

Chapter 5

Cooperative Security in D2D Communications

Device-to-Device (D2D) communication based storage offers a potential solution for traffic offloading from the cellular infrastructure, and mobile devices themselves can act as caching servers, i.e., content helpers [1]. The content requesters can ask for content items from the helpers among cellular peers without the help of eNodeB. However, the success of such content sharing via D2D links depends on physical conditions of the direct wireless links, which must be weighted against possibly additional security threats in D2D links. To realize the successful content sharing, the selected source node (i.e., content helper) must have the data for which the destination node (i.e., content requester) desires, and the physical link condition and user mobility also cannot be ignored. Thus, the social interaction between content helpers and content requesters is firstly investigated in this chapter. However, the direct transmission among mobile users also increases the risk of eavesdropping. Selecting D2D users (DUEs) to act as friendly jammers or relays can be regarded as an effective way to eliminate the risk of eavesdropping [2, 3]. However, it should be admitted that not all nodes are willing to serve as cooperative jammers or relays due to the different levels of altruistic cooperative behaviors of user nodes. Thus, social trust, which can be quantified by link stability or deduced by the trustiness of cooperative nodes, is also a critical factor for cooperative node selection [4, 5]. To improve link stability and system robustness, this chapter considers both physical links and social characteristics, which includes the social interaction and social trust. It focuses on the mechanism for selecting the best content helper and cooperative jamming partner to enhance the secrecy and transmission reliability of content sharing via D2D links against eavesdropping. Particularly, an optimization problem for joint source and cooperative jammer selection with power allocation is developed to maximize the secrecy rate of D2D links under individual and sum transmit power constraints. In addition to a common scenario in which the CSI of all the links can be accurately acquired, two more practical cases where only statistical CSI is available are also considered in this chapter.

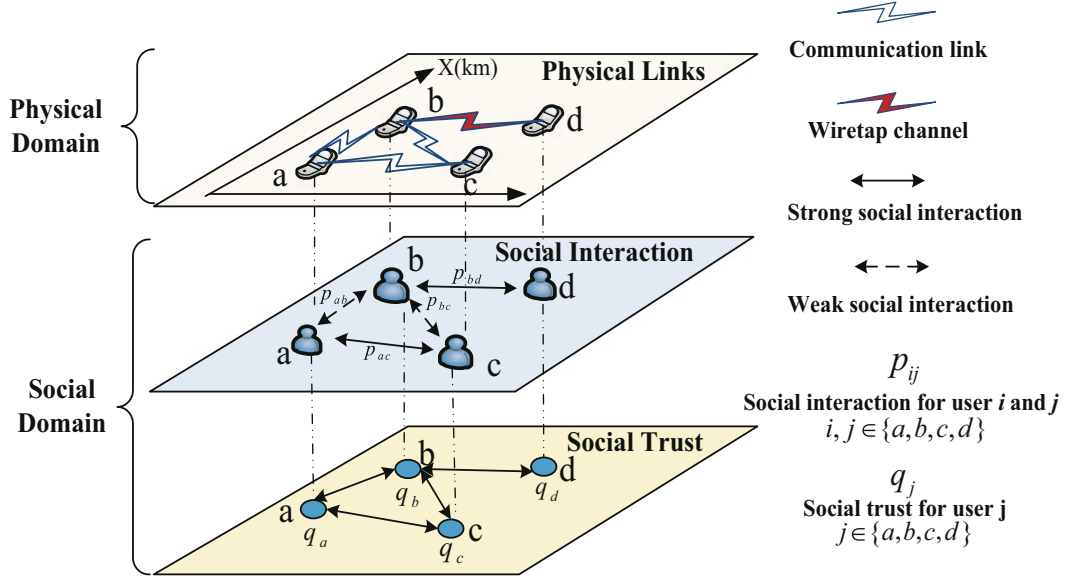


Fig. 5.1 Physical domain and social domain in D2D communications

5.1 Background and Motivations

D2D communications offer a potential solution for traffic offloading from the cellular infrastructure. By storing content items, individual mobile devices themselves can act as caching servers (i.e., content helpers) to help the content requesters to obtain the desired content without going through eNodeB. Thus, the success of such content delivery via D2D links of mobile users depends on physical condition of the direct wireless links. Besides, the social characteristics should also be considered for communication enhancement. So in this chapter, we are going to analyze the secrecy performance by jointly considering the physical link conditions and social relationships among content requesters and content helpers.

Figure 5.1 shows a three-layer structure which describes both physical domain and social domain in D2D communications. The first layer in Fig. 5.1 presents the conventional physical consideration for D2D communications, which would be effected by the quality of wireless physical links. Both the second layer and the third layer describe the social domain of users, and social considerations are made in terms of social interaction and social trust. The social interaction between users presented in the second layer of Fig. 5.1 is effected by the user mobility, which is indicated by the success probabilities between users, e.g., p_{ij} . In the third layer, each user is characterized with a social trust, which indicates user trustworthiness for cooperative communications, e.g., q_j . Though D2D communications improve communication efficiency, there exist some security threats during the signal transmission, such as eavesdropping, which is one of the most common security risk for wireless communications.

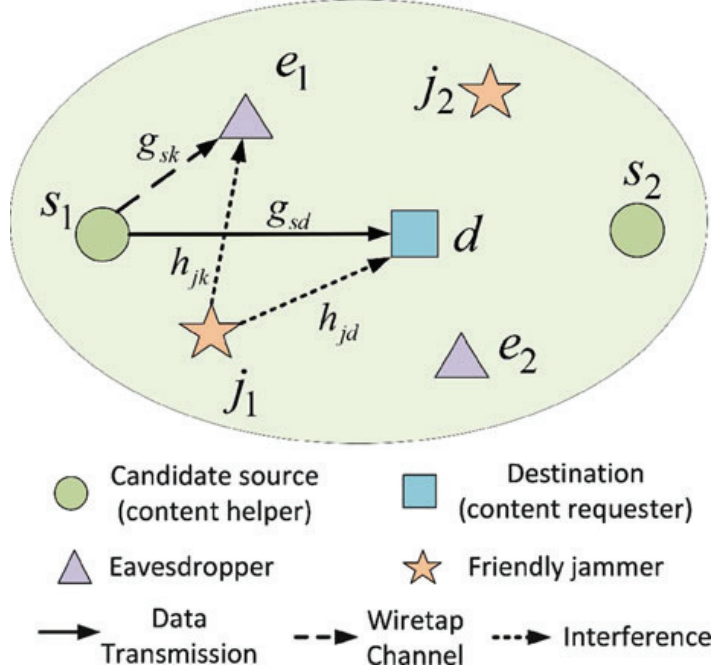
Traditionally, security enhancement is considered by assuming static transmission links between the source nodes and the destination nodes. However, this assumption is not always practical due to users' mobility and other specific demands. Moreover, in the multiple-source scenarios, i.e., there are many candidate caching nodes can be chosen as content helpers, which is vital for content requesters to make suitable decisions. Meanwhile, social factors such as contact frequency and duration should also be considered except for the physical factors for content transmission, as shown in Fig. 5.1. Besides, friendly neighbor nodes can be recruited to serve as cooperative relays or jammers to protect the communication links and overcome security vulnerabilities. However, in a mobile environment, one cannot simply rely on arranged jammers for each communication link. Instead, it is important to dynamically select friendly and efficient cooperative jamming partners by considering their physical link conditions, and their willingness for serving as cooperative jammers in the mobile environment.

Based on Fig. 5.1, the social interaction impacted by user mobility and social trust based on the interactive relationship among network nodes can be exploited for efficient and effective cooperative networking. There are a number of existing studies on cooperative jamming for improving secrecy. However, most of them assume a full channel state information (CSI) knowledge between all user nodes, which is not very practical. For the links involving passive and mobile eavesdropper nodes, it is difficult and costly to acquire accurate and real-time CSI. Consequently, the basic system model for content sharing between source nodes and destination nodes via D2D links with the help of jammer nodes in the presence of eavesdroppers is described and discussed under the consideration of either full CSI case or statistical CSI case. Both the physical domain and the social domain are discussed to improve the communication stability and system robustness.

5.1.1 System Model and Assumptions

The system model considers the problem of reliability and secrecy enhancement for wireless content sharing between content source nodes and content requesters. Scenario used in this chapter comprises of several source nodes (i.e., content helpers) in possession of content required by the destination nodes (i.e., content requesters), and potential social eavesdroppers who may attempt to eavesdrop on the legitimate data transmission. Several intermediate nodes serve as jammers to thwart eavesdropping and to improve security performance.

Figure 5.2 shows a practical D2D wireless system model in D2D overlay, avoiding cross-tier interference between CUEs and D2D links. In other words, neighboring D2D links share the same spectrum is not considered here to avoid the complication of mutual interference. Let $\mathcal{S} = \{1, \dots, S\}$, $\mathcal{K} = \{1, \dots, M\}$, and $\mathcal{J} = \{1, \dots, N\}$ be the index sets of source nodes, eavesdroppers, and jammers, respectively. One source node is chosen for data transmission to the destination node, and a neighboring node is recruited as a cooperative jamming node

Fig. 5.2 System model

to disrupt passive eavesdropping and improve security. It is assumed that a simple control protocol is used at the destination node to measure the CSI associated with the source-to-destination and jammer-to-destination links. The wireless channels between any pair of mobile nodes are characterized as independent flat Rayleigh fading. The channel power gain between source node s and destination node d is denoted as g_{sd} . Similarly, h_{jd} and h_{jk} denote the channel power gains from the jammer j to destination d and eavesdropper k , respectively. g_{sk} is the channel gain between source node s and eavesdropper k .

5.1.2 Channel State Information

Considering whether the instantaneous information of the channels is available or not, there are three general CSI cases[6] used in research, and we first list them in the following to distinguish.

- **Full CSI case:** as in the typical scenario, the channels between any pair of mobile nodes are assumed to be independent and identically distributed (i.i.d.) with flat fading. In addition, DUEs tend to be with low mobility or even stationary to keep the D2D links stable. In this case, it is usually assumed that the CSI of all the links can be accurately acquired at the BS by means of (blind) channel estimation.
- **Partial CSI case:** practically, it is costly, difficult, and perhaps impossible to acquire accurate and real-time CSI, especially for situations involving passive and mobile eavesdropper nodes [7, 8]. Thus, the model can be expanded to a more general one to accommodate less powerful BS and less accurate

channel information in D2D overlay. In this case, g_{sd} and h_{jd} can be always known at the BS since DUEs and cooperative jammers can feedback the CSI regularly. However, the BS only has statistical information for the CSI of links involving eavesdroppers. Without loss of generality, this chapter focuses on the popular Rayleigh fading channel model, assuming that the channel power gain follows exponential distribution due to fast fading. On the other hand, large-scale shadowing effect is absorbed into the mean of exponential distribution. Therefore, we can acquire the information of $g_{sk} \sim \text{Exp}(\lambda_g)$, $h_{jk} \sim \text{Exp}(\lambda_h)$, where λ_g and λ_h are the expected channel power gains of g_{sk} and h_{jk} , and $\text{Exp}(\lambda)$ denotes the exponential distribution with mean λ .

- **Statistical CSI case:** compared with the partial CSI case, the statistical CSI case is more practical by assuming that the accurate CSI of channels g_{sd} and h_{jd} is not known either. In other words, only the statistical CSI of all links, i.e., g_{sk} , h_{jk} , g_{sd} , and h_{jd} , is provided, and the expected channel power gains of g_{sd} and h_{jd} are denoted as λ_{sd} and λ_{jd} , respectively.

5.2 Social Characteristics for Cooperative Communications

As mentioned above, both physical links and social factors will impact the successful content sharing between content requesters and content helpers with the assistance of jamming partners. Thus, selecting the source node and the friendly cooperative jamming partner is important to guarantee the communication reliability. In this chapter, social interaction based selection of source node and social trust based selection of jammer are discussed, respectively.

5.2.1 Social Interaction for Content Sharing

When there exist multiple source nodes in the network, it is critical to choose the optimal source node to help the destination node to obtain the desired content. To realize the successful communications, potential D2D links between the content helpers and the content requesters may have good physical channel conditions, and their contact time must be long enough for the desired content transmission. In this part, the social interaction will be exploited to describe the successful transmission of direct content sharing between content requesters and content helpers. Generally, the social interaction is mainly evaluated by two factors: social contact rate and social contact duration. Social contact rate is the number of encounters between two users during a time interval, while social contact duration can be calculated by how long two users remain effective communications within a short distance. Practically, data blocks can be considered successfully delivered if they can be transmitted within a single encountering time or through several encounters [9]. For simplicity, this part focuses on time-sensitive services that require one-time delivery.

As shown in the second layer in Fig. 5.1, p_{sd} is an indicator to demonstrate the social interaction between source node (i.e., content helper) and destination node (i.e., content requester), which is defined as a success probability for the d -th destination node receiving the data block transmitted by the s -th source node. Notice that the success probability of D2D data transmission in a cellular D2D underlay has been studied in [9], by considering spectrum resource sharing between cellular users and D2D users. The scenario in this case focuses on a D2D overlay without spectrum sharing between cellular users and D2D links, which is different from [9], and the D2D links are assigned with dedicated spectrum resources. However, cooperative jamming spans the same spectrum as the desired data transmission.

Referring to the derivation in [9], the success probability p_{sd} can be expressed as

$$p_{sd} = \Pr \left\{ T_{sd} \geq \frac{Z}{R_{sd}} \right\} \quad (5.1)$$

$$= \int_0^\infty \frac{P_s \lambda_{sd}}{P_s \lambda_{sd} + P_j \lambda_{jd} \left(2^{\frac{Z/t_{sd}}{t}} - 1 \right)} \exp \left(-\frac{2^{\frac{Z/t_{sd}}{t}} - 1}{P_s \lambda_{sd}} t \right) dt,$$

where Z is the size of data blocks. T_{sd} indicates the social contact duration between the s -th source node and the destination node d , which is exponentially distributed with mean t_{sd} [9].

Obviously, narrowing the candidate set of source nodes with the minimum threshold of success probability $\theta_{\min}$ will result in lower complexity without noticeable performance loss. This yields a narrowed candidate source set for d , $\mathcal{S}_T$,

$$\mathcal{S}_T = \{s \in \mathcal{S} : p_{sd} > \theta_{\min}\}. \quad (5.2)$$

5.2.2 Social Trust for Cooperative Jamming

In addition to the requirements of the qualified content sharing for selecting the source nodes (i.e., content helpers), selection of potential cooperative jammers should also be considered with their trustworthiness. Recall that in the third layer in Fig. 5.1, each user is characterized with an indicator to demonstrate the trustworthiness for cooperative communications, thus to clarify the trustworthiness degree of jammers, q_j is defined in this subsection to indicate the social trust index of the j -th jammer, and $q_j \in [0, 1]$. It is noted that $q_j = 1$ indicates a fully trusted and dependable node while $q_j = 0$ indicates a node that is totally untrustworthy. Functionally, jammer j will cooperate by sending the requisite jamming signal with probability q_j . Note that $(1 - q_j)$ can also be used to model the selfishness of jammer j to conserve its own energy.

5.2.3 Objective Problem Formulation

As described above, the objective is to select the optimal source node and cooperative jamming partner, with the consideration of social characteristics and power allocation, to hamper reception by the worst-case eavesdropper for secrecy guaranteed transmission. Meanwhile, the source node and the friendly jammer can be selected considering the social interaction and social trust, respectively.

Let P_s and P_j be the transmit powers of source node s and that of jammer j , respectively, which are normalized by the power of noise. Thus, the power of AWGN on each channel will be $\sigma^2 = 1$. Furthermore, given the limited energy of mobile nodes, it is necessary to control interference between jamming nodes and legitimate transceivers when they share the same spectrum. Thus, in our formulation, we consider both individual power constraints for source and jammer, i.e., $P_{\max}^s$ and $P_{\max}^j$, and joint power constraint, i.e., $P_{\max}$. For convenience, the feasible set of the power parameters can be defined as,

$$\mathcal{X} = \left\{ (P_s, P_j) : \begin{array}{l} 0 \leq P_s \leq P_{\max}^s \\ 0 \leq P_j \leq P_{\max}^j \\ 0 \leq P_s + P_j \leq P_{\max} \end{array} \right\}. \quad (5.3)$$

Considering the social trust of jammer j , the security rate of the data transmission from the s -th source node to the d -th destination node against the k -th eavesdropper can be expressed as

$$\begin{aligned} C_{s,j,k}(P_s, P_j) = & q_j \left[\log_2 \left(1 + \frac{P_s g_{sd}}{P_j h_{jd} + 1} \right) - \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right]^+ \\ & + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \log_2(1 + P_s g_{sk})]^+, \end{aligned} \quad (5.4)$$

where $[x]^+ = \max(0, x)$, and q_j is the social trust for jammer j as aforementioned.

The most damaging eavesdropper is the one that causes the lowest secrecy rate. The worst-case eavesdropper depends only on the physical channel conditions. Here stable and reliable wiretap links are considered to demonstrate worst-case eavesdropping. With the objective to maximize the achievable secrecy rate $C_{s,j,k}(P_s, P_j)$, against the worst-case k -th non-colluding eavesdropper, the controller selects the single best s -th source node and j -th cooperative jammer and optimizes P_s and P_j in the problem formulation of

$$\max_{s \in \mathcal{S}} \max_{j \in \mathcal{J}} \min_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} C_{s,j,k}(P_s, P_j). \quad (5.5)$$

As discussed above, the social interaction between the source nodes and the destination nodes plays a role in improving the communication reliability. By considering the social interaction, the previous problem in Eq. (5.5) can be reduced to

$$\max_{s \in \mathcal{S}_T} \max_{j \in \mathcal{J}} \min_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} C_{s,j,k}(P_s, P_j). \quad (5.6)$$

Then the set of candidate source nodes can be identified by excluding nodes with poor link stability, in order to improve the stability and robustness of content sharing. Meanwhile, the smaller number of candidate source nodes leads to a lower computational complexity.

Notice that once the solution to Eq. (5.7) is found, the cooperative source and jamming partner selection process in Eq. (5.6) can be addressed more easily.

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} C_{s,j,k}(P_s, P_j) . \quad (5.7)$$

5.3 Optimization for Secrecy Rate Maximization

Recall that the secrecy rate optimization problem of Eq. (5.7) is non-convex and NP-hard. Consequently, both heuristic simulated annealing and approximate solutions will be considered, and bounds on the achievable secrecy rate will be used to simplify the above optimization problem and yield a suboptimal solution with little performance loss.

5.3.1 Secrecy Rate Maximization with Full CSI

In this subsection, the secrecy rate maximization problem is considered in the full CSI case. In other words, the instantaneous information of all the links is known at the controller. Firstly, a direct solution with the simulated annealing algorithm is presented, and then upper and lower bounds on the achievable secrecy rate are discussed to obtain the suboptimal solution with low complexity.

5.3.1.1 Heuristic Simulated Annealing Based Direct Evaluation

In this subsection, a heuristic simulated annealing (SA) approach is presented to solve the optimization problem in full CSI case. SA is a probabilistic method for finding the global minimum of a function that may possess several local minima [10]. It works by emulating the physical process whereby a solid is slowly cooled so that eventually its structure is “frozen” in a minimum energy configuration.

Given a set of source nodes, eavesdroppers, and cooperative jammers, the accurate values of q_j , g_{sd} , g_{sk} , h_{jk} , and h_{jd} are determined when assuming full CSI for all the links. Therefore, the variables of the optimization problem in Eq. (5.4) are P_s and P_j . Below is a brief overview of the steps:

Step 1: Randomly generate an initial solution (P_s, P_j) to be valued by the cost function of Eq. (5.4);

- Step 2: Generate a random neighboring solution and compute the new solution's function value;
- Step 3: Pick the new solution if its function value is larger. Otherwise, accept the new solution with a certain probability;
- Step 4: Repeat Steps 2–3 until an acceptable solution is found or upon reaching a number of iterations.

As proved in [11], after a number of iterations, the SA algorithm will converge to a solution, (P_s^*, P_j^*) , which, with high likelihood, represents the optimal or acceptably good suboptimal solution to the optimization problem. However, one limitation of the SA heuristic algorithm is the lack of worst-case performance guarantee. Furthermore, its potential for computational time reduction is limited.

Considering the weaknesses of the SA, a potentially more effective alternative is to design approximation algorithms with higher reliability and lower complexity. Here, upper and lower bounds are firstly derived on the secrecy rate. Notice that many existing relaxation methods optimize either the upper bound or the lower bound of the original problem before taking the optimized parameters as the final result [12, 13]. Thus, in addition to present algorithms based on the exact optimization, both upper and lower bounds are considered in this subsection to simplify the original optimization of transmit powers.

5.3.1.2 Low-Complexity Optimization Leveraging Upper Bound

Applying the well-known inequality $\ln(x) \leq x - 1$ to Eq. (5.4) gives

$$\ln 2 \cdot C_{s,j,k}(P_s, P_j) \leq q_j \left[\frac{1 + \frac{P_s g_{sd}}{P_j h_{jd} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} - 1 \right]^+ + (1 - q_j) \left[\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} - 1 \right]^+. \quad (5.8)$$

Reorganizing the formula above, the achievable secrecy rate can be upper bounded as

$$C_{s,j,k}(P_s, P_j) \leq \frac{q_j}{\ln 2} \frac{\left[\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right]^+}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} + \frac{(1 - q_j) P_s [g_{sd} - g_{sk}]^+}{\ln 2 (1 + P_s g_{sk})}. \quad (5.9)$$

For simplicity, further define the following:

$$f(P_s, P_j) = \left[\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right]^+, \quad (5.10a)$$

$$g(P_s, P_j) = 1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}, \quad (5.10b)$$

$$h(P_s) = P_s [g_{sd} - g_{sk}]^+, \quad (5.10c)$$

$$w(P_s) = 1 + P_s g_{sk}, \quad (5.10d)$$

$$u_k(P_s, P_j) = g(P_s, P_j) w(P_s), \quad (5.10e)$$

$$v_k(P_s, P_j) = \frac{q_j}{\ln 2} f(P_s, P_j) w(P_s) + \frac{(1-q_j)}{\ln 2} g(P_s, P_j) h(P_s). \quad (5.10f)$$

It follows that the objective function in Eq. (5.7) can use the secrecy rate upper bound in Eq. (5.9) giving

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_k \left\{ \frac{q_j}{\ln 2} \frac{f(P_s, P_j)}{g(P_s, P_j)} + \frac{(1-q_j)}{\ln 2} \frac{h(P_s)}{w(P_s)} \right\} = \max_{(P_s, P_j) \in \mathcal{X}} \min_k \left\{ \frac{v_k(P_s, P_j)}{u_k(P_s, P_j)} \right\}. \quad (5.11)$$

By referring to mathematically equivalent problems in [14], the formula above can be reformulated as follows:

$$\min_{(P_s, P_j) \in \mathcal{X}} \max_k \frac{u_k(P_s, P_j)}{v_k(P_s, P_j)}. \quad (5.12)$$

Therefore, if the optimal solution (P_s^*, P_j^*) and the corresponding optimal objective value $f^* = \frac{u_k(P_s^*, P_j^*)}{v_k(P_s^*, P_j^*)}$ is found for the problem of Eq. (5.12), then (P_s^*, P_j^*) is also the optimal solution to Eq. (5.11).

Notice that $u_k(P_s, P_j)$ and $v_k(P_s, P_j)$ are nonlinear functions of P_s and P_j . Although this optimization problem is still non-convex, fortunately, such a non-convex optimization problem has been studied before by adopting the generalized fractional programming (GFP) algorithms, e.g. in [15]. Particularly, we utilize the Dinkelbach-type algorithm, one of the most popular GFP algorithms [16, 17] to solve our optimization problem.

It should be noted that both $u_k(P_s, P_j)$ and $v_k(P_s, P_j)$ are bounded. Furthermore, $v_k(P_s, P_j) > 0$ for $P_s \in (0, P_{\max}^s)$ and $P_j \in (0, P_{\max}^j)$. Hence the optimization problem in Eq. (5.12) has an optimal solution. Firstly, Eq. (5.12) can be rewritten as follows for simplicity,

$$(P) \quad \min_{(P_s, P_j) \in \mathcal{X}} \max_k \frac{u_k(P_s, P_j)}{v_k(P_s, P_j)}.$$

To solve problem (P), one considers the following parametric problem:

$$(P_\mu) \quad F_k(\mu) = \min_{(P_s, P_j) \in \mathcal{X}} \max_k \{u_k(P_s, P_j) - \mu \cdot v_k(P_s, P_j)\}.$$

Apparently, the optimal objective value μ^* of problem (P) satisfies $F_k(\mu^*) = 0$. In other words, $F_k(\mu) = 0$ implies $\mu = \mu^*$. Therefore, solution of problem (P)

Algorithm 1: Dinkelbach-type Algorithm

$(P_s^{(i)}, P_j^{(i)})$: the i -th iteration of the transmit power for source node s and jammer node j .

$\mathcal{X}$: the feasible set of power parameters.

l : positive integer.

begin

Referring to Eq. (5.10) to Eq. (5.12),

Step 1: Take $(P_s^{(0)}, P_j^{(0)}) \in \mathcal{X}$, compute $\mu_1 = \max_k \{u_k(P_s^{(0)}, P_j^{(0)})/v_k(P_s^{(0)}, P_j^{(0)})\}$,
and let $l = 1$.

Step 2: Determine $(P_s^{(l)}, P_j^{(l)}) = \arg \min_{(P_s, P_j) \in \mathcal{X}} \left\{ \max_k \{u_k(P_s, P_j) - \mu_l v_k(P_s, P_j)\} \right\}$.

$$F_k(\mu_l) = \min_{(P_s, P_j) \in \mathcal{X}} \max_k \{u_k(P_s, P_j) - \mu_l v_k(P_s, P_j)\}.$$

Step 3:

if $F_k(\mu_l) = 0$ **then**

The optimal solution is $(P_s^*, P_j^*) = (P_s^{(l)}, P_j^{(l)})$ with optimal value $\mu^* = \mu_l$ and
Stop.

else

Let $\mu_{l+1} = \max_k \{u_k(P_s^{(l)}, P_j^{(l)})/v_k(P_s^{(l)}, P_j^{(l)})\}$, $l = l + 1$,
and go to **Step 2.**

end

end

can be achieved by finding a solution to $F_k(\mu) = 0$. Based on this observation, Dinkelbach-type algorithm solves a subproblem (P_μ) in each step, generating a sequence μ_l which converges to the optimal objective value μ^* of problem (P) . The detailed process is described in Algorithm 1.

5.3.1.3 Low-Complexity Optimization Leveraging Lower Bound

Similarly, the lower bound of the optimization problem in full CSI case is further discussed in this subsection.

Firstly, Eq. (5.4) is rewritten as

$$C_{s,j,k}(P_s, P_j) = q_j \left[\log_2 \left(1 + \frac{\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right) \right]^+ + (1 - q_j) \left[\log_2 \left(1 + \frac{P_s g_{sd} - P_s g_{sk}}{1 + P_s g_{sk}} \right) \right]^+.$$

Applying inequality $[\ln(1 + x)]^+ \geq \left[\frac{2x}{2+x} \right]^+$, gives

$$\ln 2 \cdot C_{s,j,k}(P_s, P_j) \geq \frac{2q_j}{2 \left[\frac{\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right]^+ + 1} + \frac{2(1 - q_j)}{2 \left[\frac{1 + P_s g_{sk}}{P_s (g_{sd} - g_{sk})} \right]^+ + 1}.$$

Thus, the achievable secrecy rate from the s -th source node to d -th destination node against the k -th eavesdropper using the j -th cooperative jammer as shown in Eq. (5.4) can be lower bounded as:

$$C_{s,j,k}(P_s, P_j) \geq \frac{2q_j/\ln 2}{2 \frac{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{\left[\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right]^+} + 1} + \frac{2(1 - q_j)/\ln 2}{2 \left[\frac{1 + P_s g_{sk}}{P_s (g_{sd} - g_{sk})} \right]^+ + 1}. \quad (5.13)$$

Given the lower bound, our optimization problem in Eq. (5.7) can be relaxed as,

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \frac{2q_j/\ln 2}{2 \frac{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{\left[\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right]^+} + 1} + \frac{2(1 - q_j)/\ln 2}{2 \left[\frac{1 + P_s g_{sk}}{P_s (g_{sd} - g_{sk})} \right]^+ + 1}, \quad (5.14)$$

which can also be solved with GFP in terms of the Dinkelbach-type algorithm.

5.3.2 Secrecy Rate Maximization with Statistical CSI

This subsection focuses on the joint power optimization and cooperative nodes selection problem when only statistical CSI of all the links is available. Firstly, a direct solution to the optimization problem will be presented. Then, to reduce optimization complexity, an approximate solution will be determined by maximizing the lower bound on the expected secrecy rate.

5.3.2.1 Heuristic Simulated Annealing Based Direct Evaluation

The ergodic sum rate of the system is now maximized under the circumstances that only statistical CSI of g_{sd} , h_{jd} , g_{sk} , and h_{jk} can be acquired. Mathematically, the optimization problem in Eq. (5.7) can be reformulated as,

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \mathbb{E} \{C_{s,j,k}(P_s, P_j)\}, \quad (5.15)$$

where

$$\begin{aligned} \mathbb{E} \{C_{s,j,k}(P_s, P_j)\} &= q_j \left[\mathbb{E} \left\{ \log_2 \left(1 + \frac{P_s g_{sd}}{P_j h_{jd} + 1} \right) \right\} - \mathbb{E} \left\{ \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right\} \right]^+ \\ &\quad + (1 - q_j) \left[\mathbb{E} \{ \log_2 (1 + P_s g_{sd}) \} - \mathbb{E} \{ \log_2 (1 + P_s g_{sk}) \} \right]^+. \end{aligned} \quad (5.16)$$

In order to reduce the computation complexity, Eq. (5.16) can be reduced by evaluating the expectations. Specific details can be seen from the following Lemma 5.1, based on some derivations from [18, 19].

Lemma 5.1 For $X_1 \sim \text{Exp}(\alpha_1)$, $X_2 \sim \text{Exp}(\alpha_2)$, it holds that

$$\begin{aligned} \mathbb{E} \left[\ln(1 + P_1 X_1) \right] &= \phi(P_1 \alpha_1), \\ \mathbb{E} \left[\ln \left(1 + \frac{P_2 X_2}{1 + P_1 X_1} \right) \right] &= \frac{[\phi(P_2 \alpha_2) - \phi(P_1 \alpha_1)]}{1 - \frac{P_1 \alpha_1}{P_2 \alpha_2}}, \end{aligned}$$

where $\phi(x) = e^{1/x} E_1(1/x)$, $E_1(x) = \int_x^\infty \frac{1}{t} e^{-t} dt$, $x \geq 0$.

Proof First, we expand the expectation $\mathbb{E}[\ln(1 + P_1 X_1)]$,

$$\mathbb{E}[\ln(1 + P_1 X_1)] = \int_0^\infty \frac{1}{\alpha_1} e^{-\frac{x}{\alpha_1}} \ln(1 + P_1 x) dx.$$

Using Eq. (9) on page 194 of [19], we have

$$\int_0^\infty \frac{1}{\alpha_1} e^{-\frac{x}{\alpha_1}} \ln(1 + P_1 x) dx = e^{\frac{1}{P_1 \alpha_1}} E_1 \left(\frac{1}{P_1 \alpha_1} \right) = \phi(P_1 \alpha_1).$$

Similarly, $\mathbb{E} \left[\ln \left(1 + \frac{P_1 X_1}{1 + P_2 X_2} \right) \right]$ can be expanded as,

$$\begin{aligned} &\mathbb{E} \left[\ln \left(1 + \frac{P_1 X_1}{1 + P_2 X_2} \right) \right] \\ &= \int_0^\infty \frac{1}{\alpha_2} e^{-\frac{x}{\alpha_2}} \left[\int_0^\infty \ln \left(1 + \frac{P_1 y}{1 + P_2 x} \right) \frac{1}{\alpha_1} e^{-\frac{y}{\alpha_1}} dy \right] dx \\ &= \int_0^\infty \frac{1}{\alpha_2} e^{-\frac{x}{\alpha_2}} dx \int_0^\infty \ln \left(1 + \frac{y}{(1 + P_2 x)/(\alpha_1 P_1)} \right) e^{-y} dy \\ &= \int_0^\infty \frac{1}{\alpha_2} e^{-\frac{x}{\alpha_2}} e^{(1 + P_2 x)/(\alpha_1 P_1)} E_1((1 + P_2 x)/(\alpha_1 P_1)) dx \\ &= \int_{\frac{1}{P_1 \alpha_1}}^\infty \left(\frac{P_1 \alpha_1}{P_2 \alpha_2} \right) e^{\frac{1}{P_2 \alpha_2}} \exp \left[\left(1 - \frac{P_1 \alpha_1}{P_2 \alpha_2} \right) z \right] E_1(z) dz. \end{aligned}$$

Defining $\xi = P_1 \alpha_1 / (P_2 \alpha_2)$, and using Eq. (3) on Page 197 of [19], and Eq. (12) on page 308 of [20], we have,

$$\int_{\frac{1}{P_1 \alpha_1}}^\infty \left(\frac{P_1 \alpha_1}{P_2 \alpha_2} \right) e^{\frac{1}{P_2 \alpha_2}} \exp \left[\left(1 - \frac{P_1 \alpha_1}{P_2 \alpha_2} \right) z \right] E_1(z) dz$$

$$\begin{aligned}
&= \xi e^{\frac{1}{P_2\alpha_2}} \int_{\frac{1}{P_1\alpha_1}}^{\infty} e^{(1-\xi)x} E_1(x) dx \\
&= \xi e^{\frac{1}{P_2\alpha_2}} \left(\int_0^{\infty} e^{(1-\xi)x} E_1(x) dx - \int_0^{\frac{1}{P_1\alpha_1}} e^{(1-\xi)x} E_1(x) dx \right) \\
&= \xi e^{\frac{1}{P_2\alpha_2}} \left(\frac{1}{\xi-1} \ln \xi - \frac{1}{\xi-1} \left[-e^{\frac{(1-\xi)}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) + \ln \xi + E_1\left(\frac{\xi}{P_1\alpha_1}\right) \right] \right) \\
&= \frac{\xi}{\xi-1} \left(e^{\frac{1}{P_2\alpha_2}} e^{\frac{(1-\xi)}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) - e^{\frac{1}{P_2\alpha_2}} E_1\left(\frac{\xi}{P_1\alpha_1}\right) \right) \\
&= \frac{\frac{P_1\alpha_1}{P_2\alpha_2}}{\frac{P_1\alpha_1}{P_2\alpha_2} - 1} \left(e^{\frac{1}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) - e^{\frac{1}{P_2\alpha_2}} E_1\left(\frac{1}{P_2\alpha_2}\right) \right) \\
&= \frac{\phi(P_1\alpha_1) - \phi(P_2\alpha_2)}{1 - \frac{P_2\alpha_2}{P_1\alpha_1}}.
\end{aligned}$$

Applying the Lemma 5.1, the optimization problem in Eq. (5.16) can be expressed as

$$\begin{aligned}
\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} & \left\{ \frac{q_j}{\ln 2} \left[\frac{\phi(P_s \lambda_{sd}) - \phi(P_j \lambda_{jd})}{1 - \frac{P_j \lambda_{jd}}{P_s \lambda_{sd}}} - \frac{\phi(P_s \lambda_g) - \phi(P_j \lambda_h)}{1 - \frac{P_j \lambda_h}{P_s \lambda_g}} \right]^+ \right. \\
& \left. + \frac{(1-q_j)}{\ln 2} [\phi(P_s \lambda_{sd}) - \phi(P_s \lambda_h)]^+ \right\}. \quad (5.17)
\end{aligned}$$

5.3.2.2 Ergodic Lower Bound for Complexity Reduction

The achievable ergodic secrecy rate shown in Eq. (5.17) can be lower bounded as

$$\begin{aligned}
\mathbb{E} \{C_{s,j,k}(P_s, P_j)\} &\geq q_j \left[\frac{\phi(P_s \lambda_{sd}) - \phi(P_j \lambda_{jd})}{\ln 2 \cdot \left(1 - \frac{P_j \lambda_{jd}}{P_s \lambda_{sd}}\right)} - \log_2 \left(1 + \frac{P_s \lambda_{sk}}{P_j \lambda_h} \phi(P_j \lambda_h)\right) \right]^+ \\
&+ (1-q_j) \left[\frac{\phi(P_s \lambda_{sd})}{\ln 2} - \log_2(1 + P_s \lambda_g) \right]^+, \quad (5.18)
\end{aligned}$$

which can also be proved from the Jensen's inequality as similar with the Eq. (1.15), and the derivations are omitted in this part.

Leveraging the conclusion in Eq. (5.18), a lower bound on the objective function can be maximized, i.e., the following lower bound on the ergodic sum rate can be maximized to achieve optimized transmit powers.

$$\begin{aligned} \max_{(P_s, P_j) \in \mathcal{R}} \min_{k \in \mathcal{K}} \left\{ q_j \left[\frac{\phi(P_s \lambda_{sd}) - \phi(P_j \lambda_{jd})}{\ln 2 \cdot \left(1 - \frac{P_j \lambda_{jd}}{P_s \lambda_{sd}}\right)} - \log_2 \left(1 + \frac{P_s \lambda_{sk}}{P_j \lambda_h} \phi(P_j \lambda_h)\right) \right]^+ \right. \\ \left. + (1 - q_j) \left[\frac{\phi(P_s \lambda_{sd})}{\ln 2} - \log_2(1 + P_s \lambda_g) \right]^+ \right\}. \end{aligned} \quad (5.19)$$

Thus far, the sum secrecy rate has been considered under the assumptions of both full CSI and statistical CSI, respectively. The brute force search and SA were both used to solve the optimization problem in Eqs. (5.7) and (5.17). Also, low-complexity optimization problems based on bounds of the secrecy rate were developed. To further reduce the computation complexity, a one dimensional search with low complexity is proposed in the following to solve the optimization problems with little performance loss.

5.3.3 One-Dimensional Search with Low Complexity

Recall that the brute-force approach is an available algorithm to solve the optimization problem, which must search over a 2-dimensional (2-D) space of (P_s, P_j) for every k . To reduce the computation complexity, a lower complexity algorithm which is suggested by focusing on a one-dimensional (1-D) space is presented in this subsection with little performance loss.

Proposition 5.1 *The optimal solution (P_s, P_j) to maximize the sum secrecy rate of Eq. (5.4), Eq. (5.11), Eq. (5.14) and the ergodic sum rate of Eq. (5.17) and Eq. (5.19) must satisfy $P_s = P_s^{\max}$ or $P_s + P_j = P_{\max}$.*

Proof Taking the optimization problem in Eq. (5.4) for example, the expression of achievable secrecy rate can be rewritten as

$$\begin{aligned} C_{s,j,k}(P_s, P_j) & \quad (5.20) \\ &= q_j \left[\log_2 \left(\frac{1 + \frac{P_s g_{sd}}{P_j h_{jd} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right) \right]^+ + (1 - q_j) \left[\log_2 \left(\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} \right) \right]^+ \\ &= q_j \log_2 \left(1 + \left[\frac{\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right]^+ \right) + (1 - q_j) \log_2 \left(1 + \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}} \right) \\ &= q_j \log_2 \left(1 + \left[\frac{\frac{g_{sd}}{P_j h_{jd} + 1} - \frac{g_{sk}}{P_j h_{jk} + 1}}{\frac{1}{P_s} + \frac{g_{sk}}{P_j h_{jk} + 1}} \right]^+ \right) + (1 - q_j) \log_2 \left(1 + \frac{[g_{sd} - g_{sk}]^+}{\frac{1}{P_s} + g_{sk}} \right). \end{aligned}$$

Table 5.1 Main abbreviations of simulation results

Abbreviations	Explanations
BF	Brute force search is used to optimize the objective function
DE-SA	The optimization problem is solved by direct evaluation by utilizing SA
LB-SA	The optimization problem is solved by leveraging the lower bound solved by SA
UB-D	The optimization problem is solved by leveraging the upper bound solved by Dinkelbach
LB-D	The optimization problem is solved by leveraging the lower bound solved by Dinkelbach
1-D, DE	The optimization problem is solved by direct evaluation leveraging the 1-D search
1-D, UB	The optimization problem is solved by upper bound leveraging the 1-D search
1-D, LB	The optimization problem is solved by lower bound leveraging the 1-D search

Table 5.2 Main simulation parameters

Parameters	Values
Bandwidth	20 MHz
Noise power (σ^2)	−96 dBm
Maximum transmit power of D2D transmitter ($P_{\max}^s$)	23 dBm
Maximum transmit power of jammer nodes ($P_{\max}^j$)	19 dBm
Maximum total sum power ($P_{\max}$)	24 dBm
Number of eavesdroppers (M)	4

Clearly, the secrecy rate increases monotonically with P_s . Without the joint power constraint in Eq. (5.3), the trivial solution $P_s = P_s^{\max}$ applies. With the joint power constraint $P_s + P_j \leq P_{\max}$, the optimal solution either reaches the upper limit of P_s or satisfies $P_s + P_j = P_{\max}$ to maximize the target secrecy and its corresponding bounds for both the full CSI case and statistical CSI model.

From Proposition 5.1, the optimization problem with two variables can be transformed into one with only a single variable. Thus, it suffices to implement the 1-D search to maximize the secrecy rate. For notational simplicity, the boundary is denoted as

$$\begin{aligned} \mathcal{L} &= \{(P_s, P_j) | P_s = P_s^{\max} \text{ or } P_s + P_j = P_{\max}\}, \\ \text{s.t. } & 0 \leq P_s \leq P_s^{\max}, 0 \leq P_j \leq P_j^{\max}. \end{aligned} \quad (5.21)$$

Instead of the exhaustive 2-D search over the plane $[0, P_s^{\max}] \times [0, P_j^{\max}]$, the proposed 1-D search over $\mathcal{L}$ can significantly reduce the computation complexity.

5.3.4 Simulation and Numerical Results

Different methods have been adopted to optimize P_s and P_j to maximise the secrecy rate of D2D links. The label “1-D” indicates that the power optimization has been simplified into a problem with only one variable, and other methods without “1-D” means that the power optimization is made over the 2-D space of (P_s, P_j) . The main related abbreviations of simulation results are listed in Table 5.1. Additionally, large scale path-loss exponents between any two user nodes are assumed to be the same and equal to 4. Other simulation parameters are listed in Table 5.2.

5.3.4.1 Impact of Number of Jammer Nodes and Sum Transmit Power Limitation

- **Full CSI Case**

Figure 5.3 illustrates the achievable secrecy rate and simulation time comparison of the algorithms under the assumption of full CSI. Clearly, by increasing number N of cooperative jammer nodes, both secrecy rate and simulation time grow as shown in Fig. 5.3. More candidate cooperative jammer nodes provide for more choices and possibly better cooperative jammer selection to combat eavesdropping, thereby achieving better performance. Meanwhile, since the power optimization should be executed for every potential cooperative jammer node during the selection step, the computational time grows with more candidate cooperative jammer nodes. It is also natural that a larger $P_{\max}$ achieves better performance for all the optimization problems by comparing the two parts in Fig. 5.3. If a more flexible power allocation is available for the source node and cooperative jamming nodes, then a better power allocation can be found for higher achievable secrecy rate.

Generally, the brute force search and the direct evaluation via simulated annealing achieve nearly the same performance, as expected. The approximation methods via upper-bound and lower-bound optimization lead to somewhat worse performance, although the performance gaps among these methods are rather small. Therefore, our proposed simulated annealing optimization demonstrates little performance loss as seen from Fig. 5.3a. However, it still consumes substantial computation time as shown in Fig. 5.3b. Observe that the upper-bound and lower-bound optimization methods combined with the process of narrowing the candidate source set provides a very good performance-complexity tradeoff. It exhibits very little loss in terms of secrecy rate, while achieving orders of magnitude reduction in complexity.

- **Statistical CSI Case**

Figure 5.4 illustrates the performance comparison of different algorithms under the assumption of statistical CSI. Similar to the full CSI scenario, for all optimization cases, more jammers lead to better performance and higher complexity, and larger secrecy rate can be achieved with a larger $P_{\max}$ as shown in Fig. 5.4. Specifically,

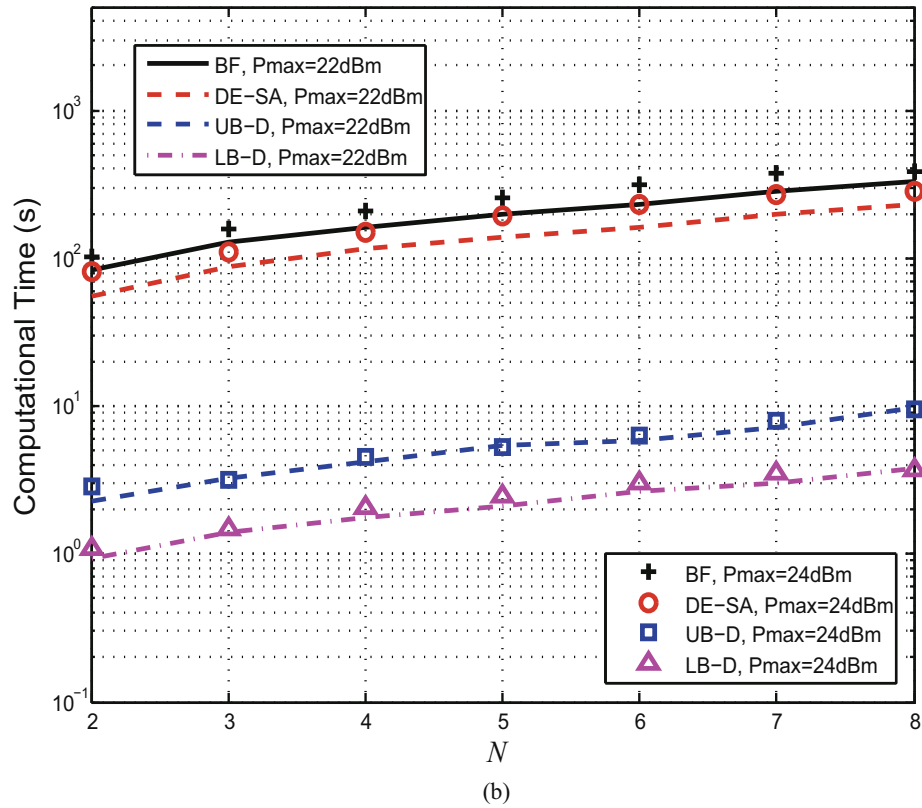
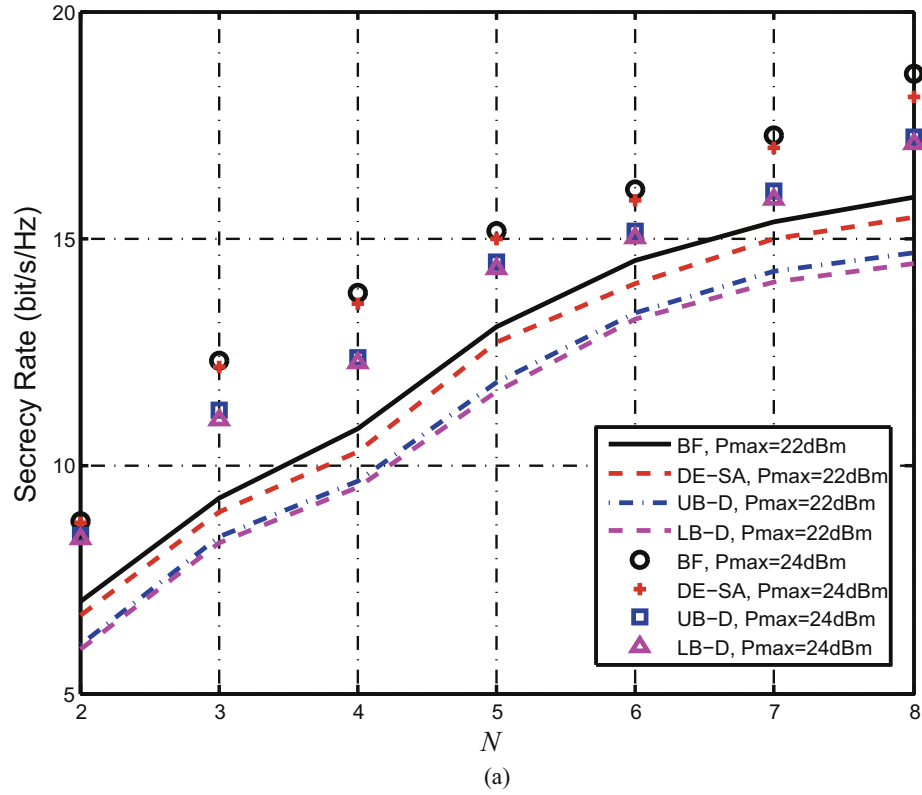


Fig. 5.3 Achievable secrecy rate in full CSI model. $S = 4$, $q_j = 0.8$, $\theta_{\min} = 0.5$. (a) Achievable secrecy rate. (b) Computational time

the brute force search and the SA solution achieve very similar secrecy rate, and the proposed lower bound optimization yields lower secrecy rate, though the performance gaps among different methods remain small as shown in Fig. 5.4a.

Focusing on the simulation time as measure of computation complexity in Fig. 5.4b, similarly, the proposed low-complexity optimization method, by narrowing the candidate source set and optimizing the lower bound of the original secrecy rate, presents a good tradeoff between complexity and performance. Suffering little performance loss, it consumes dramatically less time as seen from Fig. 5.4b.

5.3.4.2 Impact of Searching Dimension over Transmission Power

It should be noted that for the fact that the methods using the procedure of narrowing candidate source set sacrifice little secrecy rate. Thus all the methods involved in this part have narrowed the candidate source set before cooperative jamming node selection and power optimization unless otherwise specified. The label “1-D” indicates that the power optimization has been simplified into a problem with only one variable.

- **Full CSI Case**

Figure 5.5 illustrates the performance and complexity comparison of different optimization algorithms under full CSI case. Naturally, the achievable secrecy rate of the D2D links increases with the number of source nodes, since more source nodes make it more likely for a better option. It can be seen that although the direct evaluation outperforms the proposed upper-bound method and lower-bound method as expected, the performance gap is insignificant, as shown in Fig. 5.5a. While the proposed 1-D search methods achieve identical performance as the 2-D search method, but the computation time difference are very significant as shown in Fig. 5.5b. Observably, a larger number of source nodes leads to higher complexity.

- **Statistical CSI Case**

Figure 5.6 illustrates the performance and complexity comparison of different optimization algorithms under statistical CSI assumption. Similarly, the achievable secrecy rate of the D2D links and the computation time increase with the number of source nodes in statistical CSI case. Meanwhile, the direct evaluation outperforms the proposed lower-bound method as expected. Again, the proposed 1-D search method for statistical CSI case achieves identical performance while consuming much less time than 2-D search, as shown in Fig. 5.6a, b, respectively. Thus, a 1-D search for power is adopted for optimization in the sequel unless specified otherwise.

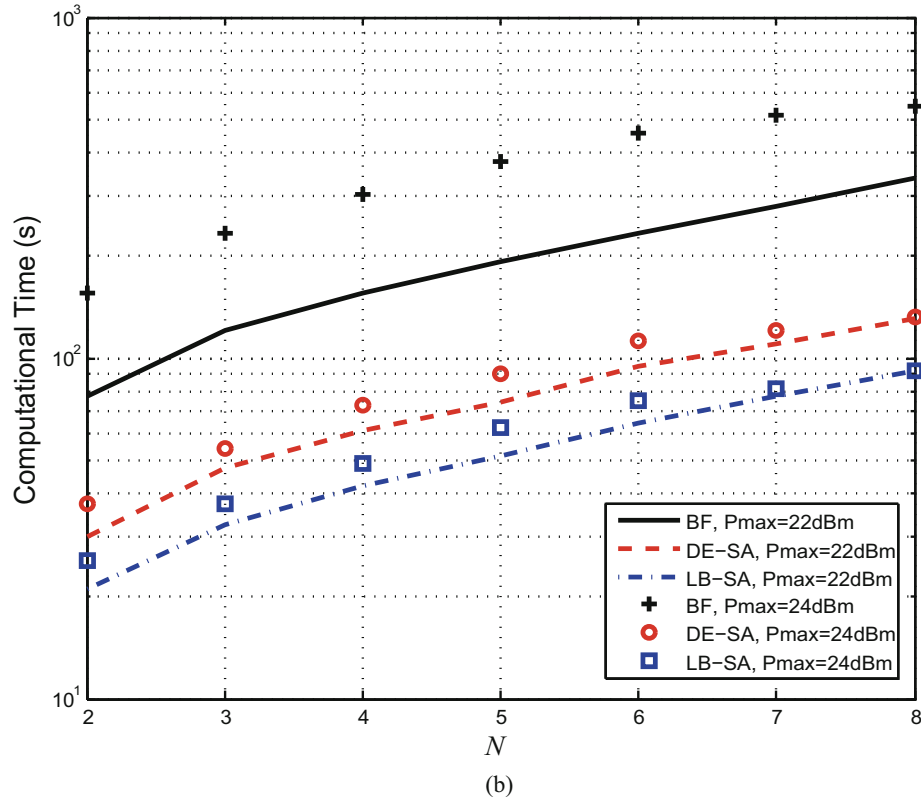
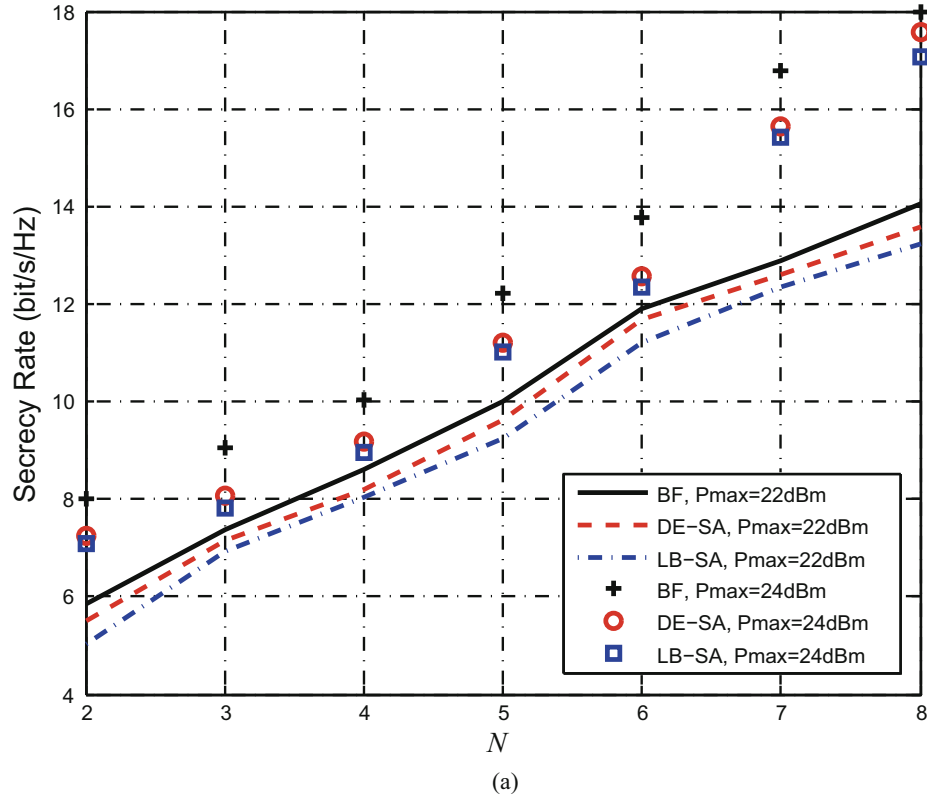


Fig. 5.4 Achievable secrecy rate in statistical CSI model. $S = 4, q_j = 0.8, \theta_{\min} = 0.5$. (a) Achievable secrecy rate. (b) Computational time

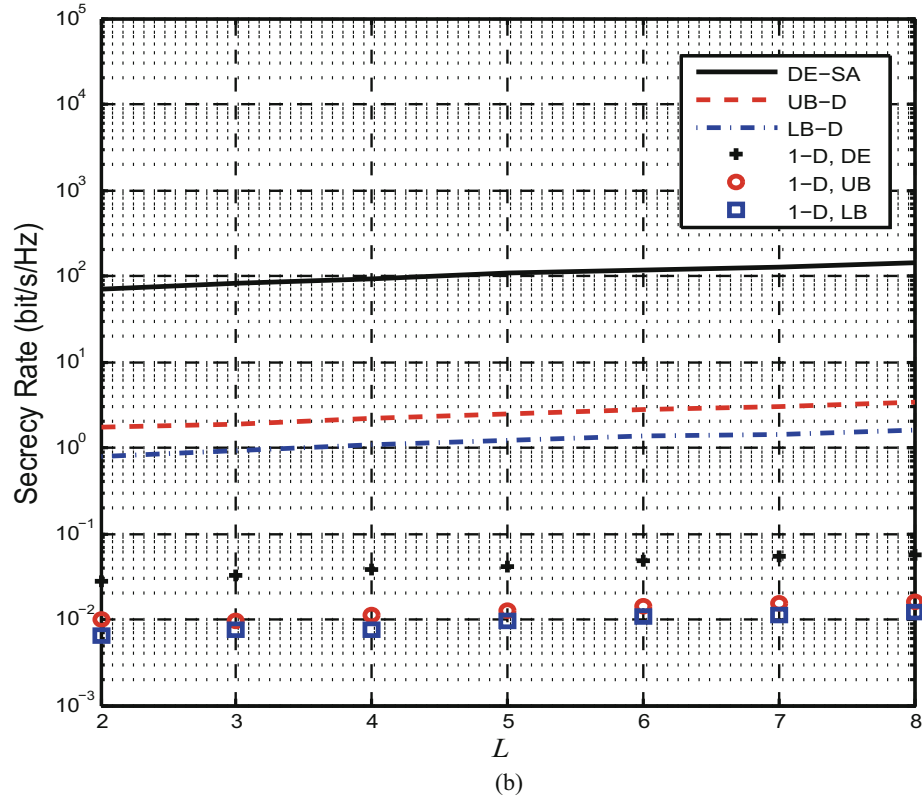
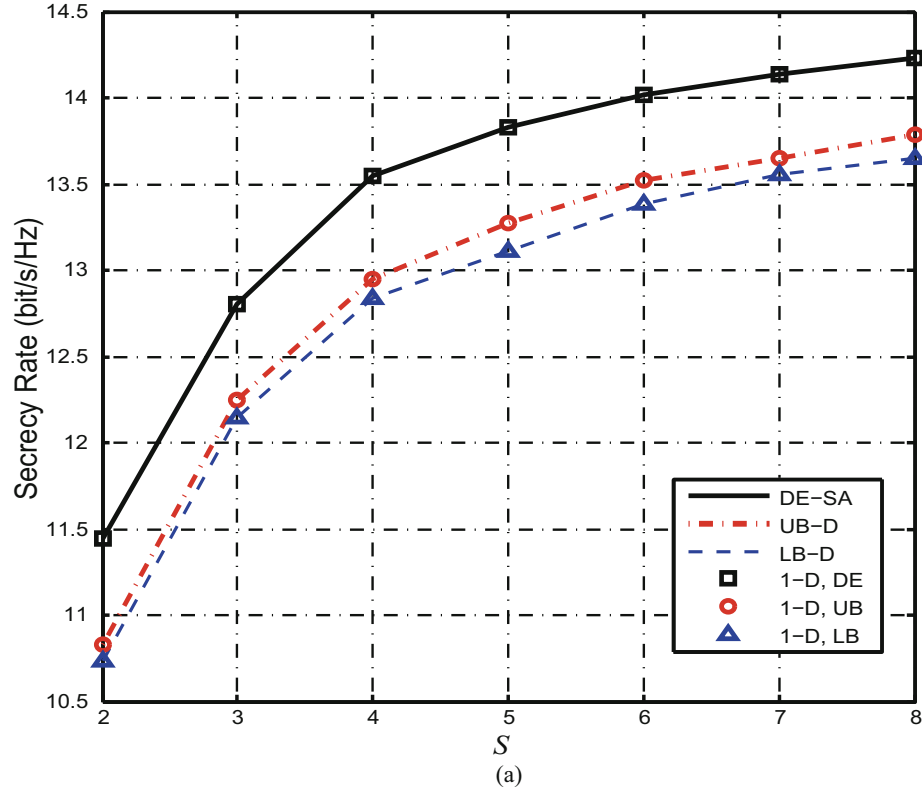
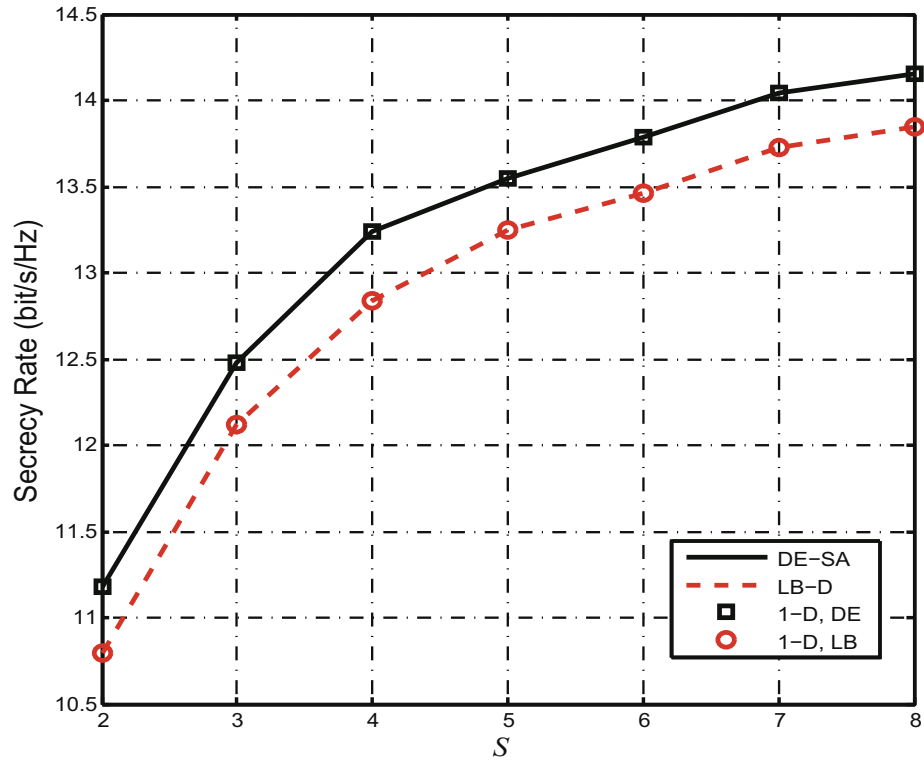
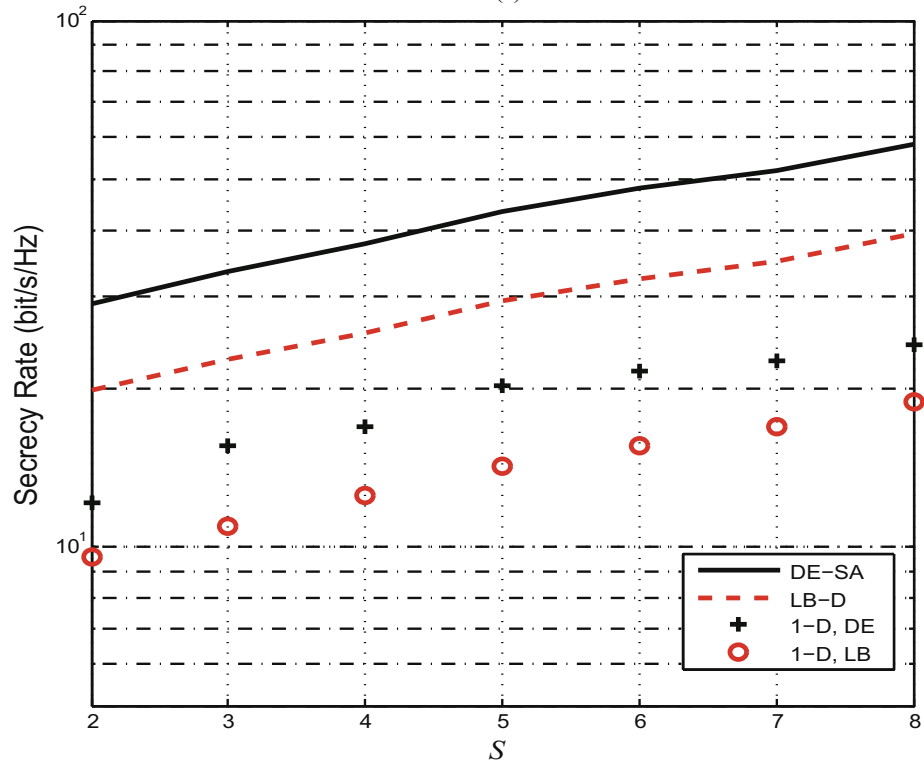


Fig. 5.5 Performance comparison of different optimization methods in full CSI case. $N = 5$, $q_j = 0.8$, $\theta_{\min} = 0.5$. (a) Achievable secrecy rate. (b) Computational time



(a)



(b)

Fig. 5.6 Performance comparison of different optimization methods in statistical CSI case. $N = 5$, $q_j = 0.8$, $\theta_{\min} = 0.5$. (a) Achievable secrecy rate. (b) Computational time

5.3.4.3 Impact of Social Characteristics Consideration

- **Impact of Success Rate Threshold**

Figure 5.7 illustrates the impact of success rate threshold, $\theta_{\min}$, on achievable performance. It can be seen from Fig. 5.7 that both the achievable secrecy rate and the corresponding computational time decline with larger $\theta_{\min}$. With increasing $\theta_{\min}$, more source nodes with success probability lower than $\theta_{\min}$ will be excluded from $\mathcal{S}_T$, leading to faster selection and optimization. However, a higher $\theta_{\min}$ may result in the elimination of source nodes with a prominent physical link but less contact duration, i.e., low success probability. Since such source nodes may potentially have the best resistance capability to eavesdropping due to their physical location, their exclusion may result in poor performance.

On the other hand, when the value of $\theta_{\min}$ is relatively small, the decrease in achievable secrecy rate is negligible, but the reduction of computational time is not satisfying. Generally, the larger $\theta_{\min}$ is, the more the secrecy performance will be sacrificed but more computing time will be saved as well. Therefore, the choice of $\theta_{\min}$ is key to the tradeoff between secrecy performance and computational time.

- **Socially Stable Source Node Selection**

The impact of social interaction on achievable secrecy rate is further investigated as shown in Fig. 5.8. The labels “No Social Interaction” and “With Social Interaction” are used to denote cases when the social interaction is not considered or considered, respectively, for cooperative source and jammer node selection and power allocation. Naturally, a larger $P_{\max}$ allows source and jamming nodes to find a better power allocation and consequently, a higher secrecy rate. Meanwhile, when ignoring social interaction between source and destination nodes, the secrecy rate drops since nodes selected for transmission may have low contact duration with the destination, thereby failing in content delivery. Conversely, consideration of social behavior of candidate source nodes leads to a better performance.

- **Socially Trusted Jammer Node Selection**

In Fig. 5.9, labels “No Social Trust” and “With Social Trust” are used here to denote the cases when the social trust of jammers is not considered versus considered, respectively. Similar to the results in Fig. 5.8, a larger secrecy rate can be achieved with a larger $P_{\max}$ regardless of social trust assumption as shown in Fig. 5.9. Without exploiting knowledge of social trust of cooperative jamming nodes, the secrecy rate will suffer as unreliable jamming partners may be selected. On the other hand, better performance can be achieved by giving consideration to the social trust of candidate cooperative jammers.

- **Social Characteristics Estimation Error**

The social characteristics and social relationship among different nodes (i.e., users) is time varying and the estimation of social interaction and social trust index is prone to errors. To illustrate the robustness of our approach, the impact of estimation errors

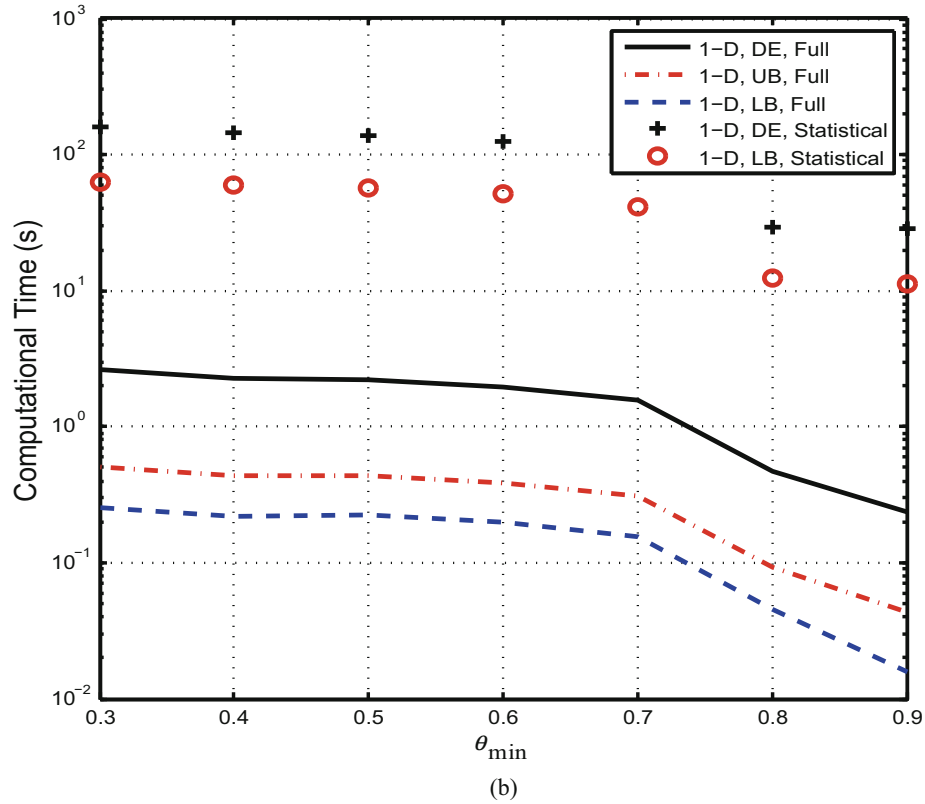
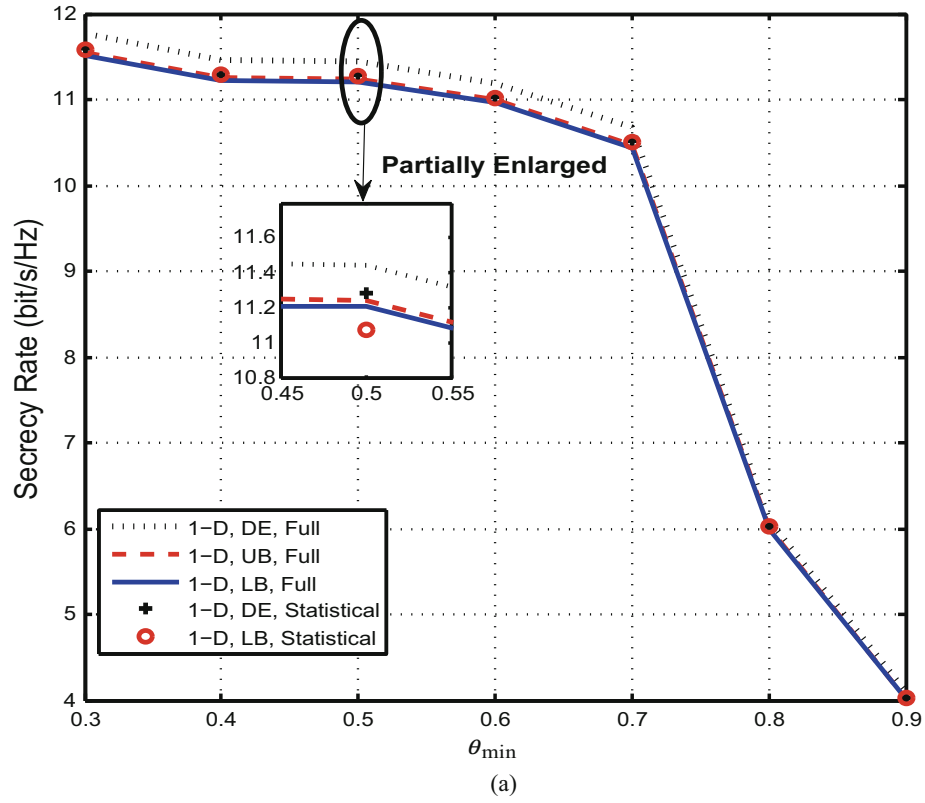


Fig. 5.7 Performance comparison with different success rate threshold. $S = 4, N = 5, q_j = 0.8$.
(a) Achievable secrecy rate. **(b)** Computational time

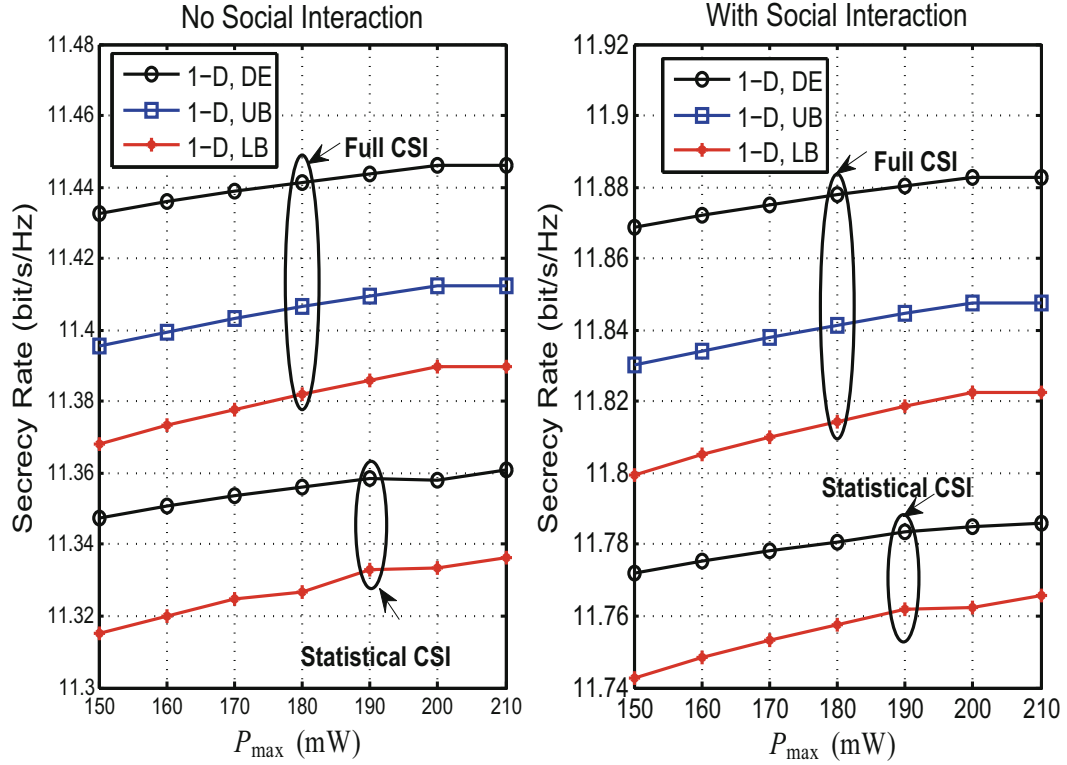


Fig. 5.8 Performance comparison with different social interaction assumptions. $S = 4, N = 5, \theta_{\min} = 0.5$

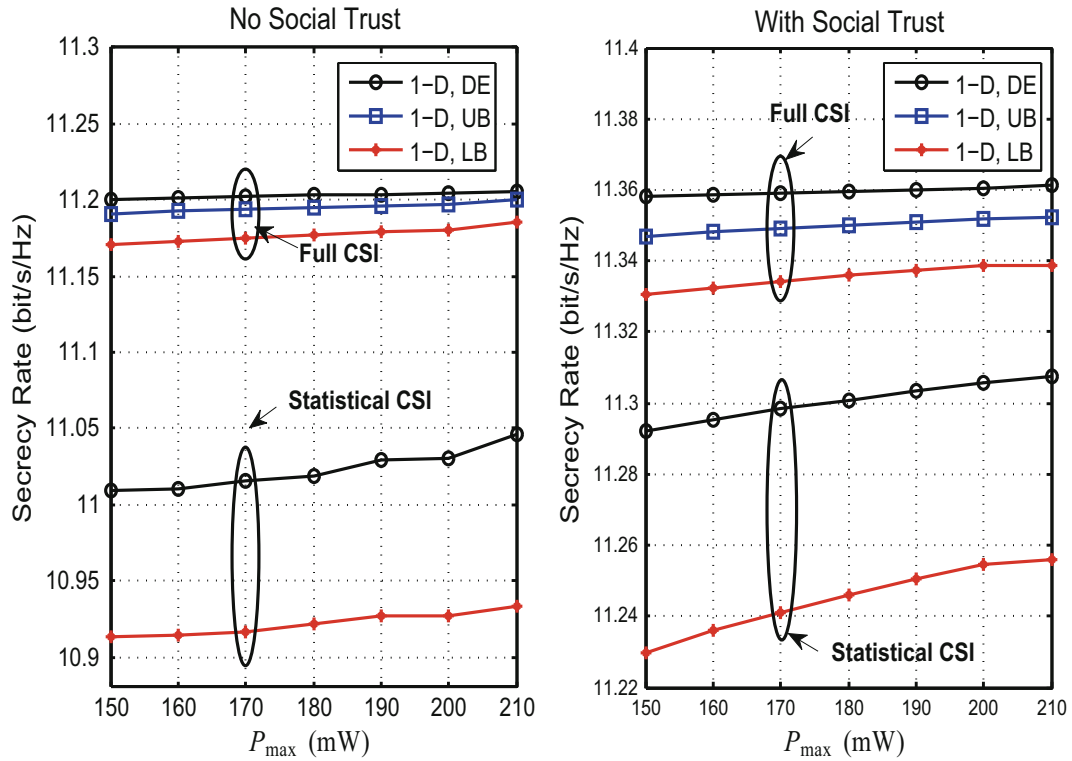


Fig. 5.9 Performance comparison with different social trust assumptions. $S = 4, N = 5, \theta_{\min} = 0.5$

of the social information index (including social interaction of candidate source nodes and social trust index of jammer nodes) on the achievable performance should be considered. In particular, let the estimated social trust index, the true social trust index, and the social trust index estimation error be $\tilde{q}_j$, $\hat{q}_j$, and Δq_j , respectively. They are related as

$$\tilde{q}_j = \hat{q}_j + \Delta q_j. \quad (5.22)$$

The normalized estimation error $\delta_q = |\Delta q_j / \hat{q}_j|$ characterizes the relative uncertainty of the social trust index. The parameter δ_T here characterizes the estimation error of social contact duration between mobile users. By using the estimated social characteristic index in the proposed algorithms, the secrecy rate and the ergodic secrecy rate are both affected and the impact of social characteristic index uncertainty can be assessed accordingly.

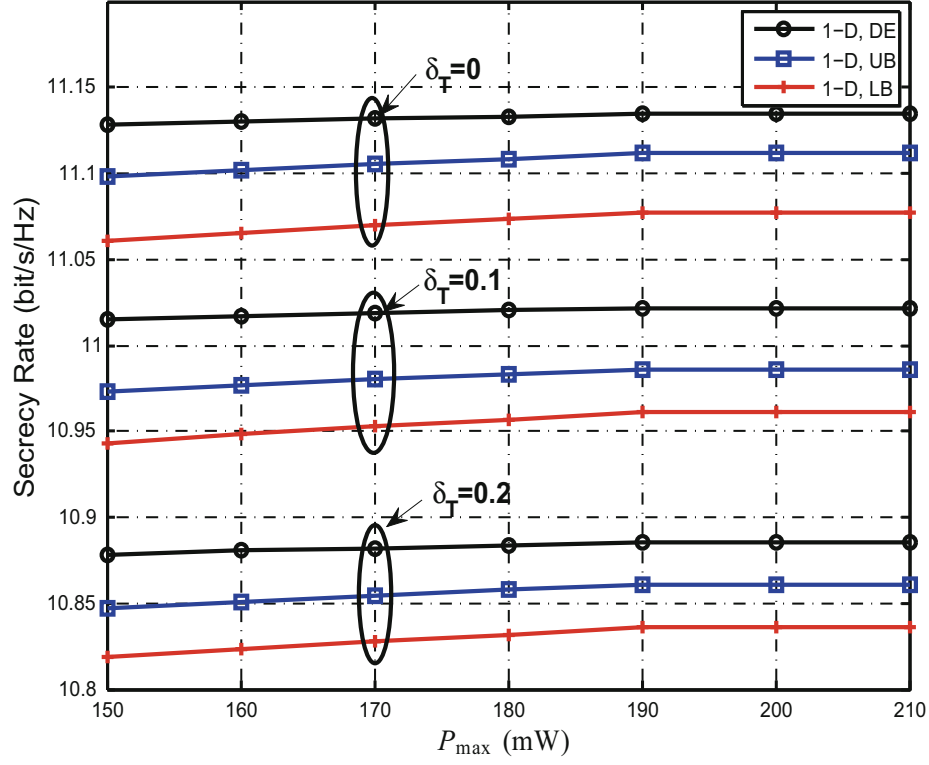
To illustrate the robustness of our approach, the impact of inaccurate social information indices with different estimation errors is shown in Fig. 5.10. Normally, the achievable secrecy rate increases with higher $P_{\max}$. However, a larger estimation error of δ_T and δ_q leads to a lower secrecy rate as expected. Nevertheless, the proposed optimization methods remain robust to such errors with graceful performance degradation.

5.4 The Social Interaction Case for Jammer Selection

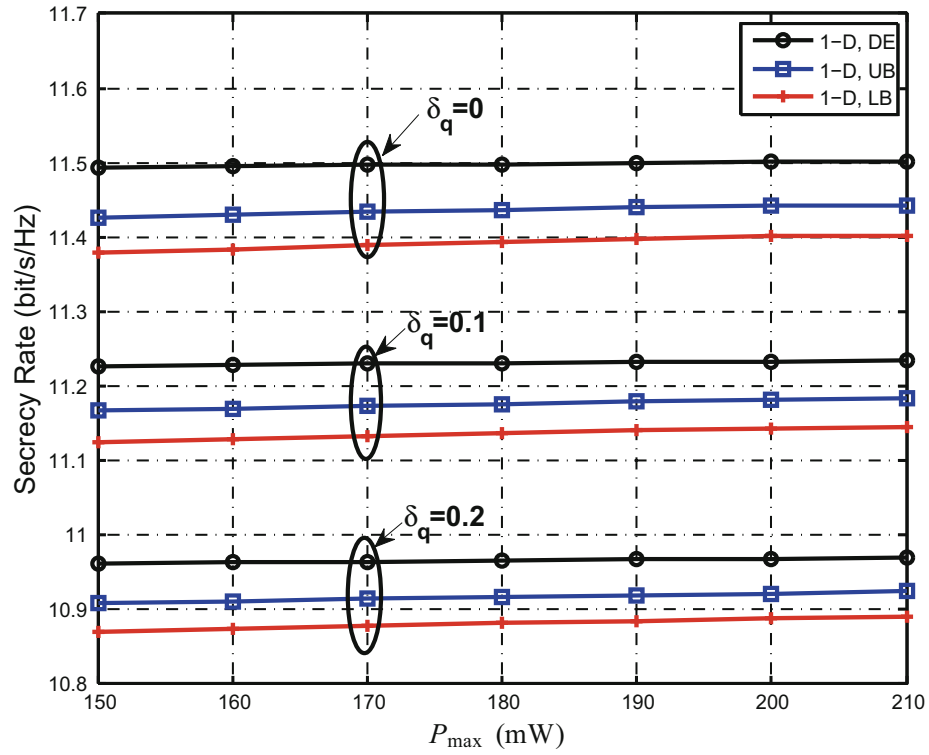
After the source nodes are firstly selected considering their social interaction, the selection of the cooperative jamming partners are mainly discussed in this subsection. In a special and simple case, we can assume that there only exists one source node, and the social trust for jammer selection is mainly considered under the full CSI case and the partial CSI case, respectively. It should be noted that though there exists interference from the candidate jammers to the destination node, it can be known in advance and suppressed at the destination in a certain way. In addition to the Heuristic Genetic algorithm, the low-complexity approximate algorithms are also presented here to obtain the optimized results.

5.4.1 Optimal Jammer Selection with Full CSI

In this subsection, we focus on how to select the best jamming partner to hamper reception by the smartest social eavesdropper in D2D overlay for secrecy guarantee and high quality transmission, and it is assumed that BS can acquire accurate CSI of all involved links without considering the jamming interference at the destination. Meanwhile, one source node is considered, i.e., $S = 1$, thus the symbol s in the following objective function only stands for the source node, but not a variable.



(a)



(b)

Fig. 5.10 Performance comparison with different social information estimation error in full CSI case. $S = 4$, $N = 5$, $\theta_{\min} = 0.5$. (a) Impact of social interaction index estimation error. (b) Impact of social trust index estimation error

Thus, the problem Eq. (5.4) can be relaxed as

$$C_{j,k}(P_s, P_j) = q_j \left[\log_2(1 + P_s g_{sd}) - \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right]^+ \quad (5.23)$$

$$+ (1 - q_j) [\log_2(1 + P_s g_{sd}) - \log_2(1 + P_s g_{sk})]^+.$$

The optimization problem in Eq. (5.23) is non-convex, and its solution can be found by using genetic algorithm (GA) [21].

5.4.1.1 Heuristic Genetic Algorithm Based Direct Evaluation

GA is a well-known heuristic optimization algorithm that imitates some processes in natural evolution. Following the model of evolution, GA establishes a population of individuals, each corresponds to a point in the search space. Using well-conceived operations, the next generation is formed based on the survival of the fittest. Therefore, the evolution from one generation to the next tends to result in potentially better solutions in the search space. Studies have shown that GA can possibly converge to global optima for a large class of non-convex problems [22].

In the situation that optimal jammer selection with full CSI, for a given set of eavesdropper and jammer, the values of q_j , g_{sd} , g_{sk} , and h_{jk} are determined. Therefore, variables of the optimization problem in Eq. (5.23) are P_s and P_j . Detailed, we can use the following four steps to obtain the optimal solution of Eq. (5.23).

- Step 1: Randomly create a population of individuals, representing an initial set of P_s and P_j ;
- Step 2: Every individual in the population is evaluated by fitness values, which are associated with values of $C_{j,k}$;
- Step 3: The population is evolved to form a new one by selection, crossover and mutation. New population usually indicates more suitable P_s and P_j which lead to a larger $C_{j,k}$;
- Step 4: Go to Step 2 unless the termination condition is satisfied.

After several iterations, GA will converge to the best individual, which hopefully represents the optimal or suboptimal solution to the optimization problem. In other words, the finally generated individuals are the optimal or suboptimal transmit powers for D2D transmitter and the corresponding jamming partner, P_s, P_j , for the optimization problem.

Obviously, the heuristic GA has the potential to converge to a global optimum. However, this heuristic algorithm does not provide a (worst-case) performance guarantee. In order to reduce computation complexity, the upper and lower bounds of the original secrecy rate are utilized for making comparisons.

5.4.1.2 Complexity Reduction Leveraging Upper Bound

Similar to the discussion in Sect. 5.3.1.2, using the well-known inequality $\ln(x) \leq x - 1$ for any $x > 0$, we have

$$\begin{aligned}
 \ln 2 \cdot C_{j,k}(P_s, P_j) &= q_j \left[\ln \frac{1 + P_s g_{sd}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right]^+ + (1 - q_j) \left[\ln \frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} \right]^+ \\
 &\leq q_j \left[\frac{1 + P_s g_{sd}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} - 1 \right]^+ + (1 - q_j) \left[\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} - 1 \right]^+ \\
 &= q_j \left[\frac{P_s g_{sd} - \frac{P_s g_{sk}}{P_j h_{jk} + 1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right]^+ + (1 - q_j) \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}}, \quad (5.24)
 \end{aligned}$$

using the j -th jammer to intercept the k -th eavesdropper.

In practical, interference from jammer to eavesdropper is usually dominant over background noise, i.e., $P_j h_{jk} \gg 1$. Thus, $P_j h_{jk} + 1 \approx P_j h_{jk}$, which can be used to further simplify Eq. (5.24). Hence the upper bound for the worst case can be approximated as

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \left\{ q_j \left[\frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}} \right]^+ + (1 - q_j) \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}} \right\}, \quad (5.25)$$

which can significantly reduce the complexity of optimization.

5.4.1.3 Complexity Reduction Leveraging Lower Bound

From $[\ln(1 + x)]^+ \geq \left[\frac{2x}{2+x} \right]^+$, we have

$$\begin{aligned}
 \ln 2 \cdot C_k(P_s, P_j, q_j) &= q_j \left[\ln \frac{1 + P_s g_{sd}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} \right]^+ + (1 - q_j) \left[\ln \frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} \right]^+ \\
 &\geq \frac{2q_j \left[\frac{1 + P_s g_{sd}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} - 1 \right]^+}{2 + \left[\frac{1 + P_s g_{sd}}{1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}} - 1 \right]^+} + \frac{2(1 - q_j) \left[\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} - 1 \right]^+}{2 + \left[\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} - 1 \right]^+}. \quad (5.26)
 \end{aligned}$$

Similarly, it is supposed that the interference from jammer to eavesdropper is dominant comparing to the background noise, i.e., $P_j h_{jk} \gg 1$, and $P_j h_{jk} + 1 \approx P_j h_{jk}$.

Hence optimization problem can be approximated to the following problem,

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_k \left\{ \frac{2q_j}{2 \left[\frac{P_j h_{jk} + P_s g_{sk}}{P_s P_j g_{sd} h_{jk} - P_s g_{sk}} \right]^+ + 1} + \frac{2(1 - q_j)}{2 \left[\frac{1 + P_s g_{sk}}{P_s (g_{sd} - g_{sk})^+} \right]^+ + 1} \right\}. \quad (5.27)$$

Let

$$\begin{aligned} f_1(P_s, P_j) &= 2 \left[\frac{P_j h_{jk} + P_s g_{sk}}{P_s P_j g_{sd} h_{jk} - P_s g_{sk}} \right]^+ + 1, \\ f_2(P_s, P_j) &= 2 \left[\frac{1 + P_s g_{sk}}{P_s (g_{sd} - g_{sk})^+} \right]^+ + 1. \end{aligned} \quad (5.28)$$

Equation (5.27) can be rewritten as,

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_k \left\{ \frac{2q_j}{f_1(P_s, P_j)} + \frac{2(1 - q_j)}{f_2(P_s, P_j)} \right\}. \quad (5.29)$$

Equivalently, the problem in Eq. (5.29) can be expressed as

$$\min_{(P_s, P_j) \in \mathcal{X}} \max_k \left\{ \frac{f_1(P_s, P_j) f_2(P_s, P_j)}{2q_j f_2(P_s, P_j) + 2(1 - q_j) f_1(P_s, P_j)} \right\} = \min_{(P_s, P_j) \in \mathcal{X}} \max_k \left\{ \frac{w_k(P_s, P_j)}{z_k(P_s, P_j)} \right\}. \quad (5.30)$$

Notice that the optimization problem is no-convex, since both $w_k(P_s, P_j)$ and $z_k(P_s, P_j)$ are nonlinear functions of P_s and P_j .

Similar with the Sect. 5.3.1.2, the Dinkelbach-type algorithm is applied here to solve the generalized fractional programming problem, and the details of the optimization using Dinkelbach-type Algorithm are given as Algorithm 2.

5.4.2 Optimal Jammer Selection with Partial CSI

In this subsection, joint power allocation with cooperative jammer selection in partial CSI case is considered, where instantaneous CSI of g_{sd} and h_{jd} , and statistical CSI of g_{sk} and h_{jk} are available.

5.4.2.1 Direct Evaluated Ergodic Sum Rate

Since only statistical CSI of g_{sk} and h_{jk} can be acquired by the BS, the maximization of sum rate of the system as shown in Eq. (5.7) can be changed into

$$\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \mathbb{E} \{ C_{j,k}(P_s, P_j) \}, \quad (5.31)$$

Algorithm 2: Dinkelbach-type Algorithm

$(P_s^{(i)}, P_j^{(i)})$: the i -th iteration of the transmit power for D2D transmitter and jammer node.
 $\mathcal{X}$: the feasible set of power parameters. l : the number of iteration.

begin

Referring to Eq. (5.28) and Eq. (5.30),

Step 1: Take $(P_s^{(0)}, P_j^{(0)}) \in \mathcal{X}$, compute $\mu_1 = \max_k \{w_k(P_s^{(0)}, P_j^{(0)})/z_k(P_s^{(0)}, P_j^{(0)})\}$,
and let $l = 1$.

Step 2: Determine $(P_s^{(l)}, P_j^{(l)}) = \arg \min_{(P_s, P_j) \in \mathcal{X}} \left\{ \max_k \{w_k(P_s, P_j) - \mu_l z_k(P_s, P_j)\} \right\}$.

$F_k(\mu_l) = \min_{(P_s, P_j) \in \mathcal{X}} \max_k \{w_k(P_s, P_j) - \mu_l z_k(P_s, P_j)\}.$

Step 3:

if $F_k(\mu_l) = 0$ **then**

The optimal solution is $(P_s^*, P_j^*) = (P_s^{(l)}, P_j^{(l)})$ with optimal objective value $\mu^* = \mu_l$ and **Stop**.

else

Go to **Step 4**;

end

Step 4: Let $\mu_{l+1} = \max_k \{w_k(P_s^{(l)}, P_j^{(l)})/z_k(P_s^{(l)}, P_j^{(l)})\}$,
let $l = l + 1$, and go to **Step 2**.

end

where

$$\begin{aligned}
\mathbb{E} \{C_{j,k}(P_s, P_j)\} = & q_j \left[\log_2(1 + P_s g_{sd}) - \mathbb{E} \left\{ \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right\} \right]^+ \\
& + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \mathbb{E} \{ \log_2(1 + P_s g_{sk}) \}]^+. \quad (5.32)
\end{aligned}$$

Recall that, the s is only a symbol that stands for the source node as aforementioned.

Applying the Lemma 5.1, the optimization problem in Eq. (5.31) can be expressed as,

$$\begin{aligned}
\max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \left\{ q_j \left[\log_2(1 + P_s g_{sd}) - \frac{\phi(P_s \lambda_g) - \phi(P_j \lambda_h)}{\ln 2 \cdot (1 - \frac{P_j \lambda_h}{P_s \lambda_g})} \right]^+ \right. \\
\left. + (1 - q_j) \left[\log_2(1 + P_s g_{sd}) - \frac{\phi(P_s \lambda_g)}{\ln 2} \right]^+ \right\}. \quad (5.33)
\end{aligned}$$

5.4.2.2 Complexity Reduction with Ergodic Lower Bound

By leveraging Jensen's inequality, the lower bound of the ergodic sum rate in Eq. (5.33) can be expressed as

$$\begin{aligned}
& q_j \left[\log_2(1 + P_s g_{sd}) - \mathbb{E} \left\{ \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right\} \right]^+ \\
& + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \mathbb{E} \{\log_2(1 + P_s g_{sk})\}]^+ \\
& \geq q_j \left[\log_2(1 + P_s g_{sd}) - \log_2 \left(1 + \mathbb{E} \left[\frac{P_s g_{sk}}{P_j h_{jk} + 1} \right] \right) \right]^+ \\
& + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \log_2(1 + \mathbb{E} [P_s g_{sk}])]^+ \\
& = q_j \left[\log_2(1 + P_s g_{sd}) - \log_2 \left(1 + P_s \lambda_g \mathbb{E} \left[\frac{1}{P_j h_{jk} + 1} \right] \right) \right]^+ \\
& + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \log_2(1 + P_s \lambda_g)]^+. \tag{5.34}
\end{aligned}$$

Using Eq. (6) on page 194 of [19], for $X \sim \text{Exp}(\lambda)$, we have,

$$\begin{aligned}
\mathbb{E} \left[\frac{1}{PX + 1} \right] &= \int_0^\infty \frac{1}{Px + 1} \frac{1}{\lambda} e^{-\frac{x}{\lambda}} dx = \int_0^\infty \frac{1}{P\lambda x + 1} e^{-x} dx \\
&= \frac{1}{P\lambda} \int_0^\infty \frac{1}{t + 1} e^{-\frac{1}{P\lambda} t} dt = \frac{1}{P\lambda} e^{\frac{1}{P\lambda}} E_1 \left(\frac{1}{P\lambda} \right) = \frac{\phi(P\lambda)}{P\lambda}. \tag{5.35}
\end{aligned}$$

Using Jensen's inequality in this case, therefore,

$$\mathbb{E} \left\{ \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right\} \leq \log_2 \left(1 + \frac{P_s \lambda_g}{P_j \lambda_h} \phi(P_j \lambda_h) \right), \tag{5.36}$$

$$\mathbb{E} \{\log_2(1 + P_s g_{sk})\} \leq \log_2(1 + P_s \lambda_g). \tag{5.37}$$

Thus, the problem can be optimized by maximizing the lower bound of the original objective function by considering power allocation, i.e. maximizing the lower bound of the ergodic sum rate:

$$\begin{aligned}
& \max_{(P_s, P_j) \in \mathcal{X}} \min_{k \in \mathcal{K}} \left\{ q_j \left[\log_2(1 + P_s g_{sd}) - \log_2 \left(1 + \frac{P_s \lambda_g}{P_j \lambda_h} \phi(P_j \lambda_h) \right) \right]^+ \right. \\
& \quad \left. + (1 - q_j) [\log_2(1 + P_s g_{sd}) - \log_2(1 + P_s \lambda_g)]^+ \right\}. \tag{5.38}
\end{aligned}$$

Although Eq. (5.38) is much simpler than Eq. (5.33), it is still a non-convex function, and the GA can also be used to accomplish the joint power optimization of P_s and P_j .

5.4.3 One Dimensional Search with Low Complexity

To further reduce the complexity of the proposed algorithm, a one-dimensional search is also presented here under the full CSI case. Considering the total transmission power constraint of P_j and P_s , the following Proposition 5.2 is presented firstly.

Proposition 5.2 *The optimal solution of Eq. (5.25) must satisfy $P_s + P_j = \min(P_{\max}^s + P_{\max}^j, P_{\max})$.*

Proof Denoting

$$f(P_s, P_j) = q_j \left[\frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}} \right]^+ + (1 - q_j) \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}}, \quad (5.39)$$

and the monotonicity of $f(P_s, P_j)$ will be discussed by means of partial derivative as follows.

1. $g_{sd} > g_{sk}$ and $P_j g_{sd} > \frac{g_{sk}}{h_{jk}}$:

Then we can rewrite $f(P_s, P_j)$ and the corresponding partial derivative as,

$$\begin{aligned} f(P_s, P_j) &= q_j \frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}} + (1 - q_j) \frac{P_s (g_{sd} - g_{sk})}{1 + P_s g_{sk}}, \\ \frac{\partial f(P_s, P_j)}{\partial P_s} &= q_j \frac{\left(P_j g_{sd} - \frac{g_{sk}}{h_{jk}} \right) P_j}{\left(P_j + \frac{g_{sk}}{h_{jk}} P_s \right)^2} (1 - q_j) \frac{g_{sd} - g_{sk}}{(1 + P_s g_{sk})^2} > 0, \\ \frac{\partial f(P_s, P_j)}{\partial P_j} &= q_j \frac{\left(g_{sd} + \frac{1}{P_s} \right) \frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}} \right)^2} > 0. \end{aligned}$$

2. $g_{sd} > g_{sk}$ and $P_j g_{sd} \leq \frac{g_{sk}}{h_{jk}}$:

In this case, $f(P_s, P_j)$ and its partial derivative can be expressed as,

$$f(P_s, P_j) = (1 - q_j) \frac{P_s (g_{sd} - g_{sk})}{1 + P_s g_{sk}},$$

$$\frac{\partial f(P_s, P_j)}{\partial P_s} = (1 - q_j) \frac{g_{sd} - g_{sk}}{(1 + P_s g_{sk})^2} > 0,$$

$$\frac{\partial f(P_s, P_j)}{\partial P_j} = 0.$$

3. $g_{sd} \leq g_{sk}$ and $P_j g_{sd} > \frac{g_{sk}}{h_{jk}}$:

Then we have,

$$f(P_s, P_j) = q_j \frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}},$$

$$\frac{\partial f(P_s, P_j)}{\partial P_s} = q_j \frac{\left(P_j g_{sd} - \frac{g_{sk}}{h_{jk}}\right) P_j}{\left(P_j + \frac{g_{sk}}{h_{jk}} P_s\right)^2} > 0,$$

$$\frac{\partial f(P_s, P_j)}{\partial P_j} = q_j \frac{\left(g_{sd} + \frac{1}{P_s}\right) \frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}\right)^2} > 0.$$

4. $g_{sd} \leq g_{sk}$ and $P_j g_{sd} \leq \frac{g_{sk}}{h_{jk}}$:

Then $f(P_s, P_j) = 0$.

To sum up, the partial derivative of $f(P_s, P_j)$ in Eq. (5.39) can be expressed as,

$$\frac{\partial f(P_s, P_j)}{\partial P_s} = q_j \frac{\left[P_j g_{sd} - \frac{g_{sk}}{h_{jk}}\right]^+ P_j}{\left(P_j + \frac{g_{sk}}{h_{jk}} P_s\right)^2} + (1 - q_j) \frac{[g_{sd} - g_{sk}]^+}{(1 + P_s g_{sk})^2} \geq 0,$$

$$\frac{\partial f(P_s, P_j)}{\partial P_j} = q_j \frac{\left(g_{sd} + \frac{1}{P_s}\right) \frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}\right)^2} \cdot u\left(P_j g_{sd} - \frac{g_{sk}}{h_{jk}}\right) \geq 0,$$

where $u(\cdot)$ is the unit step function.

Therefore, the problem described in Eq. (5.25) is a nondecreasing function with the increasing of P_s and P_j , respectively. Similarly, without joint power constraint in Eq. (5.3), we have a trivial solution $P_s = P_{\max}^s$ and $P_j = P_{\max}^j$. With the joint power constraint $P_s + P_j \leq P_{\max}$, the optimal solution must satisfy $P_s + P_j = \min(P_{\max}^s + P_{\max}^j, P_{\max})$.

Furthermore, it can be inferred from Proposition 5.2 that:

- (i) For the case when $P_{\max}^s + P_{\max}^j \leq P_{\max}$, the optimal solution is $P_s = P_{\max}^s$ and $P_j = P_{\max}^j$.

- (ii) For the case when $P_{\max}^s + P_{\max}^j > P_{\max}$, the optimization problem can be rewritten as

$$\max_{P_s} \min_k \left\{ q_j \left[\frac{(P_{\max} - P_s)g_{sd} - \frac{g_{sk}}{h_{jk}}}{P_{\max}/P_s - 1 + g_{sk}/h_{jk}} \right]^+ + (1 - q_j) \frac{P_s[g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}} \right\}. \quad (5.40)$$

In other words, there is no need to search for optimal power for the case of $P_{\max}^s + P_{\max}^j \leq P_{\max}$. As a result, power optimization will be executed only in the case of $P_{\max}^s + P_{\max}^j > P_{\max}$, where the optimization problem turns into a 1-dimension searching problem over P_s .

5.4.4 Simulation and Numerical Results

For convenience, in the simulation test, “Full” represents the case when full knowledge of CSI is assumed for all the links, and “Partial” means that full CSI of g_{sd} and h_{jd} and statistical knowledge of CSI of g_{sk} and h_{jk} are available. In this case, different methods have been adopted to optimise P_s and P_j to maximise the secrecy rate of D2D links, and only the optimization solved by upper bound leverages the 1-D search. Table 5.3 shows some related abbreviations in simulation results, and the main simulation parameters are generally in consistent with the general case in Table 5.2.

5.4.4.1 Impact of Number of Jammer Nodes

Figures 5.11 and 5.12 illustrate the effects of number of jammer nodes (N) on the achievable secrecy rate and corresponding computational time. Figure 5.11 shows that the achievable secrecy rate grows with increasing N when the other parameters are fixed, since more jammers result in a higher possibility that a better jammer can be found to combat eavesdropping, thereby lead to better performance.

Generally, the performance of full CSI case exceeds that of partial CSI case as we can imagine, yet the performance gap is negligible. In addition, the brute force algorithm outperforms the direct evaluation by GA with very limited performance

Table 5.3 Main abbreviations in simulation results

Abbreviations	Connotations
DE-GA	The optimization problem is solved by direct evaluation by utilizing GA
LB-GA	The optimization problem is solved by leveraging the lower bound by utilizing GA

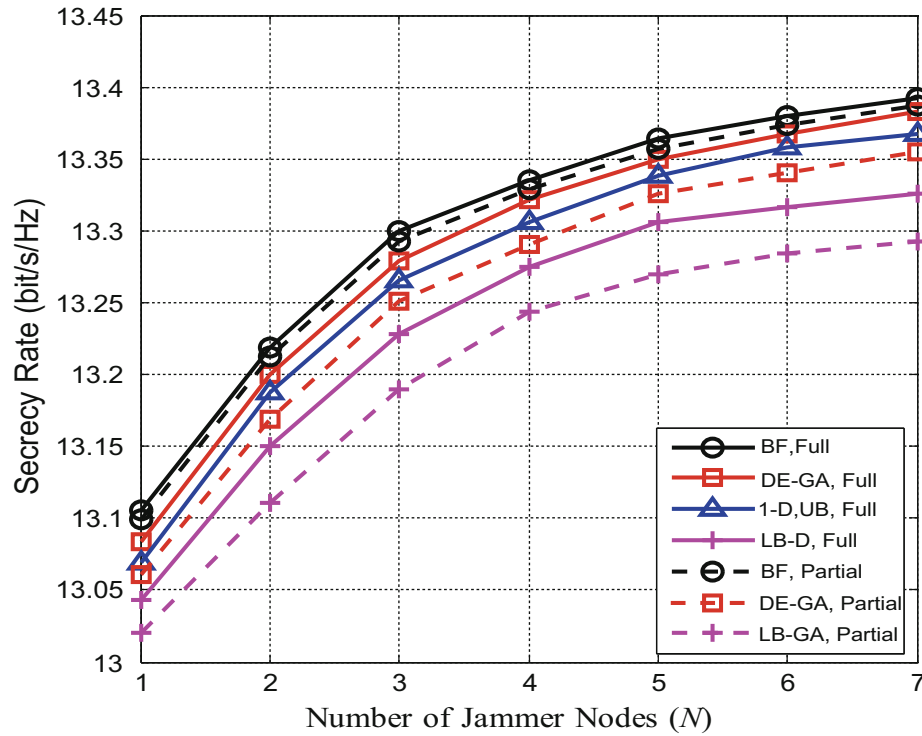


Fig. 5.11 Secrecy rate vs. the number of jammer nodes index, $q_j = 0.5$

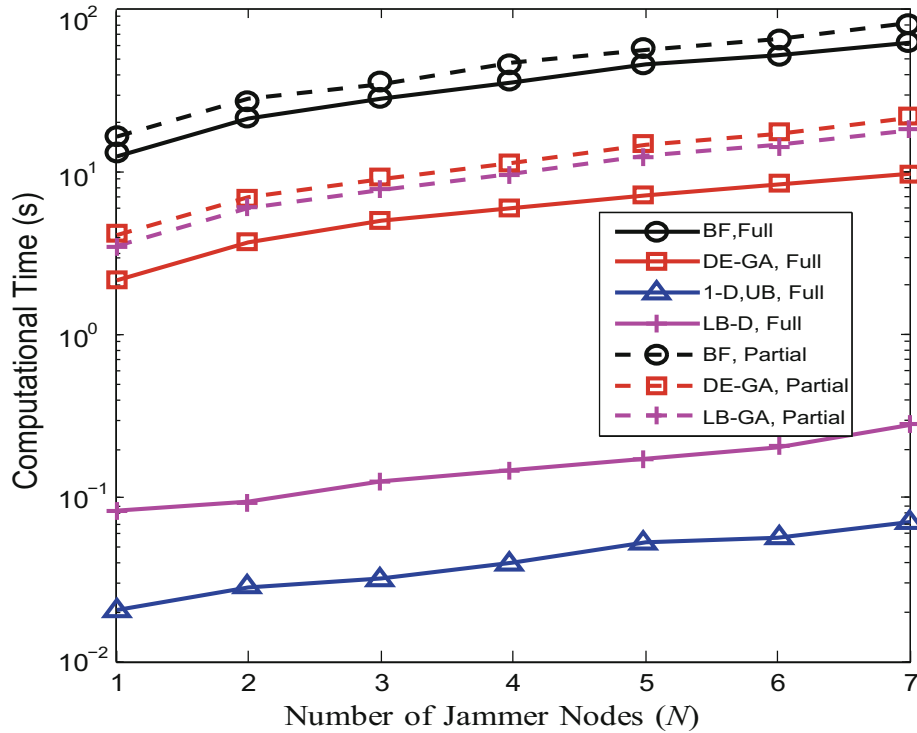


Fig. 5.12 Computational time vs. the number of jammer nodes index, $q_j = 0.5$

gap. Algorithms leveraging upper and lower bounds achieve less satisfying performance when compared to the brute force algorithm and GA, but the performance gap between different algorithms is insignificant.

Figure 5.12 demonstrates the computational time of different methods, which can reflect the complexities of different algorithms. Apparently, the computational time increases significantly with larger number of jammer nodes since power optimization should be executed for every candidate jammer node to select the best one. Methods with partial CSI is generally more time-consuming than that with full CSI, since the calculation of the expectation consumes more time than using accurate channel gains in the expression of achievable secrecy rate. Furthermore, computational time of the brute force algorithm is much higher than the other methods. Direct evaluation, which is taken by using GA, costs less time than brute force but is still more time-consuming compared to the other methods. In partial CSI case, the lower-bound method computes faster since it has less number of integration than direct evaluation. In the assumption of full CSI, the lower-bound method, which is solved by GFP, does have lower complexity. The upper-bound method is the most time-saving since it transforms the joint power optimization into a problem with only one variable.

5.4.4.2 Impact of Sum Transmit Power Limitation

In this part, 5 and 10 jammer nodes are randomly generated respectively, which are uniformly distributed within the network coverage area. The achievable secrecy rate is averaged over 10 random network realizations for each transmit power limitation $P_{\max}$. As shown in Fig. 5.13, the achievable secrecy rate increases with looser power constraint in partial CSI case. Larger $P_{\max}$ indicates that more power is available at D2D transmitter and jammer nodes, which leads to a higher probability that better power allocation can be found to achieve higher secrecy rate. From Fig. 5.11 and 5.13, it is clear that higher secrecy rate can be achieved with increased jammer density, i.e., more jammers in vicinity can lead to better performance.

Comparing the algorithms in both full CSI and partial CSI cases, Fig. 5.14 shows that higher secrecy rate can be achieved with larger $P_{\max}$, which is coincident with the results in Fig. 5.13. Naturally, full CSI case outperforms the partial CSI case. Moreover, the achievable secrecy rate of the brute force algorithm exceeds that of the other methods, among which GA is a close second best. The upper-bound method and lower-bound method exhibit mild performance gap when compared to the high complexity brute force algorithm as well as the GA.

5.4.4.3 Impact of Social Trust Index

The trust level of jammer nodes is crucial for the selection of the best jammer to hamper eavesdropping. In Fig. 5.15, the impact of social trust index of jammer nodes on the performance of secrecy rate is investigated by comparing different

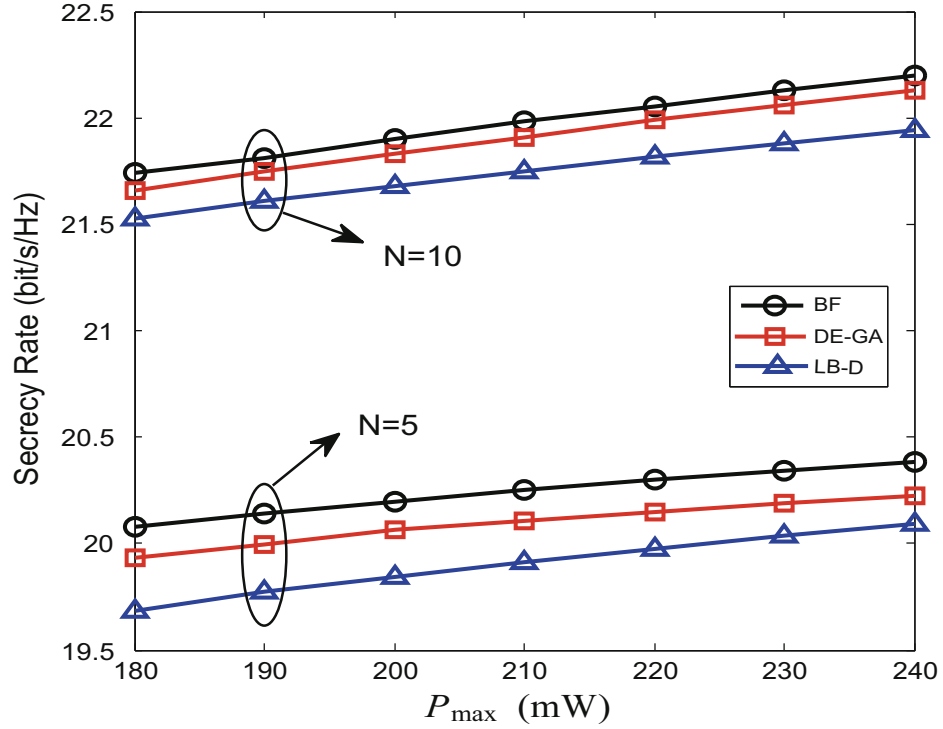


Fig. 5.13 Secrecy rate vs. sum transmit power limitation and number of jammer nodes in partial CSI case, $q_j = 0.5$

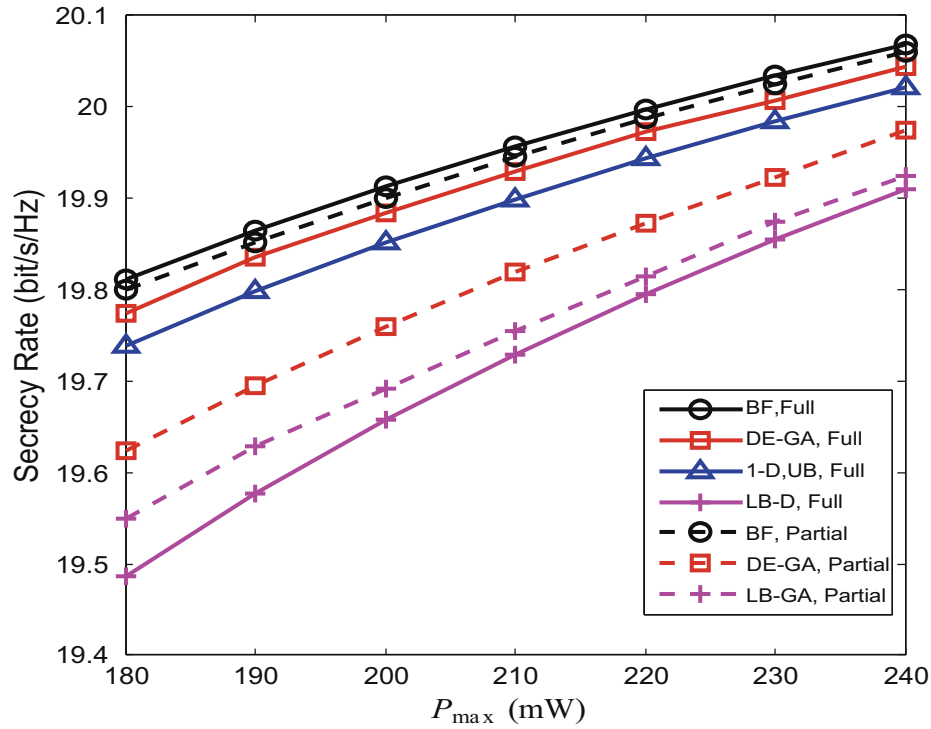


Fig. 5.14 Secrecy rate vs. sum transmit power limitation, $q_j = 0.5$

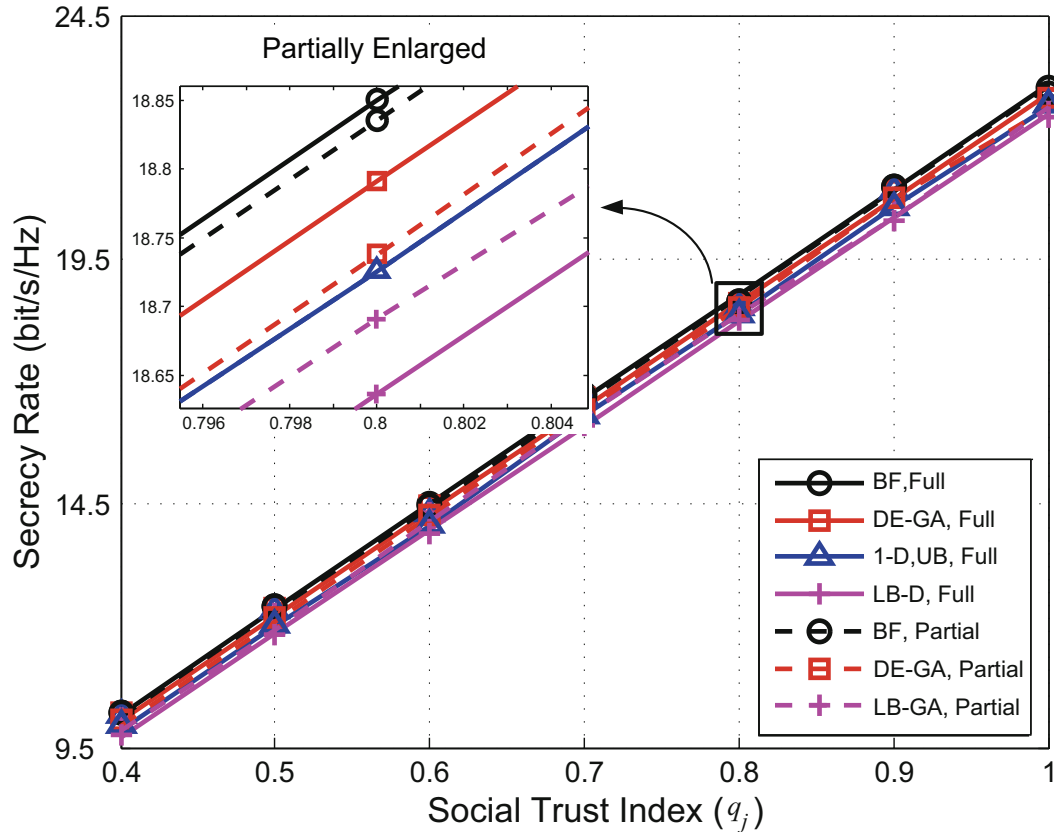


Fig. 5.15 Secrecy rate vs. social trust index of jammer nodes

optimization methods with different CSI assumptions. Recall that, social trust can be represented by link stability or deduced by trustiness of the cooperative jamming nodes, i.e., the probability to utilize the allocated transmit power to support secure transmission of the desired links. When social trust index is higher for the jammer nodes, it is more dependable to act as a jammer when requested. However, a jammer node with low social trust index has a high probability to refuse sending jamming transmission even though it is allocated a certain power. In this case, the allocated jamming power is wasted and the secrecy rate would deteriorate as a result. In other words, the social trust index of the jammer nodes indicates the success probability of acting as desired friendly jammer nodes. Higher social trust index naturally leads to better system performance.

5.5 Chapter Summary

In this chapter, secure transmission for content sharing has been investigated in cellular D2D overlays communication system. The schemes of joint power allocation with the source and jammer selection have been investigated to improve

secrecy and privacy of D2D communications. When there exist multiple source nodes, the social interaction has been exploited for selecting the optimal source node who holds the desired content to share with the destination node by considering both the physical links and social characteristics. Meanwhile, targeting the worst eavesdropping case by the potential smartest eavesdropper, reliable jammer has been selected based on its inherent social trust property. To maximize the achievable secrecy rate of the content sharing between content helper and content requester with the help of jammer partner against eavesdropping, a cooperative security optimization problem has been proposed. To solve the non-convex optimization problem, low complexity solutions have been developed in addition to the brute force search algorithm and heuristic algorithms. Specifically, upper bound and lower bound of the original objective function have also been considered to obtain the optimized solutions with low complexity. Meanwhile, in addition to the ideal case assuming that full CSI of all involved links can be acquired, more practical cases have also been discussed in terms of the partial CSI case and the statistical CSI case when only channel statistics information is available.

References

1. J. Pääkkönen, C. Hollanti, and O. Tirkkonen, "Device-to-device data storage for mobile cellular systems," in *Proc. 2013 IEEE Global Communications Conference Workshops (GLOBECOM Workshops)*, Atlanta, Georgia, USA, Dec. 2013, pp. 671–676.
2. L. Wang, C. Cao, and H. Wu, "Secure inter-cluster communications with cooperative jamming against social outcasts," *Computer Communications*, vol. 63, no. 1, pp. 1–10, Jun. 2015.
3. L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *IEEE Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, Feb. 2017.
4. X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. 14th ACM International Symposium on Mobile Ad Hoc NETWORKING and Computing*, Bangalore, India, Aug. 2013, pp. 187–196.
5. L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming aided secrecy enhancement in P2P communications with social interaction constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, Feb. 2017.
6. H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.
7. Z. Ding and Y. Li, *Blind Equalization and Identification*, New York: Marcel Dekker, 2001.
8. A. K. Sadek, Z. Han, and K. J. R. Liu, "Distributed relay-assignment protocols for coverage expansion in cooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 4, pp. 505–515, Apr. 2010.
9. L. Wang, H. Tang, and M. Čierný, "Device-to-device link admission policy based on social interaction information," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 9, pp. 4180–4186, Sept. 2015.
10. D. Bertsimas and J. Tsitsiklis, "Simulated Annealing," *Statistical Science*, vol. 8, no. 1, pp. 10–15, Feb. 1993.
11. V. Granville, M. Křivánek, and J.-P. Rasson, "Simulated annealing: A proof of convergence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 16, no. 6, pp. 652–656, Jun. 1994.

12. T. D. Hoang, L. B. Le, and T. L.-Ngoc, "Energy-efficient resource allocation for D2D communications in cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6972–6986, Sept. 2015.
13. H. Min, J. Lee, S. Park, and D. Hong, "Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 3995–4000, Dec. 2011.
14. S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
15. A. I. Barros, J. B. G. Frenk, S. Schaible, and S. Zhang, "A new algorithm for generalized fractional programs," *Mathematical Programming*, vol. 72, no. 2, pp. 147–175, Feb. 1996.
16. J. P. Crouzeix, J. A. Ferland, and S. Schaible, "An algorithm for generalized fractional programs," *Journal of Optimization Theory and Applications*, vol. 47, no. 1, pp. 35–49, Sept. 1985.
17. R. G. Ródenas, M. L. López, and D. Verastegui, "Extensions of Dinkelbach's algorithm for solving non-linear fractional programming problems," vol. 7, no. 1, pp. 33–70, Jun. 1999.
18. M.-S. Alouini and A. J. Goldsmith, "Capacity of rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 4, pp. 1165–1181, Jul. 1999.
19. M. Geller and E. W. Ng, "A table of integrals of the exponential integral," *Journal of reserach of the national bureau of standards - B. Mathematics and Mathematical Science*, vol. 73, no. 3, pp. 191–210, Jul.-Sept. 1969.
20. A. Erdélyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi, *Tables of Integral Transforms*, McGraw Hill, 1954.
21. P. Guo, X. Wang, and Y. Han, "The enhanced genetic algorithm for the optimization design," in *Proc. 3rd International Conference on Biomedical Engineering and Informatics*, Yantai, China, Oct. 2010, pp. 2990–2994.
22. L. Davis, Ed., *Handbook of Genetic Algorithm*, Van Nostrand Reinhold, 1991.