EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Bargaining-based jammer power allocation for dynamic eavesdropping scenario

Duan Bowen, Cai Yueming, Zheng Jianchao*, Yang Weiwei and Yang Wendong

Abstract

This paper proposes a bargaining-based jammer power allocation scheme for multi-source multi-destination wireless network in the presence of a friendly jammer and a malicious node which eavesdrops erratically. We formulate the erratic behavior of the eavesdropper as a novel model where the eavesdropper wiretaps the message of the legitimate sources with a certain probability in a time slot. Moreover, in order to obtain a fair and efficient solution, the jammer power allocation problem is modeled as a Nash bargaining game under the constraint of maximum transmit power of a friendly jammer, which is a convex optimization problem. Then, the closed form of the Nash bargaining solution (NBS) is derived, and a simple but effective centralized algorithm is proposed. Besides, we find that the even power allocation solution and the sum-secrecy-rate optimal solution are the special cases of the NBS, when the bargaining power is properly selected. Simulation results demonstrate that the NBS achieves a good performance in terms of both effectiveness and fairness.

Keywords: Dynamic eavesdropping; Friendly jammer; Power allocation; Nash bargaining solution

1 Introduction

The shared nature of the wireless communication channel poses numerous security challenges, one of which is making wireless communications susceptible to eavesdropping [1-4]. Privacy and security are the key aspects in wireless communication systems while the traditional encryption cannot ensure that the message of legitimate source is absolutely infeasible to be deciphered especially when the mismanagement of key occurs. Fortunately, many researches find that the physical layer of wireless communications also enables novel ways to defend against the eavesdroppers [1-5]. Therefore, physical layer security approaches are gaining extensive attention.

Friendly jamming is one of the techniques in physical layer security, whose idea is to produce the artificial noise to deteriorate the eavesdropping channels to such an extent that successful decoding of the legitimate messages becomes infeasible [3-13]. The works [3-8] investigate the jammer-assisted communication system in terms of the design of transmission plan and the analysis of performance. [3] investigate the impact of the jammer's antenna number on system secrecy rate, and they find that only the eavesdropper's channel will be degraded when the jammer uses multiple antennas to generate artificial noise. Moreover, Tippenhauer et al. in [4] consider the reliability of the jammer-assisted communication system and illustrate the limitation of the jammer in terms of maintaining confidentiality from a perspective of attacker. Besides, Tang et al. in [6] analyze the secrecy performance of the jammer-assisted communication system in the case of the discrete memoryless channels and the Guassian channels. The secrecy capacity and the achievable secrecy rate are given for both channels.

Specifically, it is pioneered by [9-13] in terms of the jammer power allocation [9] and [10] use the auction theory to design the jammer power allocation schemes. The friendly jammer and the sources act as the auctioneer and the bidders, respectively. A distributed solution is obtained, and the properties such as convergence and equilibrium are analyzed. Han et al. in [11] introduce the Stackelberg game to investigate the interaction between the source and the friendly jammers. Through exchanging the 'price' between the sources and the friendly jammer repeatedly, a distributed solution with desirable performance is obtained. In [12,13], the authors design a Stackelberg game framework to encourage terminals

*Correspondence: longxingren.zjc.s@163.com
College of Communications Engineering, PLA University of Science and Technology, Yudao Road, Nanjing 210007, China

to act as the jamming node by compensating them with an opportunity to access the channel of legitimate parties. This cooperative mechanism cannot only increase the spectral efficiency but also improve secrecy rate meaningfully.

For the works above, it is worth mentioning that the scenario they consider is the case that the eavesdropper works all the time. However, in some practical systems, the eavesdropper is likely to wiretap erratically or has different preferences to different legitimate source's message, especially when the antenna number of the eavesdropper is limited and its eavesdropping ability tends to be reserved for the more valuable legitimate users. In this paper, this erratic nature of eavesdropper is referred to as the *dynamic nature of the eavesdropper* and this kind of scenario is called *dynamic eavesdropping scenario*. Undoubtedly, one of the results that the dynamic nature of eavesdropper brings about is the change on the strategy of jammer power allocation. If the network operator implements the jammer power allocation regardless of the dynamic nature of eavesdropper, it is likely that some sources experiencing securer communication link are allocated redundant jammer power while the packets of other sources endangered may be received by the eavesdropper. To the best of our knowledge, there is no any research on the scenario where the eavesdroppers work intermittently. Therefore, a study on the model which can reflect the dynamic nature of the eavesdroppers and the corresponding optimization schemes is urgently required.

In addition, the objective of the aforementioned works is to improve the secrecy rate or maximize the secrecy capacity, while seldom works consider the fairness among the sources. The works [9-13] have made progress in terms of the interaction between the sources and the jammer, but the fairness among the sources has not been taken into consideration, and thus, that kind of solution will generally suffer from severe fairness problem. Although [14] has investigated the similar physical layer security scenario with consideration of fairness, the author only compared the proposed scheme with the even power allocation scheme. Thus, the effectiveness of that scheme is questionable. Fortunately, cooperative game theory often acts as a powerful tool to investigate how the sources negotiate to achieve their conflicting objectives. Specifically, the Nash bargaining solution (NBS), a core concept in the cooperative game theory, possesses the NBS fairness and Pareto optimality, and thus, it is introduced to increase efficiency while maintaining fairness in the jammer power allocation.

Briefly, the contributions and novelty of our work are summarized below:

- To the best of our knowledge, this is the first paper that studies the jammer power allocation in the dynamic eavesdropping scenario. Furthermore, this novel model is a generalized physical layer security model. When the malicious node is ensured to eavesdrop all the time, the generalized model will degenerate to the classic physical layer security model [9-13].
- We take both the sum-secrecy-rate and the fairness among the sources into account by proposing a NBS-based optimization scheme. Moreover, the closed-form NBS is derived so that the iteration progress in the Stackelberg game and auction game can be replaced by a simple but effective centralized implementation.
- The impact of bargaining power on system performance is investigated. Theoretical analysis and numerical results indicate that the even power allocation solution and the sum-secrecy-rate optimal solution are the special cases of the NBS, when the bargaining power is properly selected.

The remainder of the paper is organized as follows. The system model and utility function are presented in Section 2. In Section 3, the optimization problem in dynamic eavesdropping scenario is modeled as the NBS-based power allocation problem. The NBS is derived, and the effect of bargaining power on network performance is investigated. Section 4 presents our simulation results, and Section 5 concludes the paper.

2 System model and utility function

2.1 System model

We consider a multi-source multi-destination wireless network which consists of N sources and destinations, denoted by S_i and D_i, $i = 1, \ldots, N$, in the presence of a friendly jammer J and an eavesdropping node E which eavesdrops erratically, as illustrated in Figure 1. We denote the gain of the channel from the source S_i to the destination D_i, from the source S_i to the eavesdropping node E and from the jammer J to the eavesdropping node E as h^i_{sd}, h^i_{se}, and h_{je}, respectively. The available channel bandwidth is divided equally into N orthogonal channels, and the bandwidth of each channel is assumed to be 1. Each source occupies a free orthogonal channel, and all of the channels can be used by the jammer. Each source transmits with power P_0. Without loss of generality, the variance of independent thermal noise for each link is σ^2. We define the power the jammer contribute to helping the source S_i as P_i, and P_J stands for the total power of the jammer.

Due to the dynamic nature of the eavesdropper, the discussion on the cases whether the source S_i is wiretapped or not should be conducted in advance. First, when there is an eavesdropper wiretapping the message sent from the

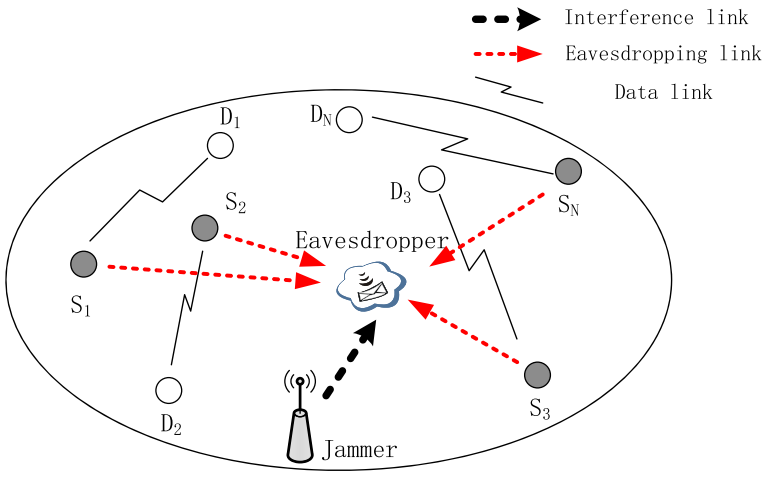

Figure 1 Illustration of system model. S, source; D, destination.

source S_i, the secrecy rate for the source S_i to the destination D_i without the help of the jammer is given as [15]

$$\begin{aligned} R_{i,0}^{S} &= \left\{\log_2\left(1+P_0\left|h_{sd}^{i}\right|^2/\sigma^2\right)\right. \\ &\quad \left.-\log_2\left(1+P_0\left|h_{se}^{i}\right|^2/\sigma^2\right)\right\}^{+} \\ &\triangleq \left\{\log_2\left(1+P_0\gamma_{sd}^{i}\right)-\log_2\left(1+P_0\gamma_{se}^{i}\right)\right\}^{+} \\ &= \left\{\log_2\left(1+\frac{P_0\left(\gamma_{sd}^{i}-\gamma_{se}^{i}\right)}{1+P_s\gamma_{se}^{i}}\right)\right\}^{+}, \end{aligned} \tag{1}$$

where $\{\cdot\}^{+} = \max\{\cdot, 0\}$. Just like [11], it is assumed that the jammer is close to the eavesdropper and far from the destination. Thus, the interference from the jammer to the destination is negligible when compared to the additive noise. In this case, the secrecy rate for the source S_i to the destination D_i with the help of the jammer can be approximated as

$$\begin{aligned} R_i^S &\approx \left\{\log_2\left(1+P_0\left|h_{sd}^{i}\right|^2/\sigma^2\right)-\log_2\left(1+\frac{P_0\left|h_{se}^{i}\right|^2/\sigma^2}{1+P_i\left|h_{je}\right|^2/\sigma^2}\right)\right\}^{+} \\ &\triangleq \left\{\log_2\left(1+P_0\gamma_{sd}^{i}\right)-\log_2\left(1+\frac{P_0\gamma_{se}^{i}}{1+P_i\gamma_{je}}\right)\right\}^{+} \\ &= \left\{\log_2\left(1+\frac{P_0\left(\gamma_{sd}^{i}-\frac{\gamma_{se}^{i}}{1+P_i\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^{i}}{1+P_i\gamma_{je}}}\right)\right\}^{+}. \end{aligned} \tag{2}$$

Then, when eavesdropper is not wiretapping the source S_i, the message sent from the source S_i is secure, and the secrecy rate for the source S_i to the destination D_i is given as

$$\begin{aligned} R_{i,0}^{S} &= \left\{\log_2\left(1+P_0\left|h_{sd}^{i}\right|^2/\sigma^2\right),0\right\}^{+} \\ &\triangleq \log_2\left(1+P_0\gamma_{sd}^{i}\right). \end{aligned} \tag{3}$$

For the convenience of modeling, we define the security factors Γ_i, $\Gamma_{i,0}$, and Γ_i' from Equations 2, 1, and 3, respectively. The security factor Γ_i derived from Equation 2, reflecting the security performance of source S_i's communication link, is defined as

$$\Gamma_i = \frac{P_0\left(\gamma_{sd}^{i}-\frac{\gamma_{se}^{i}}{1+P_i\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^{i}}{1+P_i\gamma_{je}}}. \tag{4}$$

In addition, since the secrecy rate for the source S_i to the destination D_i without the help of the jammer is $R_{i,0}^{S}$, the security factor $\Gamma_{i,0}$ derived from Equation 1, is defined as

$$\Gamma_{i,0} = \frac{P_0\left(\gamma_{sd}^{i}-\gamma_{se}^{i}\right)}{1+P_s\gamma_{se}^{i}}, \tag{5}$$

which will be regarded as the disagreement point in the following Nash bargaining game. When the source S_i ensures that there is no eavesdropper wiretapping its message, we defined the security factor Γ_i' from Equation 3 as

$$\Gamma_i' = P_0\gamma_{sd}^{i}. \tag{6}$$

Obviously, the Γ_i, Γ_i', and $\Gamma_{i,0}$ represent how secure the received signal is and is closely related to the security performance. It can be seen from Equation 4 that the more jammer power to be allocated to a source, the more seriously the eavesdropper's ability will be impaired and the larger security factor can be obtained. However, since the jammer power is limited, a competition among sources for the jammer power will exist inevitably. Moreover, to

maximize the security performance of the network, considering the requirement of sources in the static scenario is not enough, the jammer has to take the dynamic nature of the eavesdropper into account. To resolve the conflict among sources and describe the scenario more precisely, the interaction among the sources will be modeled as a Nash bargaining game and the utility function will be designed according to the whole probability formula.

2.2 Utility function

In this paper, we assume all the sources believe that the action of the eavesdropper closely depends on the importance of their confidential message. We define the happening of the eavesdropping action in a time slot as an eavesdropping probability θ_i. It reflects an evaluation of the message security by source itself, e.g., the more important the source considers the message in this time slot, the more likely it is, the source S_i think, to be wiretapped by the malicious node. Given the N sources in the system, the utility vector is denoted as $\mathrm{u} = (u_1\, u_2 \cdots u_N)$. In a given time slot, the utility function of a source S_i is defined as the expectation of the instantaneous security factor Γ_{dynamic}. According to the whole probability formula, we define the source S_i's utility function u_i related to the security factors of the source S_i given in Equations 4 and 6, to be

$$\begin{aligned} u_i\left(P_i,\theta_i\right) &\triangleq \mathbb{E}\left[\Gamma_{\text{dynamic}}\right] \\ &= \theta_i\Gamma_i + \left(1-\theta_i\right)\Gamma' = \theta_i \frac{P_0\left(\gamma_{sd}^i - \frac{\gamma_{se}^i}{1+P_i\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^i}{1+P_i\gamma_{je}}} \\ &\quad + \left(1-\theta_i\right)P_0\gamma_{sd}^i. \end{aligned} \tag{7}$$

The utility function represents expectation of the instantaneous security factor and is directly related to the performance of the communication security. θ_i represents the probability with which the eavesdropper will wiretap source S_i in the given time slot. It can be seen that when $\theta_i = 1,\ \forall i \in \mathcal{N}$, the scenario will degenerate to the classic physical layer security model. When $\theta_i = 0$, it means that there is no risk that the message of source S_i will be wiretapped. Moreover, since we use the mathematic expectation to study the dynamics, the channel coefficient should be averaged over time and thus, only pass loss is considered in this paper. Besides, it is clear that u_i is an increasing function of P_i. Then, we denote the disagreement point as $\mathrm{u}_0 = \left(u_{1,0}\, u_{2,0} \cdots u_{N,0}\right)$, which is defined as

$$u_{i,0} \triangleq \Gamma_{i,0} = \frac{P_0\left(\gamma_{sd}^i - \gamma_{se}^i\right)}{1+P_s\gamma_{se}^i}. \tag{8}$$

It is the equivalent received signal-to-noise ratio of the source S_i without the help of the jammer, and the u_0 is the vector of the utility below which the sources will not reach an agreement and quit the bargaining. Specifically, the disagreement point is the worst condition that each source expects when the eavesdropper is ensured to wiretap the source's message and the jammer is not willing to help the source. Given the definitions of the utility function and the disagreement point, a feasible utility set U is defined as

$$U \triangleq \left\{ (u_1 \ldots u_N) \,\middle|\, \textstyle\sum_{i=1}^{N} P_i \le P_J\ , P_i \ge 0 \right\}. \tag{9}$$

Formally, a bargaining game is defined by a set of feasible utilities U and a disagreement point $\mathrm{u}_0 \in U$. The set U contains utility vectors $\mathrm{u} = (u_1\, u_2 \cdots u_N)$, denoting the payoff to each source, for all possible strategies the players may implement. The disagreement point u_0 represents the 'status quo' prior to bargaining or the worst possible outcomes for the sources. In our model, although the strategies are the power contributed by jammer to help each source instead of the sources action, it can be interpreted as an outcome of the bargaining among the sources. In other words, sources cooperatively choose a compromise point. That is, rather than individually focusing on payoff maximization, sources jointly choose a mutually agreeable utility vector and agree to implement the strategies at the jammer.

3 NBS-based jammer power allocation

3.1 Nash bargaining game

The NBS is a core solution concept in cooperative game theory, and we choose it as the bargaining game solution among many bargaining games for the following reasons: First, since the NBS is obtained based on a certain set of axioms representing the fairness of the solution, it can improve the sources' utility and maintain the fairness among sources at the same time. Second, the NBS has flexibility in bargaining power selection. This property makes it available to balance between the optimal sum-secrecy-rate and the optimal fairness among sources, which is preferred on system design perspective. Third, due to the property of the Nash bargaining game, an efficient and fair solution can be obtained readily, with no need for the iteration used for converging to the equilibrium in the noncooperative game. Thus, the pricing mechanism which will result in heavy overheads to the network can be avoided.

In the Nash bargaining game, given the disagreement point u_0 and the feasible utility set U, the Nash bargaining solution provides a fair and efficient method to distribute jammer power among all the sources. Suris et al. [16] have made it clear that the convexity of the utility space (U) is a sufficient condition to guarantee that the optimization problem of the Nash product (NP) is a Nash bargaining game. In order to obtain the NBS, the conclusion in [16] will be applied to prove the following theorem first.

Theorem 1. The game $\{\mathcal{N}, U\}$ is a Nash bargaining game.

Proof. The game $\{\mathcal{N}, U\}$ is a bargaining game if and only if U is a closed and convex subset of $U^{\mathcal{N}}$ [17]. It is obvious that the utility set U is closed, we only need to check whether the convexity of set U is met, which means for any $0 \leq \theta \leq 1$, if $U^a = \left(U_1^a, \cdots, U_2^a\right) \in \mathbb{U}$ and $U^b = \left(U_1^b, \cdots, U_2^b\right) \in \mathbb{U}$, then $\theta U^a + (1-\theta)\, U^b \in \mathbb{U}$. □

From Equation 7, we have

$$u_i\left(P_i, \theta_i\right) = \theta_i \frac{P_0\left(\gamma_{sd}^i - \frac{\gamma_{se}^i}{1+P_i\gamma_{je}}\right)}{1+\frac{P_s\gamma_{se}^i}{1+P_i\gamma_{je}}} + \left(1-\theta_i\right) P_0 \gamma_{sd}^i, \tag{10}$$

which is an increasing function of P_i and $\lim_{P_i\to\infty} u_i = P_s\gamma_{sd}^i$. According to Equation 10, we can obtain that

$$P_i = \frac{\theta_i P_0\left(\gamma_{sd}^i - \gamma_{se}^i\right) + \left(1-\theta_i\right) P_0\gamma_{sd}^i\left(1+P_0\gamma_{se}^i\right) - u_i\left(1+P_0\gamma_{se}^i\right)}{u_i\gamma_{je} - \theta_i P_0\gamma_{sd}^i\gamma_{je} - \left(1-\theta_i\right) P_0\gamma_{sd}^i\gamma_{je}}. \tag{11}$$

Then, the feasible utility set U can be rewritten as

$$U = \left\{ \mathrm{u} \,\middle|\, \varphi(\mathrm{u}) \triangleq \textstyle\sum_{i=1}^N P_i \leq P_J,\ u_{i,0} \leq u_i < P_s\gamma_{sd}^i,\ \ i = 1, \ldots, N \right\}, \tag{12}$$

where the last constraint means that $0 \leq P_i < \infty, \forall i$. To make the problem solvable, we define $U_1 \triangleq \left\{\mathrm{u} \,\middle|\, u_i \geq u_{i,0}, i = 1, \ldots, N\right\}$ and $U_2 \triangleq \left\{\mathrm{u} \,\middle|\, \varphi(\mathrm{u}) \leq P_J, u_i < P_s\gamma_{sd}^i, i = 1, \ldots, N\right\}$. Hence, we have $U = U_1 \cap U_2$. Since U_1 is a convex set obviously, to prove the utility set U is convex, we only need to prove that U_2 is a convex set.

To begin with, we need to prove that $\varphi(\mathrm{u})$ is a convex function which will be applied to prove the convexity of U_2. From the definition of φ in Equation 12, it is obvious that the Hessian matrix of $\varphi(\mathrm{u})$ is a diagonal matrix. Moreover, its i th diagonal element is

$$\frac{\partial^2\varphi\left(\mathrm{u}\right)}{\partial u_i^2} = -2\frac{P_0\gamma_{sd}^i\left(1+P_0\gamma_{se}^i\right) - \left[\theta_i P_0\left(\gamma_{sd}^i - \gamma_{se}^i\right) + \left(1-\theta_i\right) P_0\gamma_{sd}^i\left(1+P_s\gamma_{se}^i\right)\right]}{\gamma_{je}\left(u_i - P_s\gamma_{sd}^i\right)^3}. \tag{13}$$

Since $u_i < P_s\gamma_{sd}^i$ for any finite P_i, we have $\frac{\partial^2\varphi(\mathrm{u})}{\partial u_i^2} > 0$ for all $i = 1, \ldots, N$, which means the Hessian matrix of $\varphi(\mathrm{u})$ is positive definite. Therefore, $\varphi(\mathrm{u})$ is a convex function and for set $\theta U_2^a + (1-\theta)U_2^b$, we have $\varphi(\theta U_2^a + (1-\theta)U_2^b) \leq \theta\varphi(U_2^a) + (1-\theta)\varphi(U_2^b) \leq \theta P_J + (1-\theta)P_J = P_J$, which means $\theta U_2^a + (1-\theta)U_2^b \in \mathbb{U}$. As a result, U_2 is a convex set [18], and thus, the game $\{\mathcal{N}, U\}$ is a Nash bargaining game. This completes the proof.

With the theorem above, we know the NBS is the unique point that maximizes the NP, e.g., finding the NBS results in the following optimization problem [17]:

$$\max_{P_1,\cdots P_N} \prod_{i=1}^N \left(u_i - u_{i,0}\right)^{\beta_i}, \quad s.t.\ P_i \geq 0,\ \textstyle\sum_{i=1}^N P_i \leq P_J, \tag{14}$$

where $\sum_{i=1}^N \beta_i = 1$, $\beta_i \geq 0, \forall i$. β_i is the bargaining power of each source and shows the advantage of each player in the game. Since the function of ln is monotonically increasing when $u_i - u_{i,0} \geq 0$, $\forall i$, thus, the optimization problem in Equation 14 is equivalent to

$$\begin{aligned} &\arg\max_{P_1,\cdots P_N} \sum_{i=1}^N \beta_i \ln\left\{\theta_i \frac{P_0\left(\gamma_{sd}^i - \frac{\gamma_{se}^i}{1+P_i\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^i}{1+P_i\gamma_{je}}} + \left(1-\theta_i\right) P_0\gamma_{sd}^i - \frac{P_0\left(\gamma_{sd}^i - \gamma_{se}^i\right)}{1+P_0\gamma_{se}^i}\right\}. \\ &\mathrm{s}.t. P_i \geq 0, \quad \textstyle\sum_{i=1}^N P_i \leq P_J. \end{aligned} \tag{15}$$

In order to find the NBS, we should solve Equation 15. The jammer power vector is defined as $\mathrm{P} \triangleq [P_1 \cdots P_N]$, and the Lagrangian function for problem in Equation 15 can be represented as

$$L(\mathrm{P}, \alpha, \lambda) \triangleq \sum_{i=1}^{N} \beta_i \ln \left\{ \theta_i \frac{P_0 \left(\gamma_{sd}^i - \frac{\gamma_{se}^i}{1+P_i \gamma_{je}} \right)}{1 + \frac{P_0 \gamma_{se}^i}{1+P_i \gamma_{je}}} + (1-\theta_i) P_0 \gamma_{sd}^i - \frac{P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right)}{1 + P_0 \gamma_{se}^i} \right\} - \sum_{i=1}^{N} \lambda_i P_i - \alpha \left(\sum_{i=1}^{N} P_i - P_J \right). \tag{16}$$

Here, α and λ_i are Lagrangian multipliers for the equality and inequality constraints, respectively. The objective function in Equation 16 can be proved to be concave, which is omitted here because of the limitation of the space. In addition, since the equality and the inequality constraints are affine, the optimization problem in Equation 15 is a convex optimization problem [19]. Hence, its first-order Karush-Kuhn-Tucker (KKT) conditions become sufficient for the solution of Equation 15 [18], which are given as

$$\frac{\partial L(\mathrm{P}, \alpha, \lambda)}{\partial P_i} = \beta_i \frac{\left(P_0 \gamma_{sd}^i \gamma_{je} \theta_i \left(1 + P_0 \gamma_{se}^i \right) - \gamma_{je} \theta_i P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right) \right) \Big/ \left(\gamma_{je} P_i + \left(1 + P_0 \gamma_{se}^i \right) \right)^2}{\frac{\left(P_S \gamma_{sd}^i \gamma_{je} \theta_i P_i + \theta_i P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right) \right)}{\gamma_{je} P_i + \left(1 + P_0 \gamma_{se}^i \right)} - \left(\frac{P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right)}{1 + P_0 \gamma_{se}^i} - (1-\theta_i) P_0 \gamma_{sd}^i \right)} - \lambda_i - \alpha = 0, \tag{17}$$

$$P_i \geq 0, \ \sum_{i=1}^{N} P_i = P_J, \ \lambda_i \geq 0, \ \lambda_i P_i = 0. \tag{18}$$

Note that if the jammer's total power is too small, due to the property of the KKT condition, there is $P_i = 0$ and $\lambda_i > 0$ for some sources experiencing serious eavesdropping risk. In other words, the limited total power will be assigned to some minority sources only, in order to guarantee the optimality of the solution, regardless the requirement of others. Here, we only consider the condition that the jammer's total power is sufficient enough to ensure that all the sources will enter the bargaining game, e.g., $P_i > 0$ for all i. When $P_i > 0$ and we have $\lambda_i = 0$, thus

$$P_i = \frac{-\left(J_i K_i + I_i L_i - 2 H_i I_i J_i \right) + \sqrt{\left(J_i K_i + I_i L_i - 2 H_i I_i J_i \right)^2 - 4 \left(K_i I_i - H_i I_i^2 \right) M_i}}{2 \left(K_i I_i - H_i I_i^2 \right)}, \tag{19}$$

where $H_i = \frac{P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right)}{1 + P_0 \gamma_{se}^i} - (1-\theta_i) P_0 \gamma_{sd}^i$, $I_i = \gamma_{je}$, $J_i = 1 + P_0 \gamma_{se}^i$, $K_i = P_0 \gamma_{sd}^i \gamma_{je} \theta_i$, $L_i = \theta_i P_0 \left(\gamma_{sd}^i - \gamma_{se}^i \right)$, $M_i = -\frac{\beta_i}{\alpha} \left(K_i J_i - I_i L_i \right)$ for $i = 1, \cdots, N$. Then, according to the total power constraint of the jammer, the following equation holds:

$$\sum_{i=1}^{N} \frac{-\left(J_i K_i + I_i L_i - 2 H_i I_i J_i \right) + \sqrt{\left(J_i K_i + I_i L_i - 2 H_i I_i J_i \right)^2 - 4 \left(K_i I_i - H_i I_i^2 \right) M_i}}{2 \left(K_i I_i - H_i I_i^2 \right)} = P_J. \tag{20}$$

We can see that if α changes from 0 to ∞, the left side of Equation 20 will monotonically decrease from ∞ to 0. Hence, it is ensured that a unique positive solution α exists for Equation 20, and the optimal α can be found using bisection method. Then, the Nash bargaining solution can be obtained using Equation 19 and the optimal α.

3.2 Analysis of bargaining power

The bargaining power of the source S_i represents the priority of the source, which can be tuned by the jammer to achieve a balance between the optimal global security performance and the optimal fairness among sources. In the respect of the fairness among sources, since the optimal secrecy-rate fairness, which depends on the topology of the network, is not always achievable, here, we only derive the relationship between the NBS and the optimal power fairness solution. The following theorem shows the effect of the bargaining power analytically.

Theorem 2. The Nash bargaining solution proves to be the even power allocation solution and the sum-secrecy-rate optimal solution, respectively, when

$$\beta_i^E = \frac{q_i^E}{\sum_{i=1}^{N} q_i^E} \tag{21}$$

and

$$\beta_i^{\mathrm{o}} = \frac{q_i^{\mathrm{o}}}{\sum_{i=1}^{N} q_i^{\mathrm{o}}}, \tag{22}$$

where $q_i^E = \frac{(K_iP_J+L_iN)(I_iP_J+J_iN)-H_i(I_iP_J+J_iN)^2}{(K_iJ_i-I_iL_i)}$ and $q_i^{\mathrm{O}} = \frac{\frac{\left(K_iP_i^{\mathrm{O}}+L_i\right)}{\left(I_iP_i^{\mathrm{O}}+J_i\right)}-H_i}{\ln 2\left(1+\frac{\left(K_iP_i^{\mathrm{O}}+L_i\right)}{\left(I_iP_i^{\mathrm{O}}+J_i\right)}\right)}$.

Proof. First, from Equation 17, we have

$$\beta_i = \alpha\frac{(K_iP_i+L_i)(I_iP_i+J_i)-H_i(I_iP_i+J_i)^2}{(K_iJ_i-I_iL_i)} \triangleq \alpha q_i^E. \tag{23}$$

Considering the even power allocation, e.g., $P_i = \frac{P_J}{N}, \forall i$, the following equation holds

$$\frac{\beta_i}{\beta_j} = \frac{q_i^E}{q_j^E}. \tag{24}$$

Thus, when $\beta_i = \frac{q_i^E}{\sum_{i=1}^{N} q_i^E}$, the NBS coincides with the even power allocation solution. □

Then, in terms of global secrecy performance, the sum-secrecy-rate optimal solution is the maximizer of the following optimization problem:

$$\begin{aligned}&\max_{\mathrm{P^o}} \sum_{i=1}^{N}\log_2\left(1+\theta_i\frac{P_0\left(\gamma_{sd}^i-\frac{\gamma_{se}^i}{1+P_i^{\mathrm{o}}\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^i}{1+P_i^{\mathrm{o}}\gamma_{je}}}+(1-\theta_i)P_0\gamma_{sd}^i\right).\\ &s.t.\quad \sum_{i=1}^{N}P_i^{\mathrm{o}}\le P_J,\quad P_i^{\mathrm{o}}\ge 0.\end{aligned} \tag{25}$$

Also, the optimal problem in Equation 25 is a convex optimal problem and its Lagrangian function is

$$\begin{aligned}L^{\mathrm{O}}\left(\mathrm{P^O},\alpha^{\mathrm{O}},\lambda^{\mathrm{O}}\right) \triangleq &\sum_{i=1}^{N}\log_2\left\{1+\theta_i\frac{P_0\left(\gamma_{sd}^i-\frac{\gamma_{se}^i}{1+P_i^{\mathrm{o}}\gamma_{je}}\right)}{1+\frac{P_0\gamma_{se}^i}{1+P_i^{\mathrm{o}}\gamma_{je}}}+(1-\theta_i)P_0\gamma_{sd}^i\right\}\\ &-\sum_{i=1}^{N}\lambda_i^{\mathrm{O}}P_i-\alpha^{\mathrm{O}}\left(\sum_{i=1}^{N}P_i^{\mathrm{O}}-P_J\right).\end{aligned} \tag{26}$$

Correspondingly, its KKT conditions are

$$\frac{\partial L^{\mathrm{O}}\left(\mathrm{P^O},\alpha^{\mathrm{O}},\lambda^{\mathrm{O}}\right)}{\partial P_i} = \frac{(K_iJ_i-I_iL_i)/\left(I_iP_i^{\mathrm{O}}+J_i\right)^2}{\ln 2\left(1+\frac{\left(K_iP_i^{\mathrm{O}}+L_i\right)}{I_iP_i^{\mathrm{O}}+J_i}+(1-\theta_i)P_0\gamma_{sd}^i\right)}-\alpha^{\mathrm{O}}-\lambda_i^{\mathrm{O}}=0, \tag{27}$$

$$P_i^{\mathrm{O}}\ge 0,\ \sum_{i=1}^{N}P_i^{\mathrm{O}}=P_J,\ \lambda_i^{\mathrm{O}}\ge 0,\ \lambda_i^{\mathrm{O}}P_i^{\mathrm{O}}=0, \tag{28}$$

and its solution is

$$\begin{aligned}P_i^{\mathrm{O}} = &\frac{-\left[I_i\left(J_i\left(1+\varepsilon\right)+L_i\right)+J_i\left(I_i\left(1+\varepsilon\right)+K_i\right)\right]}{2I_i\left(I_i\left(1+\varepsilon\right)+K_i\right)}\\ &+\frac{\sqrt{\left[I_i\left(J_i\left(1+\varepsilon\right)+L_i\right)+J_i\left(I_i\left(1+\varepsilon\right)+K_i\right)\right]^2-4I_i\left(I_i\left(1+\varepsilon\right)+K_i\right)\left[J_i\left(J_i\left(1+\varepsilon\right)+L_i\right)-\frac{K_iJ_i-I_iL_i}{\alpha^{\mathrm{O}}\ln 2}\right]}}{2I_i\left(I_i\left(1+\varepsilon\right)+K_i\right)},\end{aligned} \tag{29}$$

where α^{O} is the Lagrangian multiplier related to the equality constraint and $\varepsilon = (1-\theta_i)P_0\gamma_{sd}^i$. After we use bisection method to obtain the optimal α^{O}, we can calculate the P_i^{O} readily. Then, comparing Equation 25 with Equation 15, we have

$$q_i^{\mathrm{o}} \triangleq \beta_i = \frac{\frac{\left(K_i P_i^{\mathrm{O}} + L_i\right)}{\left(I_i P_i^{\mathrm{O}} + J_i\right)} - H_i}{\left[\ln 2\left(1 + \frac{\left(K_i P_i^{\mathrm{O}} + L_i\right)}{\left(I_i P_i^{\mathrm{O}} + J_i\right)} + (1-\theta_i) P_0 \gamma_{sd}^i\right)\right]}. \tag{30}$$

Therefore, when

$$\beta_i^{\mathrm{o}} = \frac{q_i^{\mathrm{o}}}{\sum_{i=1}^{N} q_i^{\mathrm{o}}}, \tag{31}$$

the NBS coincides with the sum-secrecy-rate optimal solution. This completes the proof.

3.3 Centralized implementation

Since the Stackelberg game and auction game require many iterations before converging to the Nash equilibrium, the exchange of information in the iteration progress will give rise to heavy overheads to the network. In this paper, we propose a centralized algorithm, which is simple but efficient thanks to the closed form of the NBS. Nevertheless, it requires enough computational ability and global channel state information (CSI) at the jammer.

In the centralized algorithm, we assume that the jammer have global and perfect CSI to compute the NBS proposed before. To get the NBS-based power allocation, each source informs the jammer of the eavesdropping probability θ_i through backhaul communication, according to the evaluation of the security of their message by themselves. Then, the jammer uses the bisection method to find the α that satisfies Equation 20 and computes the NBS-based power allocation solution by using Equation 19. In this way, without any iteration and resulting heavy overheads to the network, the NBS scheme can obtain its solutions precisely.

4 Simulation results

In this section, we evaluate the performance of the NBS-based jammer power allocation by MATLAB simulations. The global security performance and the fairness among sources will be demonstrated and analyzed as the eavesdropping probability increases. We compare the three optimization schemes (sum-secrecy-rate optimal (SSRO), even power allocation (EPA), and NBS) and evaluate the four parameters: network sum-secrecy-rate, individual achievable secrecy rate, Jain's fairness index (*JFI*) of the secrecy rate and the *JFI* of the allocated power [20]. Note that a larger *JFI* indicates a fairer solution. For all the channels, the path loss coefficient is $\alpha = 4$ and the static channels only with path loss is assumed due to the consideration of the average performance during a given time slot.

To begin with, to evaluate the performance of the NBS, we consider a three-source network. The simulation model is shown in Figure 2, and we assume the bargaining powers to be $\beta_i = 1/N = 1/3,\ \forall i \in \mathcal{N}$. We assume that the y coordinates of the sources and destinations are 0. The x coordinates of sources and destinations follow $X(n) = -n(-1)^n$ and $X(n) = 10 - n(-1)^n$, respectively. The coordinates of eavesdropper and jammer are (0, 8) and (0, 6), respectively. The total power constraint of the jammer P_J is set to be 15 dB, and we assume the eavesdropping probability of each source θ_i is the same and is in the range of 0 to 1.

In Figure 3, we evaluate the network sum-secrecy-rate under three different schemes. It can be seen that the sum-secrecy-rate of the NBS scheme is very nearly the same with that of the SSRO in the simulated eavesdropping probability range, while there is an increasing difference of secrecy rate between the SSRO and the EPA. When the eavesdropping probability becomes 1, the model we investigate degenerates to the classical physical layer security model and the difference of security performance is the clearest.

In Figure 4, we show the evolution of the *JFI* of security rate and allocated power versus the eavesdropping probability. In Figure 4a, we find that the *JFI* of security rate of NBS and SSRO is decreasing as the eavesdropping probability approaching 1. That is because with the eavesdropping probability increasing, the security condition of each source becomes different and the difference of secrecy rate of each source becomes large. Obviously, the NBS scheme is fairer than SSRO scheme, and the EPA is the fairest. In Figure 4b, the *JFI* of allocated power of NBS scheme is about 0.94 and almost remains constant with

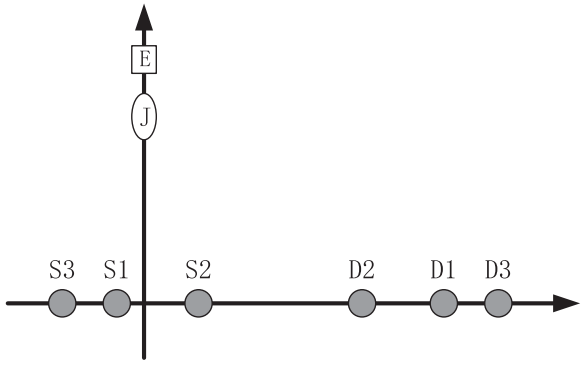

Figure 2 Illustration of the three-source network with static channels. S, source; D, destination; J, jammer.

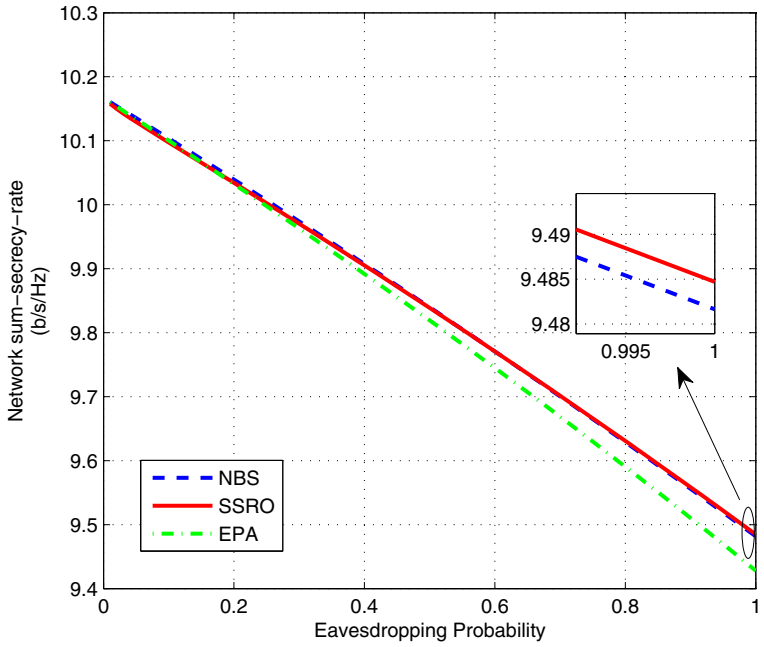

Figure 3 Sum-secrecy-rate versus eavesdropping probability in a three-source network.

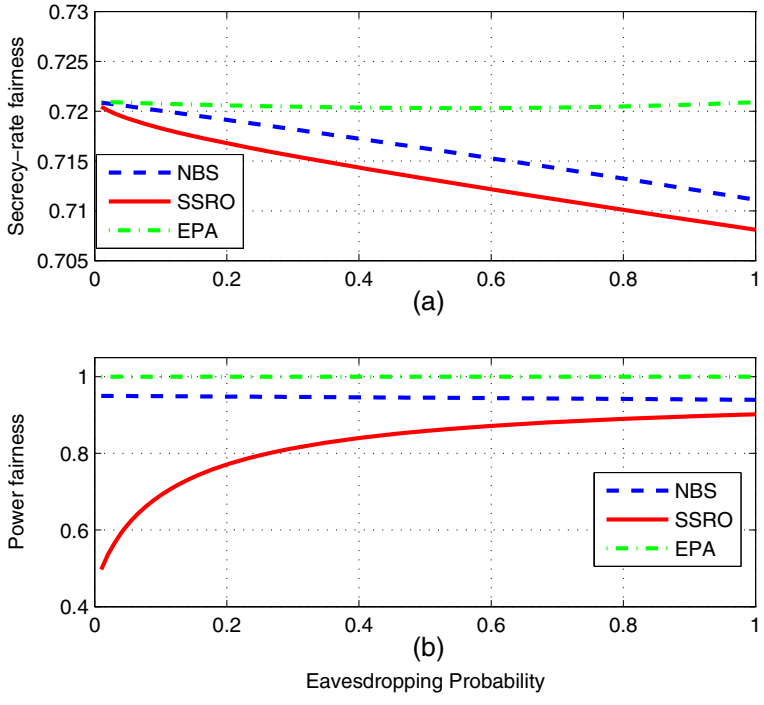

Figure 4 Secrecy-rate fairness and power fairness versus eavesdropping probability in a three-source network. (a) Secrecy-rate fairness versus eavesdropping probability. **(b)** Power fairness versus eavesdropping probability.

the eavesdropping probability growing. Besides, we find that with the eavesdropping probability is growing, the power fairness of SSRO will increase gradually. When the eavesdropping probability is low, since the source 2 is the nearest to the eavesdropper, the SSRO will allocate major jammer power to the source 2. When the eavesdropping probability is high, to keep the sum-security-rate optimal, the SSRO scheme will allocate more jammer power for other two sources than before, resulting a higher *JFI* of allocated power. For even power allocation, as the jammer allocates the same power to all three sources, the *JFI* of allocated power is 1.

To further evaluate the performance of the effect of bargaining power, we consider a two-source network, and the bargaining powers are assumed to be two different sets: NBS1: $\beta_1 = 0.3$, $\beta_2 = 0.7$; NBS2: $\beta_1 = 0.7$, $\beta_2 = 0.3$. The individual achievable secrecy rate of the sources (in Figure 5), network sum-secrecy-rate (in Figure 6), and the fairness among sources (in Figure 7) are compared.

In Figure 5, it is showed that, on the one hand, the network sum-secrecy-rate of source 2 is higher than that of source 1, for source 2 experiences a securer communication links than source 1, and, on the other hand, a source with a larger bargaining power achieves a higher achievable secrecy rate. We should note that, in fact, the NBS1 is a source 2 prefered scheme while the NBS2 is a source 1 prefered scheme. When a higher bargaining power is assigned to source 2, and thanks to the securer communication link the source 2 experiences, this kind of scheme will contribute more jammer power to help source 2 and put more emphasis on the network sum-secrecy-rate, thus giving rise to a larger difference of secrecy rate than NBS2 and vice versa.

In Figure 6, we evaluate the sum-secrecy-rate under four schemes. The result in Figure 6 is closely related to that in Figure 5: the NBS1 will emphasize the network

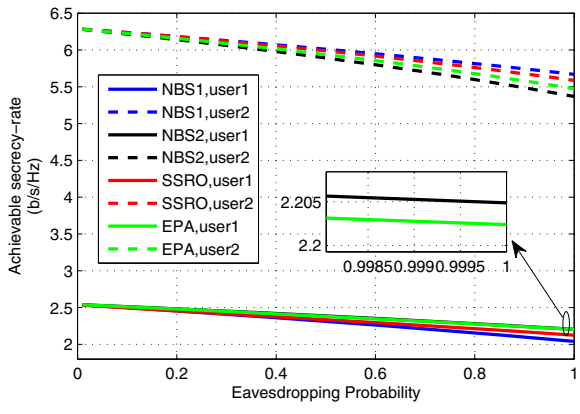

Figure 5 Achievable secrecy rates versus eavesdropping probability in a two-source network.

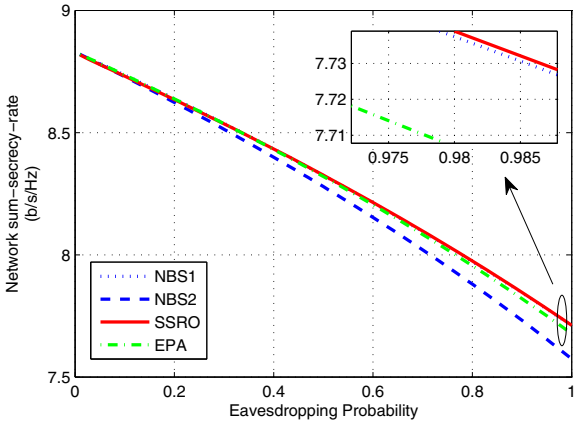

Figure 6 Sum-secrecy-rates versus eavesdropping probability in a two-source network.

sum-secrecy-rate and the NBS2 will emphasize the fairness among sources. Thus, in Figure 6, the sum-secrecy-rate of NBS1 is closer to that of SSRO than NBS2.

In Figure 7, we compare the fairness among four schemes. In Figure 7a, we find that the NBS2 is the best and NBS1 is the worst among all four schemes in terms of secrecy-rate fairness. Although the EPA is a power-fairest scheme, which, however, cannot achieve more desirable fairness than NBS2 in the simulated eavesdropping probability range. In Figure 7b, with the eavesdropping probability increasing, the power fairness of NBS2 is approaching that of EPA (e.g., $JFI = 1$). Since the NBS1 more focuses on improving sum-secrecy-rate, its power fairness is the worst in high eavesdropping probability region.

In Figure 8, to get a better understanding of the bargaining powers on network performance, we show the network sum-secrecy-rate and *JFI* of allocated power under three eavesdropping probabilities: 0.2, 0.6, and 1. The source 1's bargaining power is increasing from 0 to 1. When $\beta_1 = 1$ or $\beta_1 = 0$, all of the jammer power will be distributed to source 1 or source 2. For the three different eavesdropping probabilities, the network sum-secrecy-rate is maximized at $\beta_1 = 0.485,\ 0.470,\ 0.450$, respectively. The power fairness increases as β_1 increases until optimal power-fairness is achieved. For $\theta_i = 0.2,\ 0.6,\ 1$, the proposed NBS scheme becomes even power allocation in the range from $\theta_i = 0.6$ to $\theta_i = 0.63$.

5 Conclusion

In this paper, we investigated the security performance and designed the corresponding optimization scheme in the dynamic eavesdropping scenario. The eavesdropping probability was defined to characterize the erratic behavior of the eavesdropper, and the bargaining theory was introduced to analyze the negotiation among the sources on jammer power allocation. In order to address

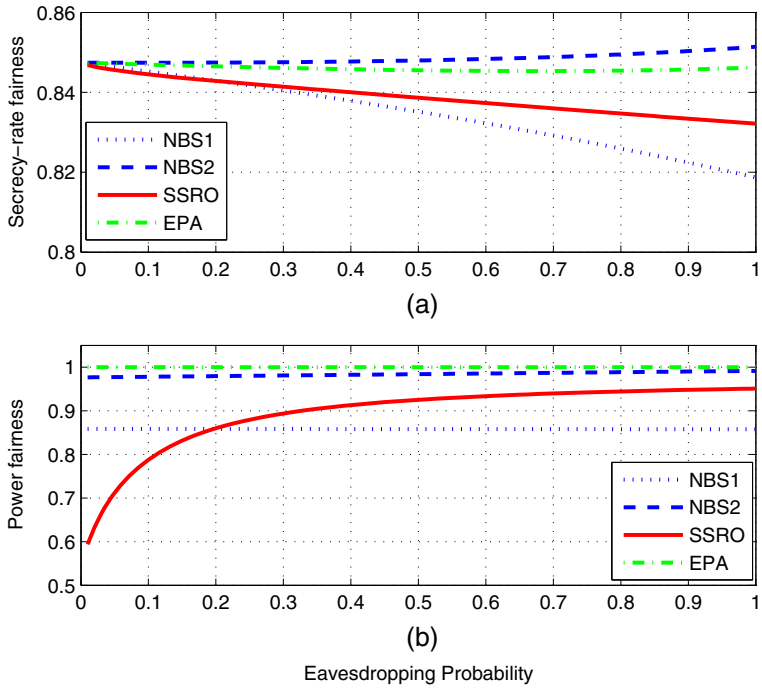

Figure 7 Secrecy-rate fairness and power fairness versus eavesdropping probability in a two-source network. (a) Secrecy-rate fairness versus eavesdropping probability. **(b)** Power fairness versus eavesdropping probability.

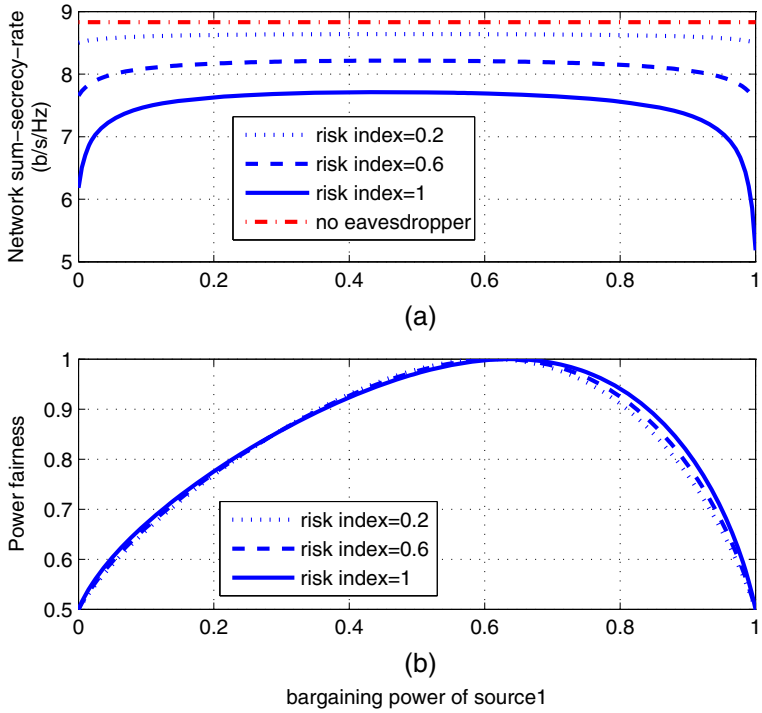

Figure 8 Sum-secrecy-rate and power fairness versus bargaining power in a two-source network. (a) Network sum-secrecy-rate versus bargaining power of source 1. **(b)** Power fairness versus bargaining power of source 1.

both the fairness among sources and global security performance, the optimization problem was formulated as a Nash bargaining game, which is a convex optimization problem. The closed-form NBS was derived, and the effect of the bargaining power was investigated analytically. Simulation results showed that the effectiveness and fairness of the proposed NBS-based resource allocation are desirable.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
This work is supported by the National Natural Science Foundation of China (No. 61371122 and No. 61301162) and the Jiangsu Natural Science Foundation (BK20130067).

Received: 30 May 2014 Accepted: 27 October 2014
Published: 12 November 2014

References

1. ZH Awan, A Zaidi, L Vandendorpe, Multiaccess channel with partially cooperating encoders and security constraints. IEEE Trans. Inform. Forensics Secur. **8**, 1243–1254 (2013)
2. ZH Awan, A Zaidi, L Vandendorpe, Secure communication over parallel relay channel. IEEE Trans. Inform. Forensics Secur. **7**, 359–371 (2012)
3. S Goel, R Negi, Guaranteeing secrecy in wireless networks using artificial noise. IEEE Trans. Wireless Commun. **7**, 2180–2189 (2008)
4. N Tippenhauer, L Malisa, A Ranganathan, S Capkun, in *IEEE Symposium on Security and Privacy (SP)*. On limitations of friendly jamming for confidentiality (Berkeley, CA, 2013), pp. 160–173
5. L Dong, Z Han, A Petropulu, H Poor, in *Proceeding of IEEE Workshop on Statistical Signal Processing (SSP)*. Cooperative jamming for wireless physical layer security (Cardiff, 2009), pp. 417–420
6. X Tang, R Liu, P Spasojevic, H Poor, Interference assisted secret communication. IEEE Trans. Inform. Theor. **57**, 3153–3167 (2011)
7. J Vilela, M Bloch, J Barros, S McLaughlin, in *Proceedings of the IEEE International Conference on Communications (ICC)*. Friendly jamming for wireless secrecy (Cape Town, South Africa, 2010), pp. 1–6
8. J Vilela, M Bloch, J Barros, S McLaughlin, Wireless secrecy regions with friendly jamming. IEEE Trans. Inform. Forensics Secur. **6**, 256–266 (2011)
9. Z Han, N Marina, M Debbah, A Hjorungnes, in *5th International Conference on Mobile Ad-hoc and Sensor Networks(MSN)*. Improved wireless secrecy capacity using distributed auction theory (Fujian, 2009), pp. 442–447
10. R Zhang, L Song, Z Han, B Jiao, in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Improve physical layer security in cooperative wireless network using distributed auction games (Shanghai, 2011), pp. 18–23
11. Z Han, N Marina, M Debbah, A Hjorungnes, Physical layer security game: interaction between source, eavesdropper and friendly jammer. EURASIP J. Wireless Commun. Netw. **2009**, 452907 (2010)
12. JY Qu, YM Cai, D Wu, HL Chen, Stackelberg game based power allocation for physical layer security of device-to-device communication underlaying cellular networks. Frequenz. **68**(5-6), 285–295 (2014)
13. I Stanojev, A Yener, Improving secrecy rate via spectrum leasing for friendly jamming. IEEE Trans. Wireless Commun. **12**, 134–145 (2013)
14. JT Yue, B Yang, XP Guan, in *International Conference on Wireless Communications and Signal Processing (WCSP)*. Fairness-guaranteed pricing and power allocation with a friendly jammer against eavesdropping (Huangshan, 2012), pp. 1-6
15. A Muthoo, *Bargaining Theory with Applications*. (Cambridge University Press, 1999)
16. J Suris, L DaSilva, Z Han, A MacKenzie, in *Proceeding of IEEE ICC*. Cooperative game theory for distributed spectrum sharing (Glasgow, 2007), pp. 5282–5287
17. Z Han, D Niyato, W Saad, T Basar, A Hjorungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. (Cambridge University Press, 2012)
18. R Jain, DM Chiu, W Hawe, A quantitative measure of fairness and discrimination for resource allocation in shared systems. DEC Research Report TR-301 (1984). http://arxiv.org/abs/cs.NI/9809099
19. S Boyd, L Vandenberghe, *Convex Optimization*. (Cambridge University Press, 2004)
20. M Andrews, K Kumaran, A Stolyar, P Whiting, R Vijayakumar, Providing quality of service over a shared wireless link. IEEE Commun. Mag. **39**, 150–154 (2001)

doi:10.1186/1687-1499-2014-186
Cite this article as: Bowen *et al.*: **Bargaining-based jammer power allocation for dynamic eavesdropping scenario.** *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:186.