A Knapsack Problem Formulation for Relay Selection in Secure Cooperative Wireless Communication

S. Luo†, H. Godrich†‡, A. Petropulu†, and H. V. Poor†

†Rutgers University, Piscataway, NJ 08854
‡Princeton University, Princeton, NJ 08544

Abstract—Cooperative jamming (CJ) schemes support secure wireless communication in the presence of one or more eavesdroppers. Larger numbers of cooperative relays provide better secrecy rate, while increasing the communication and synchronization needs associated with cooperative beamforming. For low density networks (small number of relays) the secrecy rate changes rapidly with an increase in the number of relays, while for higher density networks increasing the number of relays has significantly smaller effect on the secrecy rate. This research considers a resource-aware approach: instead of using all available relays, choose the smallest set of active relays that meet a predetermined performance goal. The problem is formulated as a knapsack problem that may be solved through an exhaustive search. As this search method has exponential complexity, three heuristic algorithms are proposed, offering significant complexity reduction. The first one relies on the individual relay secrecy rate with a greedy algorithm. The second one is based on the beamforming weights norms, and the third one successively selects relay nodes that minimize the performance gap between the temporal secrecy rate and the given secrecy rate goal. Simulation results demonstrate that the relatively high secrecy rate may be achieved with a small number of active relays. The first method performs better for low secrecy rate threshold levels, while the second does so at high threshold. The third method combines the advantages of the previous two and offers performance very close to the optimum at the expense of higher complexity than the first two.

Index Terms—relay selection, cooperative jamming, secrecy rate

I. INTRODUCTION

Secure transmission of information over wireless channels is of considerable importance in both commercial and military applications. The role of multiple antennas for secure wireless communication within the framework of Wyner’s wiretap channel [1] has been extensively investigated [2]-[6]. In a cooperative system, the additional spatial degrees of freedom, available through the use of multiple relays support methods that degrade an eavesdropper’s channel condition by sending cooperative jamming (CJ) signals [3]-[4]. In this scheme, while the source is transmitting its message to the destination, the relay nodes transmit jamming signals to confound the eavesdropper. Thus far, this type of scheme was considered with one or two relays, while for higher density networks increasing the number of relays has significantly smaller effect on the secrecy rate. This research considers a resource-aware approach: instead of using all available relays, choose the smallest set of active relays that meet a predetermined performance goal. The problem is formulated as a knapsack problem that may be solved through an exhaustive search. As this search method has exponential complexity, three heuristic algorithms are proposed, offering significant complexity reduction. The first one relies on the individual relay secrecy rate with a greedy algorithm. The second one is based on the beamforming weights norms, and the third one successively selects relay nodes that minimize the performance gap between the temporal secrecy rate and the given secrecy rate goal. Simulation results demonstrate that the relatively high secrecy rate may be achieved with a small number of active relays. The first method performs better for low secrecy rate threshold levels, while the second does so at high threshold. The third method combines the advantages of the previous two and offers performance very close to the optimum at the expense of higher complexity than the first two.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a wireless network model depicted in Figure 1, consisting of one source node $S$, a set of $N$ relay nodes ($R_i$, $i = 1, \ldots, N$), a destination node $D$, and a single eavesdropper. The noise at each node is assumed to be zero-mean white complex Gaussian with variance $\sigma^2$. The source transmits a symbol $x$ with unit average energy, i.e., $E|x|^2 = 1$. The source transmission power is $P_s$. The relays transmit a common jamming signal $z$, with a weight vector $w$.

Motivated by this observation, and also considering the increased communication and synchronization requirements of larger numbers of cooperating relay nodes, this paper addresses the following questions: In a system with $N$ collaborating relay nodes, can secrecy rate requirements be achieved with fewer active relays? In such a case, which relays should be selected such that the total number of active relays is minimized? These questions may be formulated in a combinatorial optimization framework, as a knapsack problem (KP) [8], as the objective is to obtain a performance level with the lowest cost, in terms of active system elements. Relay selection has been considered previously for cooperative wireless communication. In some approaches, a single relay node is selected based on average channel state information (CSI) [10], while in others, a set of $K$ relays is selected [11]-[12]. In all cases, the goal is communication performance optimization with given infrastructure constraints. In this framework we seek to minimize the use of available relays, constrained by a performance threshold. The secrecy rate is determined by the required performance level, in which the design method proposed in [3] is used to optimize the beamforming weights and the power transmitted by the source and relays, such that the system secrecy rate is maximized, subject to a total transmit power constraint. In general, KPs are solved using exhaustive search [8] which, although simple to implement, has computational complexity that is exponential in the number of elements. In this paper, three heuristic algorithms are proposed for active relay node set selection. All offer reduced computational complexity compared with exhaustive search.

The paper is organized as follows: The system model is introduced in Section II, including the formulation of the secrecy rate and the knapsack problem representation. Three heuristic algorithms are proposed in Section III. Simulation results are provided in Section IV, including a discussion on the comparative performance of the proposed algorithms. In this section the robustness of the proposed algorithms to channel estimation errors is evaluated. Finally, Section V concludes the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a wireless network model depicted in Figure 1, consisting of one source node $S$, a set of $N$ relay nodes ($R_i$, $i = 1, \ldots, N$), a destination node $D$, and a single eavesdropper. The noise at each node is assumed to be zero-mean white complex Gaussian with variance $\sigma^2$. The source transmits a symbol $x$ with unit average energy, i.e., $E|x|^2 = 1$. The source transmission power is $P_s$. The relays transmit a common jamming signal $z$, with a weight vector $w$.

Motivated by this observation, and also considering the increased communication and synchronization requirements of larger numbers of cooperating relay nodes, this paper addresses the following questions: In a system with $N$ collaborating relay nodes, can secrecy rate requirements be achieved with fewer active relays? In such a case, which relays should be selected such that the total number of active relays is minimized? These questions may be formulated in a combinatorial optimization framework, as a knapsack problem (KP) [8], as the objective is to obtain a performance level with the lowest cost, in terms of active system elements. Relay selection has been considered previously for cooperative wireless communication. In some approaches, a single relay node is selected based on average channel state information (CSI) [10], while in others, a set of $K$ relays is selected [11]-[12]. In all cases, the goal is communication performance optimization with given infrastructure constraints. In this framework we seek to minimize the use of available relays, constrained by a performance threshold. The secrecy rate is determined by the required performance level, in which the design method proposed in [3] is used to optimize the beamforming weights and the power transmitted by the source and relays, such that the system secrecy rate is maximized, subject to a total transmit power constraint. In general, KPs are solved using exhaustive search [8] which, although simple to implement, has computational complexity that is exponential in the number of elements. In this paper, three heuristic algorithms are proposed for active relay node set selection. All offer reduced computational complexity compared with exhaustive search.

The paper is organized as follows: The system model is introduced in Section II, including the formulation of the secrecy rate and the knapsack problem representation. Three heuristic algorithms are proposed in Section III. Simulation results are provided in Section IV, including a discussion on the comparative performance of the proposed algorithms. In this section the robustness of the proposed algorithms to channel estimation errors is evaluated. Finally, Section V concludes the paper.
and

\[ y_e = \sqrt{P_s g_0 x} + g^\dagger w z + n_e, \]

where the baseband complex channel gain between the source and the destination is denoted by \( h_0 \), the baseband complex channel gain between the source and the eavesdropper is \( g_0 \), \( h = [h_1, ..., h_N] \) with \( h_i \) representing the baseband complex channel gain between the \( i \)-th relay and the destination, and \( g = [g_1, ..., g_N] \) with \( g_i \) denoting the baseband complex channel gain between the \( i \)-th relay and the eavesdropper. The channel gains, \( h \) and \( g \), are assumed to be known. The noise components at the destination and the eavesdropper are denoted by \( n_d \) and \( n_e \), respectively. The rate at the destination is [4]

\[ R_d = \log \left( 1 + \frac{P_s |h_0|^2}{w^\dagger R_h w + \sigma^2} \right), \tag{3a} \]

the rate at the eavesdropper is

\[ R_e = \log \left( 1 + \frac{P_s |g_0|^2}{w^\dagger R_g w + \sigma^2} \right), \tag{4a} \]

and the secrecy rate is

\[ R_s (w, P_s) = R_d - R_e, \tag{5a} \]

where \( R_h = h h^\dagger \), and \( R_g = g g^\dagger \). For the case of \( N \) active relays and a given total power (source plus relays) \( P_0 \), the optimal weight vector \( w^\dagger \) and the source transmit power, \( P_s^\star \), are obtained such that the secrecy rate is maximized, i.e.,

\[ \max_{w^\dagger, P_s} \ \ \ R_s (w, P_s) \ \ \ \ \text{s.t.} \ \ \ P_s + \|w\|^2 = P_0. \]

This type of problem may be formulated as a KP by introducing a vector of binary variables

\[ q_n = \begin{cases} 1 & \text{if relay } n \text{ is selected;} \\ 0 & \text{otherwise} \end{cases}, \ \ n = 1, ..., N. \tag{7} \]

The constraint on the capacity of the KP problem is the secrecy rate. We define \( R_s^\alpha (w, P_s, q) = \exp \left( R_s (w, P_s, q) \right) \), and express it as \( R_s^\alpha (w, P_s, q) = \sum_{i=1}^{N} \sum_{j=1}^{N} R_{s_{ij}}^\alpha (w, P_s, q) \)

\[ R_{s_{ij}}^\alpha (w, P_s, q) = q_i q_j \left( \frac{P}{w_i w_j R_{h_{ij}} + \sigma^2} \right) \tag{8} \]

where the elements \( f_h \) and \( f_g \) are defined as

\[ f_h = \sum_{i'=1}^{N} \sum_{j'=1}^{N} q_{i'} q_{j'} \left( w_i w_j R_{h_{i'j'}} + \sigma^2 \right) \tag{10} \]

and

\[ f_g = \sum_{i'=1}^{N} \sum_{j'=1}^{N} q_{i'} q_{j'} \left( w_i w_j R_{g_{i'j'}} + \sigma^2 \right) \tag{11} \]

The corresponding KP is defined as follows

\[ \begin{align*} 
& \text{minimize} \quad q \quad \sum_{i=1}^{N} q_i, \\
& \text{s.t.} \quad \sum_{i=1}^{N} \sum_{j=1}^{N} R_{s_{ij}}^\alpha (w_i^\dagger, P_s^\star, q), \quad R_{s_{ij}}^\alpha (w_i^\dagger, P_s^\star, q) \geq R_{s_{ij}}^\alpha (w_i^\dagger, P_s^\star, q) \quad \forall q_i \in \{0, 1\},
\end{align*} \tag{12} \]

where \( R_{s_{ij}}^\alpha (w_i^\dagger, P_s^\star, q) \) is a nonlinear minimization KP (NL=MinKP) [9], as the first constraints is a nonlinear function of \( q_i \), and the second constraints is a linear function of \( q_i \).

The optimal solution to the KP in (12), \( q^\star \), is commonly obtained through exhaustive examination of all possibilities for \( q_i \). This has a complexity of \( \sim O \left( 2^{N} \right) \) and the optimization of the secrecy rate is performed \( 2^N \) times. In what follows, three alternative heuristic algorithms are proposed for the solution of this problem, offering reduced computational complexity.

### III. RELAY SELECTION METHODS

#### A. Select relays based on single relay's secrecy rate

Assume only the i-th relay is active in jamming, while all others \((N - 1)\) relays are inactive. The secrecy rate for this scenario is denoted as the single secrecy rate \( R_{s_i} (w_i, P_s) \). For a single active relay,

\[ w_i w_i^\dagger = P_0 - P_s, \quad R_h = h h^\dagger = |h_i|^2, \tag{14a} \]

and

\[ R_g = g g^\dagger = |g_i|^2. \tag{14b} \]

The secrecy rate is calculated as

\[ R_{s_i} (w_i, P_s) = \log \left( \frac{P_s |h_0|^2 + (P_0 - P_s)|h_i|^2 + \sigma^2}{(P_0 - P_s)|h_i|^2 + \sigma^2} \right) \tag{14d} \]

The secrecy rate, \( R_{s_i} (w_i, P_s) \), is optimized for a single relay at a time, i.e., for a given i-th relay, an optimal solution \( R_{s_i} (w_i^\star, P_s^\star) \), \( i = 1, ..., N \), is obtained by evaluating

\[ \max_{w_i, P_s} R_{s_i} (w_i, P_s) \tag{15} \]

For the example in Figure 1, the two relays' locations are uniformly distributed between the destination D and the eavesdropper E. In Figure 2, the secrecy rate, \( R_s (w_i, P_s) \), is plotted for the given example. The curve for relay A lies entirely above that of relay B for every value of \( P_s \), i.e., \( R_s (w_A, P_s) > R_s (w_B, P_s) \). The optimal value of \( R_{s_i} (w_i, P_s) \) is selected as the maximum value of the individual curves, as demonstrated in the figure.

The optimal values \( R_{s_i} (w_i^\star, P_s^\star) \) are then used in the following knapsack problem:

\[ \begin{align*} 
& \text{minimize} \quad q \quad \sum_{i=1}^{N} q_i, \\
& \text{s.t.} \quad \sum_{i=1}^{N} q_i R_{s_i} (w_i^\dagger, P_s^\star) \geq \alpha R_{s_{max}}, \quad q_i \in \{0, 1\},
\end{align*} \tag{16} \]
where \( \alpha_A \) is selected such that the resulting \( R_{s,A}(w^*, P_s^*, q^*) \geq \alpha R_{s,max} \). This is equivalent to finding the secrecy rate for each relay separately and choosing the ones with the highest secrecy rate such that a minimal value of \( \alpha R_{s,max} \) is assured. This method is known as a greedy algorithm [8].

The final secrecy rate in this case is then further optimized,

\[
\text{maximize}_{w^*, P_s} \quad R_s(w, P_s^*, q^*) \\
\text{s.t.} \quad P_s + \|w\| = P_0, \quad w(q_i = 0) = 0, \quad q_i \in \{0, 1\},
\]

resulting in \( R_{s,k}(w^*, P_s^*, q^*) \). This algorithm offers reduced complexity of \( \sim O(L) \), where \( L \) is the final number of relays in the set, and the optimization of the secrecy rate is performed \( N + 1 \) times.

**B. Select relays based on weight’s norm**

In this approach, we first calculate the optimal values of \( w^* \) and \( P_s^* \) for the case of \( N \) active relays using the methods proposed in [4]. The secrecy rate maximization protocol under CJ protocol may be expressed as

\[
\max_{P_s, w} \quad \log \left( \frac{1}{(P_0 - P_s)} (h_1^T x_1 v_1^T x_1 + \sigma^2) \right) \\
\text{s.t.} \quad \|x\| = 1, \quad P_s \in [0, P_0],
\]

where \( w = \sqrt{P_0 - P_s} x \), \( v_1 = h/\|h\| \), and \( v_2 = g/\|g\| \). Let \( x \) be a feasible point. Denote \( x^T v_1 v_1^T x = \delta, \delta \in [0, 1] \), and \( G(\delta) = x^T v_2 v_2^T x \). We can now rewrite the optimization of (18) as

\[
\max_{P_s, w} \quad \log \left( \frac{1}{(P_0 - P_s)} (P_s(h_1^T x_1 v_1^T x_1 + \alpha_3) \right) \\
\text{s.t.} \quad \delta \in [0, 1], \quad P_s \in [0, P_0],
\]

where \( \alpha_1 = \|h_1\|^2/\|h_0\|^2 \), \( \alpha_2 = \sigma^2/\|h_0\|^2 \), \( \alpha_3 = ||g||^2/\|g_0\|^2 \) and \( \alpha_4 = \sigma^2/\|g_0\|^2 \).

The problem (19) can be solved by iterating between two steps: 1) fix \( \delta \), find the optimal \( P_s^* \); and 2) fix \( P_s \), find the optimal \( \delta \). Thus, we propose an algorithm to search for the optimal \( P_s^* \) and \( \delta \) as follows.

**Algorithm 1:** Take a feasible point \( \delta^{(1)} \) as initial point. Subsequently, find the optimal \( P_s^{(1)} \). At the \( i \)-th iteration step find an optimal \( \delta^{(i)} \) using \( P_s^{(i-1)} \), then find the optimal \( P_s^{(i)} \) while fixing \( \delta^{(i)} \). The procedure converges to an optimal \( P_s^* \) and \( \delta^* \).

The value of \( \delta \) is then obtained from the optimal value of \( \delta^* \) using the following lemma.

**Lemma 1:** [4] Let \( d_1 \) and \( d_2 \) be (known) unit-norm vectors. Let \( \phi \) be the argument of \( d_1^T d_1 \), \( r = |d_1^T d_2| \), and consider \( 0 \leq q \leq 1 \). The solution of

\[
\max_{z} \quad z^T d_2 d_2^T z \\
\text{s.t.} \quad z^T d_1 d_1^T z = q, \quad \|z\| = 1
\]

is given by \( z^* = c_1 d_1 + c_2 d_2 \), where \( c_2 = \sqrt{(1 - q)/(1 - r^2)} \) and \( c_1 = r c_2 - \sqrt{|q|} e^{i(\phi - \theta)} \). The corresponding maximum value is

\[
z^*^T d_2 d_2^T z^* = 1 - r \sqrt{1 - q - \sqrt{(1 - r^2) q}}.
\]

Notice that for a fixed \( \delta = x^T v_1 v_1 x \), a larger \( G(\delta) = x^T v_2 v_2 x \) produces a larger objective value. The problem (19) can be written as

\[
\max_{x} \quad x^T v_2 v_2 x \\
\text{s.t.} \quad x^T v_1 v_1 x = \delta^*, \quad \|x\| = 1,
\]

where \( v_1 \) and \( v_2 \) are unit-norm vectors. Let \( \phi \) be the argument of \( v_1^T v_1 \), \( r = |v_1^T v_2| \), and \( 0 \leq \delta^* \leq 1 \). According to Lemma 1, the solution of (20) is given by \( x^* = k_1 v_1 + k_2 v_2 \), where \( k_2 = \sqrt{(1 - \delta^*)/(1 - r^2)} \) and \( k_1 = r k_2 + \sqrt{|\delta^*|} e^{i(\phi - \theta)} \). Finally, optimal relay weights \( w^* \) can be obtained from \( x^* \) using \( w^* = \sqrt{P_0 - P_s^*} x^* \).

The optimal values of \( w^* \) and \( P_s^* \) are applied to the following knapsack problem:

\[
\min_{q} \quad \sum_{l=1}^{N} q_l, \\
\text{s.t.} \quad R_s^e(w^*, P_s^*, q^*) \geq R_s^e_{req}, \quad q_l \in \{0, 1\},
\]

where \( R_s^e_{req} = \exp(\alpha_B R_{s,max}) \) and \( \alpha_B \) is selected such that the resulting \( R_s^e(w^*, P_s^*, q^*) \geq \alpha R_{s,max} \). This is equivalent to sorting the relays by the norm of the weight vectors, and then selecting the relays with the largest weight norms. As before, the final secrecy rate is obtained by using the optimal vector \( q^* \) in the optimization problem given in (17) resulting in \( R_{s,e}(w^*, P_s^*, q^*) \). This algorithm offers a complexity of \( \sim O(NL) \) and the optimization of the secrecy rate is performed twice.

**C. Successive relay selection**

This heuristic algorithm solves the original KP problem in (12). The system selects the relay with the highest \( R_{s,k}(w_l, P_s) \), defined in (15), as the initial node. At the \( \ell \)-th iteration step, a set of \( \ell - 1 \) selected active relays is represented by the optimal vectors \( \{w^{\ell-1}, P_s^{\ell-1}, q^{\ell-1}\} \). For each of the remaining \( M = (N - \ell + 1) \) inactive relays, the algorithm optimizes

\[
\max_{w_m, P_s, q_m} \quad R_s^e(w_m^*, P_s^*, q_m^*) \\
\text{s.t.} \quad w_m^* + \|w_m\|^2 = P_0, \quad w_m (q^*_{f} = 0) = 0, \quad q_m \in \{0, 1, \}
\]

resulting in \( M \) sets \( \{w_m^*, P_s^*, q_m^*, \ell_m\} \), where \( \ell_m \) is generated by using vector \( q_m^* \) and changing the value of the appropriate inactive \( m \)-th relay’s location from 0 to 1. The optimal vectors at the \( \ell \)-th iteration, \( w^{\ell-1}, P_s^{\ell-1}, q^{\ell-1} \), are selected such that

\[
\{w^{\ell-1}, P_s^{\ell-1}, q^{\ell-1}\} = \arg \min_{q_m^*} R_s^e(w_m^*, P_s^*, q_m^*) - R_s^e_{req}.
\]

If the optimal temporal secrecy rate, \( R_s^e(w^{\ell-1}, P_s^{\ell-1}, q^{\ell-1}) \), does not achieve the performance goal of \( R_s^e_{req} \), an additional iteration is performed. This algorithm offers a complexity of \( \sim O(\ell NL) \) and the optimization of the secrecy rate is performed \( \ell LN \) times.
Fig. 3. Normalized secrecy rate versus the optimal number of active relays: algorithms A, B, and C and an exhaustive search.

IV. SIMULATION AND ANALYSIS

The following model is used in the simulation: the source S is located at the origin, (0, 0), the destination D at (0, 50), the eavesdropper E at (51, 0). Fifteen relays are randomly located in the area between S, D, and E. In Figure 3, the secrecy rate, normalized to the maximum secrecy rate with all relays active, $R_{\text{max}}$, is plotted as a function of the number of active relays. The normalized secrecy rate is plotted for an exhaustive search and the three proposed algorithms with known channel values (solid lines) and with estimation errors for the channel gains between the relays and the eavesdropper (dashed lines). The value of $R_e$ is obtained using 1000 Monte-Carlo simulations. It is observed that if the threshold factor is set to $\alpha = 0.95$, i.e., $R_{\text{req}} = 95\% R_{\text{max}}$, the exhaustive search, algorithm B, and algorithm C will result in a group of 3 active relays, while algorithm A results in 13 relays. A threshold of $\alpha = 0.75$, will result with a group of 2 active relays for the exhaustive search, algorithm A, and algorithm C and a group of 3 relays for algorithm B. The single secrecy rate based method (algorithm A) seems to work better for lower threshold levels as the cooperative performance is not considered and therefore less information is integrated in the decision making. The weight-vector norm based method (algorithm B) works better at higher threshold level as it does not necessarily choose the best relays at first. Algorithm C works better than both, as it follows the first algorithm in choosing the relay with the best individual secrecy rate first and then adds new relays to the active group based on the joint optimal cooperative performance, instead of the individual ones. This brings the overall performance very close to the optimal exhaustive search. The robustness of the proposed algorithms to small channel estimation errors is illustrated by the dashed lines.

In Figure 4, the secrecy rate is plotted for various white noise levels at the destination, for the proposed algorithms and the exhaustive search. It is clear that the secrecy rate decreases as the noise level increases. The figure demonstrates the consistency of the proposed algorithms’ performance when compared with the optimal solution. Algorithm C performs very close to the optimum in the whole range.

V. CONCLUSIONS

Resource-aware operation has been introduced to CJ in wireless relay networks with a single eavesdropper. In our formalism, a minimal set of active relays is selected out of the available ones such that a secrecy rate performance goal is achieved. The selection problem has been defined as a KP and three heuristic algorithms have been proposed. The first offers low computational complexity ($\sim O(L)$), yet results in a larger set of relays when compared with an optimal set, obtained through an exhaustive search. The second one offers the same complexity as the first one and thus it is inferior at lower threshold values and superior at higher threshold points. The third method integrates the advantages of the previous ones; by successively adding relays to maximize the temporal secrecy rate, or minimize the gap with respect to the required performance, it provides performance very close to the optimum. It has a computational complexity of $\sim O(NL)$, which is still significantly lower than an exhaustive option. The proposed algorithms have been shown to be robust to channel estimation errors.

Acknowledgement: The authors would like to thank Dr. Jianguan Li for his contribution to the secrecy rate optimization algorithm.

REFERENCES