SCIENCE CHINA
Information Sciences

• LETTER •

December 2021, Vol. 64 229305:1–229305:2
https://doi.org/10.1007/s11432-020-2992-3

Proactive eavesdropping of wireless powered suspicious interference networks

Ding XU* & Hongbo ZHU

Wireless Communication Key Lab of Jiangsu Province, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Received 22 March 2020/Revised 7 May 2020/Accepted 20 July 2020/Published online 9 November 2021

Citation Xu D, Zhu H B. Proactive eavesdropping of wireless powered suspicious interference networks. Sci China Inf Sci, 2021, 64(12): 229305, https://doi.org/10.1007/s11432-020-2992-3

Dear editor,

Radio frequency (RF) energy harvesting is a technology that enables harvesting energy from RF signals, and the wireless powered communication network (WPCN) is a new type of wireless network, where devices are powered by RF energy harvesting [1, 2]. Meanwhile, physical layer security (PLS) is a technique to ensure communication security from the aspect of the physical layer, and how to effectively surveil wireless information transmission is an important research topic in PLS [3, 4]. Different from traditional PLS where eavesdropping is treated as a threat to legitimate communication [5], wireless information surveillance treats suspicious communication of malicious users as a threat to public safety and eavesdrops the suspicious communication. The existing studies on wireless information surveillance with RF energy harvesting include [6–8] and they considered only very simple point-to-point suspicious networks with RF energy harvesting. For more complex suspicious networks with multiple suspicious links based on RF energy harvesting, the tradeoff of eavesdropping performances among different suspicious links must be considered. However, such research topics have not been well investigated yet in the existing literature.

In this study, wireless information surveillance of a wireless powered suspicious interference network is investigated. The aim is to maximize the relative eavesdropping rate by jointly optimizing the jamming transmit power at the jammer, the transmit power and the successive interference cancellation (SIC) decoding order at the monitor. An optimal decoding order is proposed, based on which the problem is solved optimally by a bisection search, where in each search the transmit powers are obtained optimally by an exhaustive search. In addition, a low-complexity suboptimal algorithm is also proposed. It shows that the proposed algorithms significantly outperform the benchmark algorithms.

System model and problem formulation. A wireless powered suspicious interference network with K suspicious communication links is considered. Each link consists of a wireless powered suspicious transmitter (S-TX) and a suspicious receiver (S-RX). A legitimate monitor disguised as a power station wirelessly transmits energy to the suspicious users. There also exists a wireless powered jammer that can send jamming signals. The channel power gains from S-TX k to S-RX k', between the monitor and S-TX k, from the jammer to S-RX k, and between the monitor and the jammer are denoted by $h_{k,k'}$, I_k, J_k and g, respectively. It is assumed that all the channel power gains follow slow block fading and are known to the monitor. Each transmission block is assumed to consist of two phases. The first phase is for the monitor to broadcast power signals with transmit power p_M and time duration τ_0. In this phase, the energy harvested by the jammer and S-TX k can be written as $\xi_J p_M g \tau_0$ and $\xi_k p_M I_k \tau_0$, respectively, where ξ_J and ξ_k denote the energy harvesting efficiencies at the jammer and S-TX k, respectively. The second phase with time duration τ_1 is for each S-TX to send information signals to its receiver and also for the jammer to send jamming signals. Let p_J and $p_{s,k}$ denote the transmit powers of the jammer and S-TX k, respectively. Each S-TX is assumed to consume its all harvested energy for information transmission, i.e., $p_{s,k} = \frac{\xi_k p_M I_k \tau_0}{\tau_1}, k = 1, \ldots, K$, while the transmit power of the jammer is assumed to satisfy the energy causality constraint, i.e., $p_J \leqslant \frac{\xi_J p_M g \tau_0}{\tau_1}$. The achievable rate of the suspicious communication link k is

$$r_k(p_M, p_J) = \tau_1 \log_2 \left(1 + \frac{\xi_k p_M I_k \tau_0 h_{k,k}}{\tau_1(\sigma^2 + p_J J_k) + \mathcal{I}_k}\right), \quad (1)$$

where σ^2 is the noise power and $\mathcal{I}_k = \sum_{k' \neq k} \xi_{k'} p_M I_{k'} \tau_0 h_{k',k}$ is the interference from other suspicious links to suspicious link k. As for the monitor, it is assumed to be equipped with a SIC decoder and thus it can cancel the interference from S-TX k' when decoding the signals of S-TX k, provided that the signals from S-TX k' are successfully decoded. The SIC decoding order at the monitor is denoted by $\boldsymbol{\pi} = \{\pi_1, \ldots, \pi_K\}$, where π_k is the index of the suspicious communication link whose signals are the k-th to be decoded. Let $\tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi})$ denote the achievable eavesdropping rate of the suspicious communication link k at the monitor. It is assumed that the monitor can successfully decode the signals from the suspicious communication

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

link π_k provided that $\tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) \geqslant r_{\pi_k}(p_M, p_J)$. The following indicator function is defined as

$$\chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) = \begin{cases} 0, & \tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) \geqslant r_{\pi_k}(p_M, p_J), \\ 1, & \tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) < r_{\pi_k}(p_M, p_J). \end{cases} \tag{2}$$

Then, the expression of $\tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi})$ can be written as

$$\tilde{r}_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) = \tau_1 \log_2 \left(1 + \frac{\xi_{\pi_k} p_M \tau_0 \left(I_{\pi_k}\right)^2}{\tau_1(\sigma^2 + p_J g) + \mathcal{I}'_k + \mathcal{I}''_k}\right), \tag{3}$$

where $\mathcal{I}'_k = \sum_{k' \leqslant k-1} \xi_{\pi_{k'}} p_M \tau_0 (I_{\pi_{k'}})^2 \chi_{\pi_{k'}}$ is the interference from suspicious communication links $\pi_{k'}, k' \leqslant k-1$ and $\mathcal{I}''_k = \sum_{k' \geqslant k+1} \xi_{\pi_{k'}} p_M \tau_0 (I_{\pi_{k'}})^2$ is the interference from suspicious communication links $\pi_{k'}, k' \geqslant k+1$. The relative eavesdropping rate is adopted as the design criterion and the problem is formulated as P1:

$$\max_{p_M, p_J, \boldsymbol{\pi} \in \Pi} \frac{\sum_{k=1}^K r_{\pi_k}(p_M, p_J)(1 - \chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}))}{\sum_{k=1}^K r_{\pi_k}(p_M, p_J)} \tag{4}$$

$$\text{s.t. } 0 \leqslant p_M \leqslant P_{\max},\ 0 \leqslant p_J \leqslant \frac{\xi_J p_M g \tau_0}{\tau_1}, \tag{5}$$

where Π is the set of all candidate decoding orders and $P_{\max}$ is the transmit power limit of the monitor.

Proposed algorithms. An auxiliary variable q $(0 \leqslant q \leqslant 1)$ is first introduced to reformulate P1 as P2:

$$\max_{p_M, p_J, \boldsymbol{\pi} \in \Pi} q \tag{6}$$

$$\text{s.t. } \frac{\sum_{k=1}^K r_{\pi_k}(p_M, p_J)(1 - \chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}))}{\sum_{k=1}^K r_{\pi_k}(p_M, p_J)} \geqslant q, \tag{7}$$

and constraint (5).

Let q^* denote the optimal value of P1. Then, P2 is feasible if $q \leqslant q^*$ and is infeasible otherwise. Thus, by using a bisection search of q and checking the feasibility of P2 in each search, the q^* can be obtained, and the solution of P2 with $q = q^*$ is the optimal solution of P1. To check the feasibility of P2 with a given q, the following problem is formulated as P3:

$$\max_{p_M, p_J, \boldsymbol{\pi} \in \Pi} \sum_{k=1}^K r_{\pi_k}(p_M, p_J)(1 - \chi_{\pi_k}(p_M, p_J, \boldsymbol{\pi}) - q) \tag{8}$$

$$\text{s.t. } (5).$$

Note that P2 with a given q is feasible only if the optimal value of P3 is not smaller than zero. In Appendix A, an optimal decoding order given p_M and p_J is proposed. Thus, P3 can be optimally solved by a brute-force search of p_M and p_J, where in each search the optimal decoding order is obtained. The proposed optimal algorithm is summarized in Appendix B. A low-complexity suboptimal algorithm which does not require a brute-force search, is also proposed in Appendix C.

Simulation results. It is assumed that 10 S-TXs and the jammer are randomly deployed around the monitor within a ring with an inner radius of 10 m and an outer radius of 15 m. Each S-RX is assumed to be randomly deployed around its paired S-TX with a distance of 5 m. The channel power gain is modeled as $10^{-4} d^{-2} z$, where d is the distance and z is an exponentially distributed random variable with unit mean. Besides, $P_{\max} = 25$ W, $\sigma^2 = -80$ dBm, $\xi_k = 0.8, \forall k$, $\xi_J = 0.8$, $\tau_0 = 0.8$, and $\tau_1 = 0.2$. Five benchmark algorithms are considered. Specifically, benchmarks 1 and 2 adopt the proposed decoding order, while benchmarks 3–5 adopt the decoding order by the descending order of I_k similar to [9]. Besides, benchmarks 1 and 4 set $p_M = P_{\max}, p_J = \frac{\xi_J p_M g \tau_0}{\tau_1}$, benchmarks 2 and 5 set $p_M = P_{\max}, p_J = 0$, and benchmark 3 obtains p_M, p_J by exhaustive search. Figure 1 shows the comparison results of the performances of different algorithms. It can be seen that the computation time of the suboptimal algorithm is extremely lower (less than 1‰) than that of the optimal algorithm.

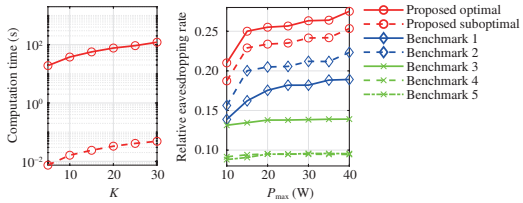

Figure 1 (Color online) Performance comparison.

It is also seen that the relative eavesdropping rate achieved by the suboptimal algorithm is lower than that of the optimal algorithm, but is higher than those achieved by the benchmarks. This indicates that the suboptimal algorithm is not only low-complexity but also having a tolerable performance loss compared to the optimal algorithm.

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Zhao N, Cao Y, Yu F R, et al. Artificial noise assisted secure interference networks with wireless power transfer. IEEE Trans Veh Technol, 2018, 67: 1087–1098
2 Xu D, Li Q. Resource allocation in cognitive wireless powered communication networks with wirelessly powered secondary users and primary users. Sci China Inf Sci, 2019, 62: 029303
3 Xu J, Duan L, Zhang R. Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm. IEEE Wirel Commun, 2017, 24: 152–159
4 Hu Y D, Gao R F, Li Y, et al. On proactive eavesdropping using anti-relay-selection jamming in multi-relay communication systems. Sci China Inf Sci, 2019, 62: 042304
5 Xu D, Zhu H B. Secure transmission for SWIPT IoT systems with full-duplex IoT devices. IEEE Internet Things J, 2019, 6: 10915–10933
6 Hu G, Cai Y. Proactive eavesdropping with masked power beacon for energy-constrained suspicious communication. IEEE Access, 2019, 7: 139035–139046
7 Xu D. Legitimate surveillance with battery-aided wireless powered full-duplex monitor. IEEE Syst J, 2020, 14: 5229–5232
8 Hu G, Cai Y. Proactive eavesdropping via jamming for ergodic rate maximization over wireless-powered multichannel suspicious system. IEEE Commun Lett, 2020, 24: 1830–1834
9 Zhang H, Wang B, Jiang C, et al. Energy efficient dynamic resource optimization in NOMA system. IEEE Trans Wirel Commun, 2018, 17: 5671–5683