A KNAPSACK PROBLEM FORMULATION FOR RELAY SELECTION IN SECURE COOPERATIVE WIRELESS COMMUNICATION

Shuangyu Luo ⌖
Hana Godrich* ⌖
Athina Petropulu ⌖
H. Vincent Poor *

* **Princeton University**
⌖ **Rutgers University**

The research was supported by the National Science Foundation under Grant CNS-0905425 and CNS-0905398

ICASSP, May 2011

OUTLINE

- Introduction
- System Model
- Knapsack problem (KP) formulation for minimal subset selection.
- Fast approximation algorithms
- Simulation analysis
- Concluding remarks

Radio Listens In On Phone Calls

AN ELECTRICAL eavesdropper, the invention of a Washington, D. C., man, Samuel S. Hixon, permits the listening in on phone conversations without connecting to the line. The device, operating on the radio principle, is capable of picking up conversation from phone wires within a radius of twenty-five feet without tapping lines.

Samuel S. Hixon, Washington, D. C. inventor, points out the interesting features of his telephone eavesdropper. The unusual radio receiving apparatus permits picking up telephone conversation without making any line taps.

Modern Mechanix, July 1936

BACKGROUND

- In a cooperative system, the additional spatial degrees of freedom, available through the use of multiple relays, may be used to degrade an eavesdropper's channel condition by sending cooperative jamming (CJ) signals.
- This type of scheme was considered with all relays participating in the jamming, transmitting weighted versions of a common jamming signal with the purpose of creating interference [Dong, Han, Petropulu and Poor, 2009].
- In [Wang and Swindlehurst, 2009] the secrecy capacity is evaluated with respect to the cooperative network node density. It is shown that the incremental effect of the network size on the secrecy rate significantly reduces as the number of relays increase, i.e., for large numbers of relays, adding additional relays will result in little gain in terms of secrecy rate.

PROBLEM DEFINITION

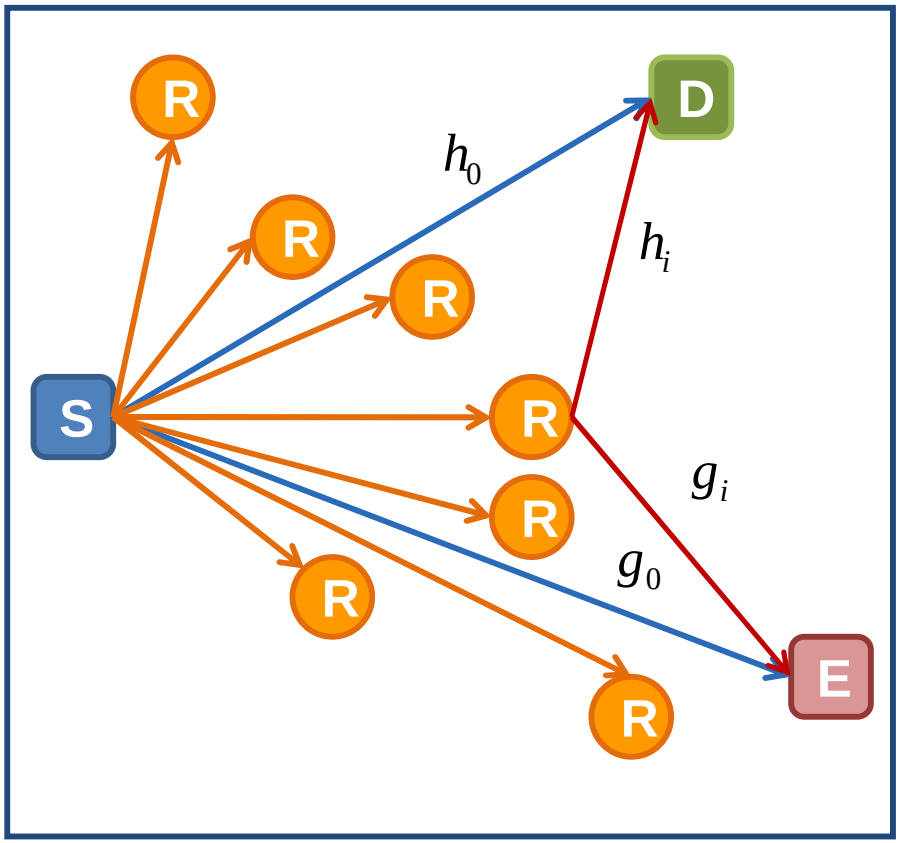
- Considering the increased communication and synchronization requirements of larger numbers of cooperating relay nodes, this paper addresses the following questions:

⇒ *In a system with N collaborating relay nodes, can secrecy rate requirements be achieved with fewer active relays?*

Objective: *Identify a minimal set of relays such that a predetermined secrecy rate objective is achieved.*

SYSTEM MODEL

- We consider a wireless network consisting of one source node S, a set of N relay nodes, a destination node D, and an eavesdropper E.
- The noise at each node is assumed to be zero-mean white complex Gaussian with variance σ^2. The source transmits a symbol x with unit energy, $|x|^2 = 1$.
- The source transmission power is P_s.
- The relays transmit a common jamming signal z, with a weight vector $\mathbf{w}$.



SIGNAL MODEL

- For the CJ-based protocol, the received symbols at the destination is:

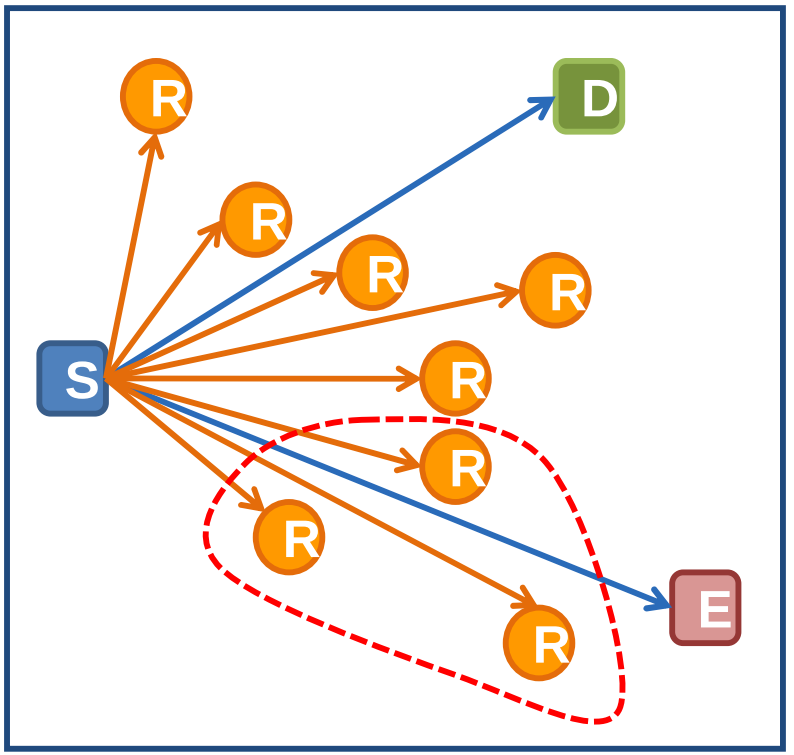
$$y_d = \sqrt{P_s} h_0 x + \mathbf{h}^T \mathbf{w} z + n_d$$

and at the eavesdropper:

$$y_e = \sqrt{P_s} g_0 x + \mathbf{g}^T \mathbf{w} z + n_e$$

where: $\mathbf{h} = [h_1, \ldots, h_N]^T; \mathbf{g} = [g_1, \ldots, g_N]^T;$

$\mathbf{w} = [w_1, \ldots, w_N]; \mathbf{R}_h = \mathbf{h}\mathbf{h}^T; \mathbf{R}_g = \mathbf{g}\mathbf{g}^T$



- The secrecy rate is:

$$R_s = R_d - R_e = \log\left[1 + \frac{P_s |h_0|^2}{\mathbf{w}^T \mathbf{R}_h \mathbf{w} + \sigma^2}\right] - \log\left[1 + \frac{P_s |g_0|^2}{\mathbf{w}^T \mathbf{R}_g \mathbf{w} + \sigma^2}\right]$$

SECRECY RATE

- For the case of N active relays and a given total power (source plus relays) is P_0, the optimal weight vector $\mathbf{w}^o$, and the source transmit power, P^o_s, are obtained such that the secrecy rate is maximized:

$$\underset{\mathbf{w}, P_s}{\text{maximize}} \quad \mathbf{R}_s(\mathbf{w}, P_s)$$

$$\text{s.t.} \quad P_s + \|\mathbf{w}\|^2 = P_o$$

- The objective is to find a minimal number of relays participating in the jamming such that a given secrecy rate goal is attained. The secrecy rate goal is defined as: $R_{s_{req}} = \alpha R_{s_{\max}}; \quad R_{s_{\max}} = R_s(\mathbf{w}^o, P_s^o, \mathbf{q}); \quad 0 < \alpha < 1$.

- This type of problem is next formulated as a KP.

KP FORMULATION

- A vector of binary variables is introduced:

$$q_i = \begin{cases} 1 & \text{if relay } i \text{ is selected} \\ 0 & \text{otherwise} \end{cases}; \quad i = 1,\ldots,N$$

- We define:

$$R_s^e(\mathbf{w}, P_s, \mathbf{q}) = \exp\left(R_s(\mathbf{w}, P_s, \mathbf{q})\right) = \sum_{i=1}^{N}\sum_{j=1}^{N} q_i q_j R_{s_{ij}}^e(\mathbf{w}, P_s, \mathbf{q})$$

$$R_{s_{ij}}^e = \left(w_i w_j^* R_{g_{ij}} + \sigma^2\right) f(\mathbf{q})$$

$$\text{where} \quad f(\mathbf{q}) = \frac{f_h(\mathbf{q}) + P_s |h_0|^2}{f_h(\mathbf{q})\left(f_g(\mathbf{q}) + P_s |g_0|^2\right)}$$

$$f_x(\mathbf{q}) = \sum_{i'=1}^{N}\sum_{j'=1}^{N} q_{i'} q_{j'} \left(w_{i'} w_{j'}^* R_{x_{i'j'}} + \sigma^2\right)$$

KP FORMULATION (2)

- The corresponding KP is defined as follows:

$$\underset{\mathbf{q}}{\text{minimize}} \quad \sum_{i=1}^{N} q_i$$

$$\text{s.t.} \quad \sum_{i=1}^{N}\sum_{j=1}^{N} q_i q_j R^{e}_{s_{ij}}\left(w^{*}_{q}, P^{*}_{s}, \mathbf{q}\right) \geq R^{e}_{s_{req}}$$

$$q_i \in \{0,1\} \qquad i = 1,\ldots, N$$

where $R^{e}_{s_{req}} = \exp\left(R_{s_{req}}\right)$. This is a nonlinear minimization KP (NLMinKP), as the first constraint is a nonlinear function of $\mathbf{q}$. The values of $\left(w^{*}_{q}, P^{*}_{s}\right)$ are obtained by solving:

$$\underset{\mathbf{w}, P_s}{\text{maximize}} \quad \mathbf{R}_s\left(\mathbf{w}, P_s\right)$$

$$\text{s.t.} \quad P_s + \|\mathbf{w}\|^2 = P_o$$

$$w_i\left(q_i = 0\right) = 0$$

FAST APPROXIMATION ALGORITHMS

- The optimal solution to the KP, $\mathbf{q}*$, is commonly obtained through exhaustive examination of all possibilities for $\mathbf{q}$. This has an exponential complexity and the optimization of the secrecy rate is performed 2^N times.
- Three alternative heuristic algorithms are proposed for the solution of this problem, offering reduced computational complexity:
  - Individual secrecy rate relay selection (INDrs)
  - Weights norm relay selection (WGHTs)
  - Successive relay selection, based on multiple start local search (MLSrs)

INDIVIDUAL SECRECY RATE (INDRS)

- Assume only the i-th relay is active in jamming, while all others $(N-1)$ relays are inactive. The secrecy rate is optimized for a single relay at a time, i. e.,

$$\underset{w_i, P_{s_i}}{\text{maximize}} \quad R_{s_{IND}}\left(w_i, P_{s_i}\right)$$

$$w_i w_i^* = P_0 - P_{s_i}$$

$$\mathbf{R}_h = |h_i|^2, \ \mathbf{R}_g = |g_i|^2$$

- The optimal values $R_{s_{IND}}\left(w_i^A, P_{s_i}^A\right)$ are then used in the following knapsack problem:

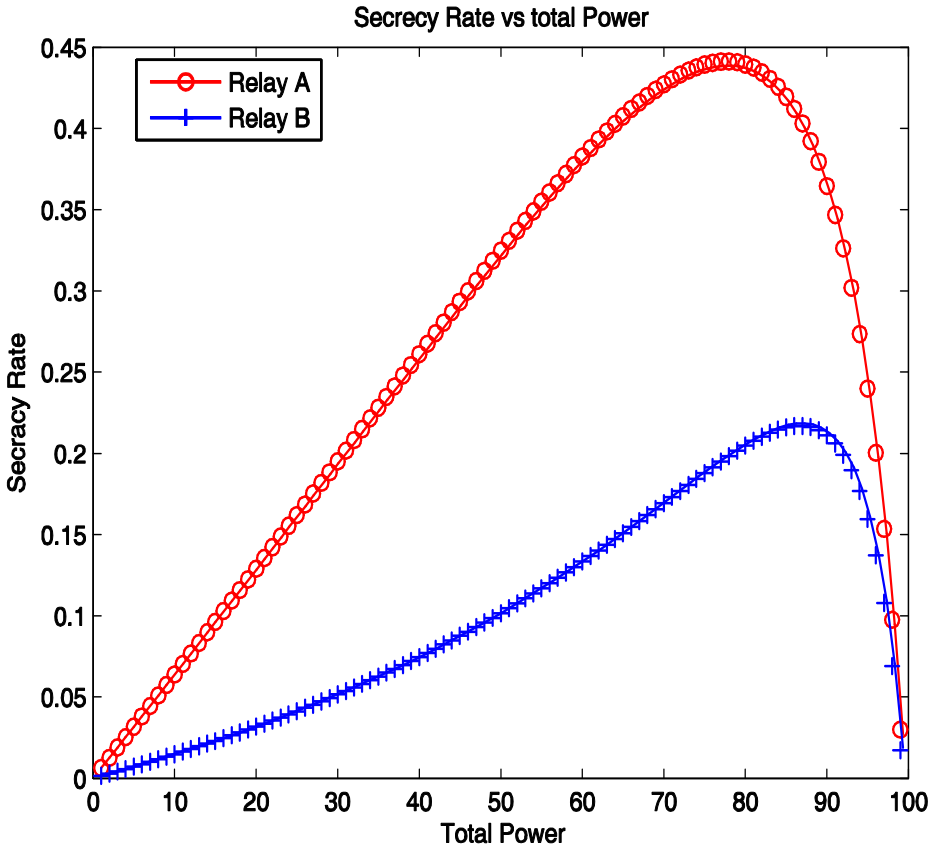
$$\underset{\mathbf{q}}{\text{minimize}} \quad \sum_{i=1}^{N} q_i$$

$$s.t. \quad \sum_{i=1}^{N} q_i R_{s_{IND}}\left(w_i^A, P_{s_i}^A\right) \geq \alpha_A R_{s_{\max}}$$

$$q_i \in \{0,1\}$$

INDRS (2)

- Plotting the individual secrecy rate as a function of the transmitted power, it is shown that for any two relays, uniformly distributed between the destination D and the eavesdropper E, the curve for relay A lies entirely above that of relay B for every value of P_s. The optimal value of $R_{s_{IND}}\left(w_i^A, P_{s_i}^A\right)$ is selected as the maximum value of the individual curves.



WEIGHTED NORM (WGTHRS)

- In this case, we first calculate the optimal values of $\left(\mathbf{w}^o, P_s^o\right)$ for the case of N active relays using the methods proposed by [Li, Petropulu, and Weber, 2010].
- The optimal values of $\left(\mathbf{w}^o, P_s^o\right)$ are applied to the following knapsack problem

$$\underset{\mathbf{q}}{\text{minimize}} \quad \sum_{i=1}^{N} q_i$$

$$s.t. \quad \sum_{i=1}^{N}\sum_{j=1}^{N} q_i q_j R_{s_{ij}}^{e}\left(w_i^o, P_s^0\right) \geq \alpha_B R_{s_{\max}}^{e}$$

$$q_i \in \{0,1\}$$

- This is equivalent to sorting the relays by the norm of the weight vectors, and then selecting the relays with the largest weight norms.

MULTIPLE START LOCAL SEARCH (MLSRS)

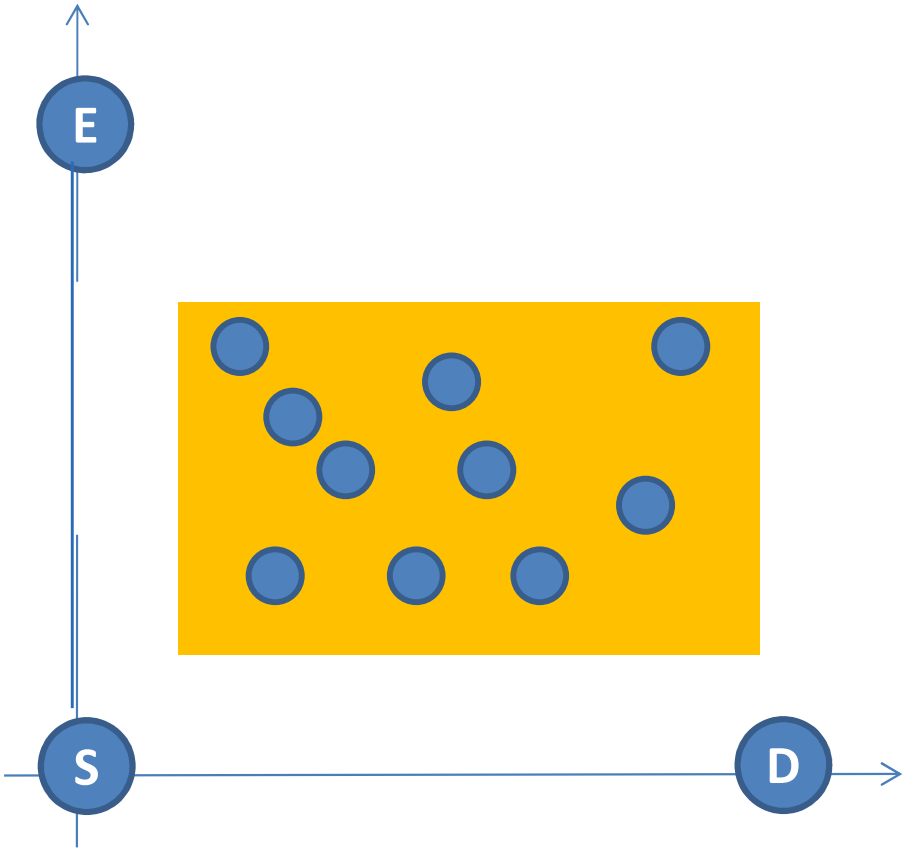
- This algorithm solves the original KP problem. The system selects an initial relay n. At each iteration step, the relay that minimizes the gap between the secrecy rate and the threshold is selected. At the l -th iteration step, a set of l – 1 selected active relays is represented by the optimal vectors $\left[\mathbf{w}_n^{\ell-1*}, P_{s_n}^{\ell-1*}, \mathbf{q}_n^{\ell-1*}\right]$. For each of the remaining inactive relays, the algorithm optimizes

$$\begin{aligned} \underset{\mathbf{w}_n^{\ell}, P_{s_n}^{\ell}}{\text{maximize}} \quad & R_{s_{ij}}^{e}\left(\mathbf{w}_n^{\ell}, P_{s_n}^{\ell}, q_n^{\ell}\right) \\ s.t. \quad & P_{s_n}^{\ell} + \left\|\mathbf{w}_n^{\ell}\right\|^2 = P_0 \\ & w_{n_i}^{\ell}\left(q_i = 0\right) = 0 \end{aligned}$$

- The search results in a set of N optimal solutions $\left[\mathbf{w}_n^{*}, P_{s_n}^{*}, \mathbf{q}_n^{*}\right]$. The ones with the minimal $\mathbf{q}_n^{*}$ are selected and out of these solutions, the one with the maximal secrecy rate is chosen.

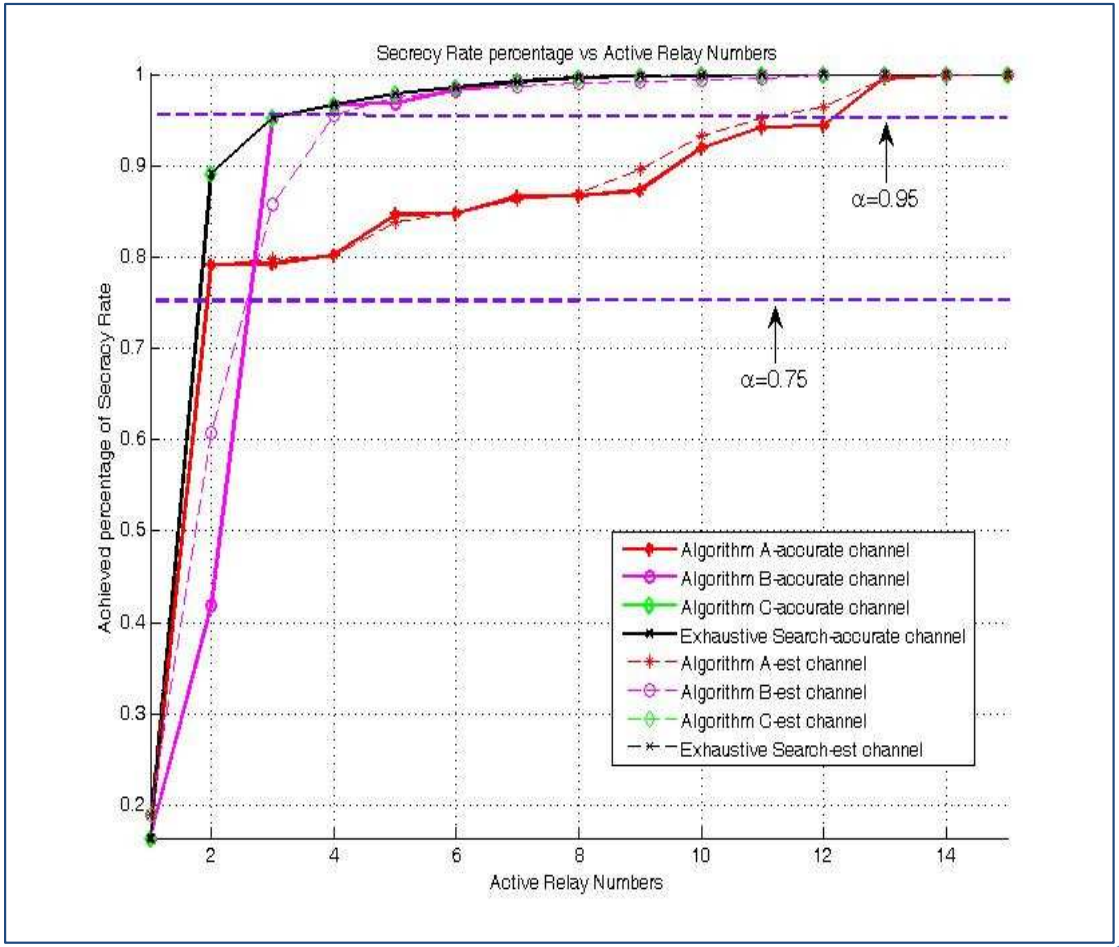
SIMULATION ANALYSIS
CONFIGURATIONS

- Fifteen relays are randomly located in the area between S, D, and E.
- The secrecy rate is normalized to the maximum secrecy rate with all relays active.
- The threshold factor is set to 95% and 75%.



SIMULATION ANALYSIS

- For a threshold factor of 0.95 the exhaustive search, algorithm B, and algorithm C result in a group of 3 active relays, while algorithm A results in 13 relays.
- For a threshold of 0.75 a group of 2 active relays for the exhaustive search, algorithm A, and algorithm C and a group of 3 relays for algorithm B.



CONCLUDING REMARKS

- The problem of selecting a minimal set of relays, achieving a given secrecy rate threshold, has been formulated as a KP and three heuristic algorithms have been proposed.
  - The first offers a computational complexity of $\square O(L)$. It results in a larger set of relays compared with an optimal set, obtained through an exhaustive search.
  - The second has the same complexity, performing better at higher threshold points.
  - The third method integrates the advantages of the previous ones; by successively adding relays to maximize the temporal secrecy rate it provides performance very close to the optimum. It has a computational complexity of $\square O(NL)$ which is still significantly lower that an exhaustive option.

Q & A

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