SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Proactive Eavesdropping of Wireless Powered Suspicious Interference Networks

Ding XU[1*] & Hongbo ZHU[1]

[1] *Wireless Communication Key Lab of Jiangsu Province, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

Appendix A Proposed Optimal Decoding Order

The following proposition presents the optimal decoding order for solving P3 given p_M and p_J.

Proposition 1: With given p_M and p_J, an optimal decoding order is proposed as $\boldsymbol{\pi}^*(p_M, p_J) = \{\pi_1^*(p_M, p_J), \ldots, \pi_K^*(p_M, p_J)\}$, with $\pi_k^*(p_M, p_J), k = 1, \ldots, K$ sequentially obtained as $\pi_k^*(p_M, p_J) = \arg\max_{k' \in \mathbb{K}_k(p_M, p_J)} \xi_{k'} (I_{k'})^2, k = 1, \ldots, K$ if the set $\mathbb{K}_k(p_M, p_J)$ is not empty, where $\mathbb{K}_k(p_M, p_J), k = 1, \ldots, K$ is also sequentially obtained as given by

$$\mathbb{K}_k(p_M, p_J) = \left\{ k'' \middle| \frac{I_{k''}}{\tau_1(\sigma^2 + p_J g) + \sum_{k' \leqslant k-1} \xi_{\pi^*_{k'}} p_M \tau_0 \left(I_{\pi^*_{k'}} \right)^2 \chi_{\pi^*_{k'}} + \sum_{k' \neq k'', k' \in \mathbb{K} \setminus \boldsymbol{\pi}^*_{k-1}(p_M, p_J)} \xi_{k'} p_M \tau_0 \left(I_{k'} \right)^2} \geqslant \frac{h_{k'', k''}}{\tau_1(\sigma^2 + p_J J_{k''}) + \sum_{k' \neq k''} \xi_{k'} p_M I_{k'} \tau_0 h_{k', k''}}, k'' \in \mathbb{K} \setminus \boldsymbol{\pi}^*_{k-1}(p_M, p_J) \right\}, \tag{A1}$$

for $k = 1, \ldots, K$, and $\boldsymbol{\pi}_k^*(p_M, p_J) = \{\pi_1^*(p_M, p_J), \ldots, \pi_k^*(p_M, p_J)\}$. Otherwise, if the set $\mathbb{K}_k(p_M, p_J)$ is empty, $\pi_k^*(p_M, p_J)$ is randomly chosen from the set $\mathbb{K} \setminus \boldsymbol{\pi}^*_{k-1}(p_M, p_J)$.

Proof: This proposition is proved by mathematical induction. Given p_M and p_J, let $\mathbb{S}$ denote the set of suspicious communication links which cannot be eavesdropped whatever the decoding order is and $\mathbb{S}' = \mathbb{K} \setminus \mathbb{S}$ denote the set of suspicious communication links which can be eavesdropped with some decoding order. Therefore, it is obvious that if we can find a decoding order that can let the monitor eavesdrop all the suspicious communication links in set $\mathbb{S}'$, this decoding order is optimal. Note that if such a decoding order does not exist, the optimal decoding order can only let the monitor eavesdrop the suspicious communication links in a subset of $\mathbb{S}'$. In what follows, we propose an optimal decoding order that can let the monitor eavesdrop all the suspicious communication links in set $\mathbb{S}'$. Define the set $\mathbb{K}_1(p_M, p_J)$ as the set of the suspicious communication links that can be decoded successfully at the first decoding order, given as

$$\mathbb{K}_1(p_M, p_J) = \left\{ k'' \middle| \frac{I_{k''}}{\tau_1(\sigma^2 + p_J g) + \sum_{k' \neq k'', k' \in \mathbb{K}} \xi_{k'} p_M \tau_0 \left(I_{k'} \right)^2} \geqslant \frac{h_{k'', k''}}{\tau_1(\sigma^2 + p_J J_{k''}) + \sum_{k' \neq k''} \xi_{k'} p_M I_{k'} \tau_0 h_{k', k''}}, k'' \in \mathbb{K} \right\}. \tag{A2}$$

Note that all the suspicious communication links in the set $\mathbb{K}_1(p_M, p_J)$ can be decoded successfully no matter what the decoding order $\boldsymbol{\pi}$ is. Note also that which suspicious communication link in the set $\mathbb{K}_1(p_M, p_J)$ is decoded first does not impact decoding the remaining suspicious communication links not in the set $\mathbb{K}_1(p_M, p_J)$, since all the suspicious communication links in the set $\mathbb{K}_1(p_M, p_J)$ can be decoded. Therefore, decoding any suspicious communication link in the set $\mathbb{K}_1(p_M, p_J)$ first is optimal. If the set $\mathbb{K}_1(p_M, p_J)$ is empty, it means no suspicious communication link can be decoded successfully, and $\pi_1^*(p_M, p_J)$ can be randomly selected from the set $\mathbb{K}$. Otherwise, in order to cancel as much interference as possible for decoding the remaining suspicious signals, the $\pi_1^*(p_M, p_J)$ is selected as $\pi_1^*(p_M, p_J) = \arg\max_{k' \in \mathbb{K}_1(p_M, p_J)} \xi_{k'} (I_{k'})^2$.

Then, suppose that $\boldsymbol{\pi}^*_{k-1}(p_M, p_J) = \{\pi_1^*(p_M, p_J), \ldots, \pi_{k-1}^*(p_M, p_J)\}$ has been optimally selected. Define the set $\mathbb{K}_k(p_M, p_J)$ as the set of the suspicious communication links that can be decoded successfully at the k-th decoding order, given as

$$\mathbb{K}_k(p_M, p_J) = \left\{ k'' \middle| \frac{I_{k''}}{\tau_1(\sigma^2 + p_J g) + \sum_{k' \leqslant k-1} \xi_{\pi^*_{k'}} p_M \tau_0 \left(I_{\pi^*_{k'}} \right)^2 \chi_{\pi^*_{k'}} + \sum_{k' \neq k'', k' \in \mathbb{K} \setminus \boldsymbol{\pi}^*_{k-1}(p_M, p_J)} \xi_{k'} p_M \tau_0 \left(I_{k'} \right)^2} \geqslant \frac{h_{k'', k''}}{\tau_1(\sigma^2 + p_J J_{k''}) + \sum_{k' \neq k''} \xi_{k'} p_M I_{k'} \tau_0 h_{k', k''}}, k'' \in \mathbb{K} \setminus \boldsymbol{\pi}^*_{k-1}(p_M, p_J) \right\}. \tag{A3}$$

Note that all the suspicious communication links in the set $\mathbb{K}_k(p_M, p_J)$ can be decoded successfully no matter what the decoding order $\{\pi_k^*(p_M, p_J), \ldots, \pi_K^*(p_M, p_J)\}$ is. Note also that which suspicious communication link in the set $\mathbb{K}_k(p_M, p_J)$ is decoded at

* Corresponding author (email: xuding@ieee.org)

the k-th decoding order does not impact decoding the remaining suspicious communication links not in the set $\boldsymbol{\pi}_{k-1}^*(p_M, p_J) \cup \mathbb{K}_k(p_M, p_J)$, since all the suspicious communication links in the set $\mathbb{K}_k(p_M, p_J)$ can be decoded. Thus, decoding any suspicious communication link in the set $\mathbb{K}_k(p_M, p_J)$ at the k-th decoding order is optimal. If the set $\mathbb{K}_k(p_M, p_J)$ is empty, it means no more suspicious communication link can be decoded successfully, and thus $\pi_k^*(p_M, p_J)$ can be randomly selected from the set $\mathbb{K}\backslash\{\pi_1^*(p_M, p_J), \ldots, \pi_{k-1}^*(p_M, p_J)\}$. Otherwise if the set $\mathbb{K}_k(p_M, p_J)$ is not empty, $\pi_k^*(p_M, p_J)$ is selected as $\pi_k^*(p_M, p_J) = \arg\max_{k' \in \mathbb{K}_k(p_M, p_J)} \xi_{k'} (I_{k'})^2$ for canceling as much interference as possible for decoding the remaining suspicious signals.

Therefore, based on the above procedures, the obtained decoding order can let the monitor eavesdrop all possible suspicious communication links and is thus optimal. This completes the proof. ■

Appendix B Proposed Optimal Algorithm

```
Initialize q_min = 0, q_max = 1.
repeat
    q = (q_min + q_max) / 2.
    for p_M = 0 to P_max do
        for p_J = 0 to ξ_J p_M g τ_0 / τ_1 do
            Obtain π*(p_M, p_J) from Proposition 1.
            Calculate the objective function value in (8).
        end for
    end for
    Choose the p_M and p_J that maximize the objective function value in (8).
    if the obtained maximum objective function value in (8) is no smaller than zero then
        q_min = q.
    else
        q_max = q.
    end if
until q converges to a desired accuracy.
```

Appendix C Proposed Low-complexity Suboptimal Algorithm

Proposition 2: If $\chi_{\pi_k}(p_M, 0, \boldsymbol{\pi}^*(p_M, p_J)) = 1$ is hold for a given k, then it must have $h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M) > 0$, and the following inequalities must be satisfied in order to let $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ for $p_J \geqslant 0$:

$$I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g > 0, \tag{C1}$$

$$p_J \geqslant \frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\tau_1 \left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right)}, \tag{C2}$$

where

$$A_k(p_M) = \tau_1 \sigma^2 + \sum_{k' \leqslant k-1} \xi_{\pi^*_{k'}} p_M \tau_0 \left(I_{\pi^*_{k'}}\right)^2 \chi_{\pi^*_{k'}} + \sum_{k' \geqslant k+1} \xi_{\pi^*_{k'}} p_M \tau_0 \left(I_{\pi^*_{k'}}\right)^2, \tag{C3}$$

$$B_k(p_M) = \tau_1 \sigma^2 + \sum_{k' \neq \pi_k} \xi_{k'} p_M I_{k'} \tau_0 h_{k',\pi_k}. \tag{C4}$$

Proof: Proposition 2 is proved by contradiction. From (2), the inequality $\chi_{\pi_k}(p_M, 0, \boldsymbol{\pi}^*(p_M, p_J)) = 1$ can be easily verified to be equivalent to $h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M) > 0$. In order to let $\chi_{\pi_{\hat{k}}}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$, the following inequality shall be satisfied

$$\frac{I_{\pi_k}}{\tau_1 p_J g + A_k(p_M)} \geqslant \frac{h_{\pi_k,\pi_k}}{\tau_1 p_J J_{\pi_k} + B_k(p_M)}, \tag{C5}$$

which can be rewritten as

$$\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right) \tau_1 p_J \geqslant h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M). \tag{C6}$$

Supposing $I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g = 0$, then the inequality in (C6) becomes $h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M) \leqslant 0$, which contradicts with the condition that $h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M) > 0$. Supposing $I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g < 0$, then the inequality in (C6) becomes $p_J \leqslant \frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right) \tau_1}$. In this case, since $h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M) > 0$, the expression $\frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right) \tau_1}$ is smaller than 0. Thus, it is impossible for $p_J \geqslant 0$ to satisfy the inequality $p_J \leqslant \frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right) \tau_1}$. Therefore, based on the above analysis, $I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g > 0$ must be established, and the inequality in (C6) is equivalent to the following two inequalities:

$$I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g > 0, \tag{C7}$$

$$p_J \geqslant \frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right) \tau_1}. \tag{C8}$$

This completes the proof. ■

Proposition 2 indicates that if suspicious communication link π_k fails to be eavesdropped, the jamming power p_J must be no smaller than $\frac{h_{\pi_k,\pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\tau_1 \left(I_{\pi_k} J_{\pi_k} - h_{\pi_k,\pi_k} g\right)}$ to turn eavesdropping to be successful. Based on Proposition 2, a suboptimal algorithm is proposed as follows:

Step 1: Initialize $p_M = P_{max}$, $p_J = 0$, and obtain $\boldsymbol{\pi}^*(p_M, p_J)$ by Proposition 1. If the equality $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ satisfies for all $k = 1, \ldots, K$, then the algorithm stops and the output is p_M, p_J and $\boldsymbol{\pi}^*(p_M, p_J)$, since it is obvious that the objective function in (8) achieves its maximum value in this case. Otherwise, denote p_M, p_J and the objective function value in (8) as p_M^*, p_J^*, Ω^*, respectively, and execute the following steps.

Step 2: In this step, a new jamming transmit power is tried to be found for eavesdropping more suspicious communication links and improving the objective function value. Assume that $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 1$ for $k = \hat{k}, \ldots, K$[1]. Thus, the inequalities in (C1) and (C2) shall be satisfied in order to let $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ for $k = \hat{k}, \ldots, K$. Let $p_J^{min}(p_M)$ denote the required minimum jamming power in order to successfully eavesdrop one more suspicious communication link:

$$p_J^{min}(p_M) = \min_{k \in \left\{k' | I_{\pi_{k'}} J_{\pi_{k'}} - h_{\pi_{k'}, \pi_{k'}} g > 0, k' = \hat{k}, \ldots, K\right\}} \frac{h_{\pi_k, \pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k, \pi_k} g\right) \tau_1}. \tag{C9}$$

Depending on the value of $p_J^{min}(p_M)$, there are three possible procedures: 1) If $p_J^{min}(p_M)$ is empty, it means that no more suspicious communication links can be successfully eavesdropped, and thus the algorithm stops and the output is p_M^*, p_J^* and $\boldsymbol{\pi}^*(p_M, p_J)$. 2) If $p_J^{min}(p_M) > \frac{\xi_J p_M g \tau_0}{\tau_1}$, it means that the required minimum jamming power is higher than the available power, and go to Step 3 for finding a new transmit power of the monitor for possible improvement of the objective function value. 3) If $p_J^{min}(p_M) \leqslant \frac{\xi_J p_M g \tau_0}{\tau_1}$, update p_J as $p_J = p_J^{min}(p_M)$, obtain $\boldsymbol{\pi}^*(p_M, p_J)$ by Proposition 1, and calculate the objective function value in (8) and denote it as Ω'. If $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ for all $k = 1, \ldots, K$ and $\Omega' > \Omega^*$, it means that all suspicious communication links are successfully eavesdropped and the objective function value with the new p_J is improved compared to p_J^*. Thus, in this case the algorithm stops and the output is p_M, p_J and $\boldsymbol{\pi}^*(p_M, p_J)$. If $\Omega' < \Omega^*$, it means that the objective function value with the new p_J is degraded compared to p_J^*. Thus, in this case the algorithm stops and the output is p_M^*, p_J^* and $\boldsymbol{\pi}^*(p_M, p_J)$. Otherwise if $\Omega' > \Omega^*$ but not all $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J))$'s are equal to 0, let $p_M^* = p_M$, $p_J^* = p_J$, $\Omega^* = \Omega'$ and execute Step 2 again for finding a possible new jamming transmit power.

Step 3: In this step, a new transmit power of the monitor is tried to be found for possible improvement of the objective function value. Let $\hat{p}_M$ be the value of p_M that satisfies the equality $\frac{\xi_J p_M g \tau_0}{\tau_1} = p_J^{min}(p_M)$, from which $\hat{p}_M$ is obtained as

$$\begin{aligned} \hat{p}_M = & \tau_1 \sigma^2 (h_{\pi_{\tilde{k}}, \pi_{\tilde{k}}} - I_{\pi_{\tilde{k}}}) \Bigg(\xi_J g \tau_0 \left(I_{\pi_{\tilde{k}}} J_{\pi_{\tilde{k}}} - h_{\pi_{\tilde{k}}, \pi_{\tilde{k}}} g \right) - h_{\pi_{\tilde{k}}, \pi_{\tilde{k}}} \sum_{k' \leqslant \tilde{k} - 1} \xi_{\pi^*_{k'}} \tau_0 \left(I_{\pi^*_{k'}} \right)^2 \chi_{\pi^*_{k'}} \\ & - h_{\pi_{\tilde{k}}, \pi_{\tilde{k}}} \sum_{k' \geqslant \tilde{k} + 1} \xi_{\pi^*_{k'}} \tau_0 \left(I_{\pi^*_{k'}} \right)^2 + I_{\pi_{\tilde{k}}} \sum_{k' \neq \pi_{\tilde{k}}} \xi_{k'} I_{k'} \tau_0 h_{k', \pi_{\tilde{k}}} \Bigg)^{-1}, \end{aligned} \tag{C10}$$

where

$$\tilde{k} = \arg \min_{k \in \{\hat{k}, \ldots, K\}} \frac{h_{\pi_k, \pi_k} A_k(p_M) - I_{\pi_k} B_k(p_M)}{\left(I_{\pi_k} J_{\pi_k} - h_{\pi_k, \pi_k} g\right) \tau_1}. \tag{C11}$$

If $\hat{p}_M < 0$ or $\hat{p}_M > P_{max}$, it means that a new transmit power of the monitor is unable to be found, and thus the algorithm stops and the output is p_M^*, p_J^* and $\boldsymbol{\pi}^*(p_M, p_J)$. Otherwise if $0 \leqslant \hat{p}_M \leqslant P_{max}$, update p_M as $p_M = \hat{p}_M$ and execute Step 2.

The complexity of this suboptimal algorithm is in the order of K, which is much lower than that of the optimal algorithm, which is $\frac{K}{\Delta \Delta'}$ (Δ and Δ' are the accuracies of p_M and p_J, respectively). The proposed low-complexity suboptimal algorithm is summarized as follows:

Initialize $q_{min} = 0, q_{max} = 1$.
repeat
    $q = \frac{q_{min} + q_{max}}{2}$.
    Initialize $p_M = P_{max}, p_J = 0$.
    Obtain $\boldsymbol{\pi}^*(p_M, p_J)$ from Proposition 1.
    Let $p_M^* = p_M, p_J^* = p_J$.
    if $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ holds for all $k = 1, \ldots, K$ **then**
        Calculate the objective function value in (8) with $p_M, p_J, \boldsymbol{\pi} = \boldsymbol{\pi}(p_M^*, p_J^*)$ and denote it as Ω^*.
        loop
            Suppose $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 1$ for $k = \hat{k}, \ldots, K$.
            Calculate $p_j^{min}(p_M)$ from (C9).
            if $p_j^{min}(p_M) \leqslant \frac{\xi_J p_M g \tau_0}{\tau_1}$ **then**
                Update p_j as $p_j = p_j^{min}(p_M)$ and obtain $\boldsymbol{\pi}^*(p_M, p_J)$ from Proposition 1.
                Calculate the objective function value in (8) with $p_M, p_J, \boldsymbol{\pi} = \boldsymbol{\pi}^*(p_M, p_J)$ and denote it as Ω'.
                if $\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}^*(p_M, p_J)) = 0$ holds for all $k = 1, \ldots, K$ and $\Omega' > \Omega^*$ **then**
                    Let $p_M^* = p_M, p_J^* = p_J$.
                    Break the loop.
                else if $\Omega' < \Omega^*$ **then**
                    Break the loop.
                else
                    Let $p_M^* = p_M$, $p_J^* = p_J$, $\Omega^* = \Omega'$.
                end if
            else
                Obtain $\hat{p}_M$ from (C10).
                if $0 \leqslant \hat{p}_M \leqslant P_{max}$ **then**

1) From the proof of Proposition 1, the indexes of the suspicious communication links failed to be eavesdropped is high-ranking in the obtained decoding order $\boldsymbol{\pi}$.

Update p_M as $p_M = \hat{p}_M$.
else
Break the loop.
end if
end if
end loop
end if
Obtain $\boldsymbol{\pi}^*(p_M^*, p_J^*)$ from Proposition 1.
Calculate the objective function value in (8) with $p_M = p_M^*, p_J = p_J^*, \boldsymbol{\pi} = \boldsymbol{\pi}^*(p_M^*, p_J^*)$.
if the obtained objective function value in (8) is no smaller than zero **then**
$q_{min} = q$.
else
$q_{max} = q$.
end if
until q converges to a desired accuracy.