_*}^{\{N\}}$ 表示窃听信道状态信息最差的 T_* 发信号，其余发送端发干扰时的安全速率，化简得

$$\gamma\left(\log_2(1+P)-\log_2\left(1+g'P\Big/\left(\sum_{j\neq T'}^{n}Pg_j+1\right)\right)\right)$$
$$>\rho\left\{\log_2\left(1+g_{\min}P\Big/\left(\sum_{j\neq T_*}^{n}Pg_j+1\right)\right)\right\} \tag{21}$$

当 T' 对其安全速率的定价 γ 满足下述条件时，就能实现其发送信号的需求。

$$\gamma>\rho\left(1+\frac{\log_2\left(1+g'P\Big/\left(\sum_{j\neq T'}^{n}Pg_j+1\right)\right)-\log_2\left(1+g_{\min}P\Big/\left(\sum_{j\neq T_*}^{n}Pg_j+1\right)\right)}{\log_2(1+P)-\log_2\left(1+g'P\Big/\left(\sum_{j\neq T'}^{n}Pg_j+1\right)\right)}\right) \tag{22}$$

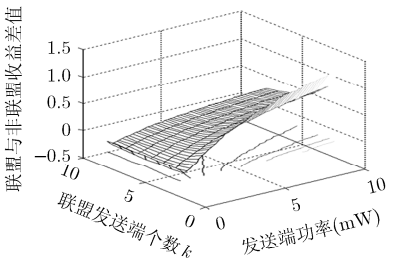

图 2 功率 P 的变化与联盟内发送端个数 k 对收益差 Δ_i 的影响

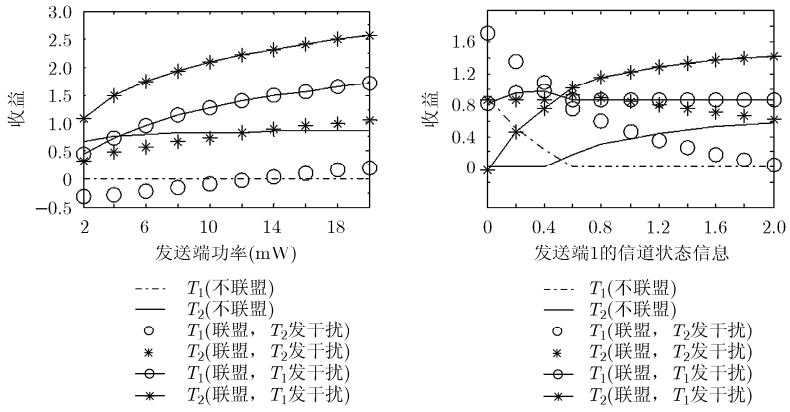

图 3 功率 P 变化时，组网联盟内不同协作方式对收益的影响

图 4 $g_2 = 0.5$，g_1 变化时，不同联盟方式对收益的影响

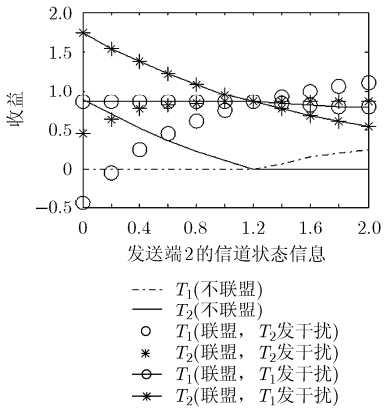

图 5 $g_1 = 1.2, g_2$ 变化时，不同联盟方式对收益的影响

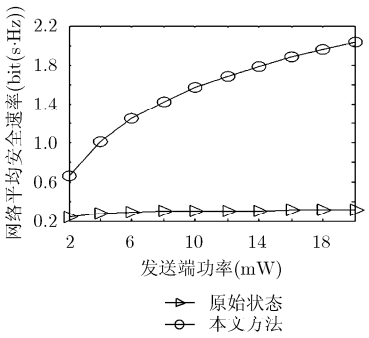

图 6 本文方法下网络平均安全速率相对初始状态的提高

5 结束语

无线协作网络多节点通过联盟组网发送人工噪声可以极大地提高安全速率，而自私节点拒绝协作会给网络带来能耗或安全速率的损失。因此，如何有效联盟组网以实现安全通信依赖于自私节点之间协作意愿以及收益分配策略。针对此问题，本文提出一种基于博弈的安全联盟组网方法，研究组网内发送端的相互协作关系，引入协作博弈中的收益分摊机制实现了联盟收益增加部分的公平分配，组网内窃听信道状态信息最差或者有紧急通信需求的发送端发送信号，其余发送端在其主信道的零空间上发送人工噪声的方式实现组网内协作，满足了不同网络下对安全和公平性的要求。仿真和分析结果表明：基于本文方法，当发送端功率为 20 mW 时，高斯信道下的网络平均安全速率相对初始状态提高 1.8 bit/(s·Hz)。

参 考 文 献

[1] Stark W and McEliece R J. On the capacity of channels with block memory[J]. *IEEE Transactions on Information Theory*, 1988, 34(2): 322–324.

[2] Geraci G and Dhillon H. A new model for physical layer security in cellular networks[C]. Proceedings of 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 2014: 2147–2152.

[3] Kashyap A, Basar T, and Srikant R. Correlated jamming on MIMO Gaussian fading channels[J]. *IEEE Transactions on Information Theory*, 2004, 50(9): 2119–2123.

[4] Geraci G, Dhillon H, and Andrews J. Physical layer security in downlink multi-antenna cellular networks[J]. *IEEE Transactions on Communications*, 2014, 62(6): 2006–2021.

[5] Wyner A. The wire-tap channel[J]. *Bell System Technical Journal*, 1975, 54(8): 1355–1387.

[6] Huiming W, Tongxing Z, and Pengcheng M. Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading[C]. Proceedings of 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 2014: 5396–5401.

[7] Walid S and Zhu H. Physical layer security: coalitional games

for distributed cooperation[C]. Proceedings of Symposium on Modeling and Optimization in Mobile Ad Hoc and Wireless Networks, Seoul, Korea, 2009: 1–8.

[8] Jorswieck E and Mochaourab R. Secrecy rate region of MISO interference channel: Pareto boundary and non-cooperative games[C]. Proceedings of International ITG Workshop on Smart Antennas, Berlin, Germany, 2009: 132–138.

[9] Fakoorian S and Swindlehurst A. Competing for secrecy in the MISO interference channel[J]. *IEEE Transactions on Signal Processing*, 2013, 61(1): 170–181.

[10] Fakoorian S and Swindlehurst A. MIMO interference channel with confidential messages: game theoretic beamforming designs[C]. Proceedings of IEEE Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 2010: 2099–2103.

[11] Fakoorian S and Swindlehurst A. MIMO interference channel with confidential messages: achievable secrecy rates and precoder design[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 640–649.

[12] Anand S, Sengupta S, and Chandramouli R. An attack-defense game theoretic analysis of multi-band wireless covert timing networks[C]. Proceedings of 2010 IEEE Computer Communications, San Diego, CA, USA, 2001: 14–19.

[13] Cho P, Hong Y, and Kuo J. A game theoretic approach to eavesdropper cooperation in MISO wireless networks[C]. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Prague, Czech, 2011: 3428–3431.

[14] Jun D, Rongqing Z, and Lingyang S. Truthful mechanisms for secure communication in wireless cooperative system[J]. *IEEE Transactions on Wireless Communications*, 2013, 12(9): 4236–4245.

[15] Mukherjee A. Principles of physical layer security in multiuser wireless networks: a survey[J]. *IEEE Communications Surveys & Tutorials*, 2014, 16(3): 1550–1573.

黄开枝： 女，1973 年生，教授，硕士生导师，研究方向为移动通信、信息处理、物理层安全.

洪 颖： 女，1989 年生，硕士生，研究方向为移动通信、通信信号处理与信息安全.

罗文宇： 男，1982 年生，讲师，研究方向为异构网络、物理层安全、认知无线电.

林胜斌： 男，1991 年生，硕士生，研究方向为移动通信、物理层安全.