Legitimate Eavesdropping with Multiple Wireless Powered Eavesdroppers

Qun Li and Ding Xu(✉)

Nanjing University of Posts and Telecommunications, Nanjing, China
xuding@ieee.org

Abstract. This paper considers a suspicious communication network with multiple suspicious source-destination nodes and multiple wireless powered legitimate eavesdroppers, where the legitimate eavesdroppers are assumed to be collusive or non-collusive. A minimum harvested energy constraint is applied at each eavesdropper such that each eavesdropper must harvest a minimum required energy. The legitimate eavesdropping in such a scenario is investigated and our aim is to maximize the average successful eavesdropping probability by optimizing the power splitting ratio at each eavesdropper under the minimum harvested energy constraint. The optimal algorithm is proposed to solve the optimization problem for both collusive eavesdroppers and non-collusive eavesdroppers. Simulation results show that the proposed algorithm achieves the upper bound of the successful eavesdropping probability when the energy harvesting efficiency is large, the required minimum harvested energy is small, or the transmit power of the suspicious source node is high.

Keywords: Legitimate eavesdropping · Wireless powered communication · Successful eavesdropping probability · Collusive eavesdroppers · Non-collusiveeavesdroppers

1 Introduction

Recently, legitimate eavesdropping in physical layer security has attracted a lot of attention due to its ability to legitimately eavesdrop the communication of suspicious users such as terrorists and criminals for government agencies [1–7]. Specifically, in [1], a legitimate eavesdropper was assumed to eavesdrop a point-to-point suspicious communication by proactive jamming to improve eavesdropping performance. In [2], legitimate proactive eavesdropping was investigated for a point-to-point suspicious communication with a multi-antenna legitimate eavesdropper. In [3], legitimate proactive eavesdropping was investigated for a three-node relay-based suspicious communication. In [4], legitimate eavesdropping was investigated for a hybrid automatic repeat request (HARQ) based point-to-point suspicious communication. In [5], legitimate eavesdropping was investigated by assuming that the legitimate eavesdropper can help the suspicious communication for improving the eavesdropping rate. In [6], the legitimate

H. Gao et al. (Eds.): ChinaCom 2019, LNICST 313, pp. 205–215, 2020.
https://doi.org/10.1007/978-3-030-41117-6_17

eavesdropper with the help from a third-party jammer was assumed to eavesdrop a point-to-point suspicious communication. In [7], legitimate eavesdropping was investigated by assuming that a spoofing relay existed for assisting the legitimate eavesdropping. Note that all the above work in [1–7] considered that the legitimate eavesdroppers are powered by conventional energy sources.

Radio frequency (RF) energy harvesting has attracted a lot of attention due to its ability to power devices by harvesting energy from RF signals [8–11]. Therefore, the legitimate eavesdroppers can also be powered by RF energy harvesting. In this respect, very few work investigated legitimate eavesdropping with wireless powered legitimate eavesdroppers. Particularly, in [12], the performance of legitimate eavesdropping in terms of successful eavesdropping probability with a wireless powered legitimate eavesdropper was investigated for a point-to-point suspicious communication. In [13], offline and online proactive jamming algorithms for the legitimate surveillance with a battery-aided full-duplex wireless powered monitor were proposed. In [14], legitimate eavesdropping in a wireless powered suspicious communication network was investigated and four different performance metrics, namely the successful eavesdropping probability, the average eavesdropping rate, the relative eavesdropping rate and the eavesdropping energy efficiency were evaluated. Note that [12–14] considered a point-to-point suspicious communication with only one legitimate eavesdropper.

This paper investigates legitimate eavesdropping in a suspicious communication network with multiple suspicious source-destination nodes and multiple wireless powered legitimate eavesdroppers. Specifically, the legitimate eavesdroppers are assumed to be collusive or non-collusive, and a minimum harvested energy constraint is applied at each eavesdropper such that each eavesdropper must harvest a minimum required energy. Our aim is to maximize the average successful eavesdropping probability by optimizing the power splitting ratio at each eavesdropper under the minimum harvested energy constraint. For both collusive eavesdroppers and non-collusive eavesdroppers, the optimal algorithm is proposed to solve the optimization problem. It is shown that the proposed algorithm outperforms the reference algorithm and achieves the upper bound of the successful eavesdropping probability when the energy harvesting efficiency is large, the required minimum harvested energy is small, or the transmit power of the suspicious source node is high.

The rest of the paper is organized as follows. Section 2 presents the system model and formulates the investigated problem. Section 3 proposes the optimal algorithms. Section 4 verifies the proposed algorithms by simulation results. Section 5 concludes the paper.

2 System Model and Problem Formulation

As shown in Fig. 1, we consider N pairs of suspicious source-destination nodes in presence of M wireless powered legitimate eavesdroppers. Semi-static fading channels are assumed, where channels are constant within a transmission block and may change from block to block. Let h_i denote the channel power gain of

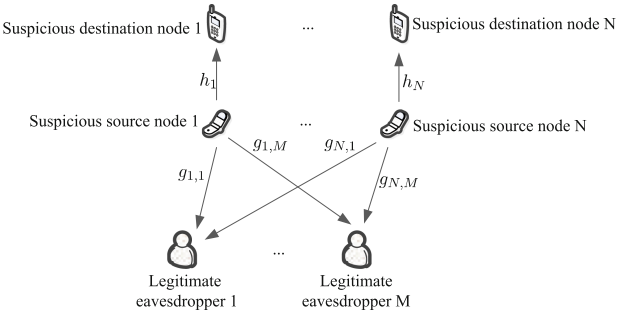

Fig. 1. System model.

the i-th pair of suspicious source-destination nodes and $g_{i,j}$ the channel power gain from the suspicious source node i to the eavesdropper j, respectively. Let p_i denote the transmit power of the suspicious source node i. The achievable rate of the i-th pair of suspicious source-destination nodes is

$$r_0^i = \log_2\left(1 + \frac{p_i h_i}{\sigma^2}\right), \tag{1}$$

where σ^2 denote the noise power. It is assumed that the eavesdroppers are not powered by conventional energy sources and they have to harvest energy for providing enough circuit power. Thus, for the eavesdropper j, a ratio $\rho_{i,j}$ of the receiving power from the suspicious source node i is split for information decoding and the remaining is for energy harvesting. A minimum harvested energy constraint is adopted to guarantee that the eavesdroppers have enough harvested energy, given by

$$\mathbb{E}\left\{\xi \sum_{i=1}^{N}(1-\rho_{i,j})p_i g_{i,j}\right\} \geq Q_j, j = 1, \ldots, M. \tag{2}$$

where $\mathbb{E}$ is the expectation, ξ is the energy harvesting efficiency and Q_j is the minimum harvested energy requirement for the eavesdropper j. The achievable rate at the eavesdropper j for eavesdropping the suspicious source node i is written as

$$r_1^{i,j} = \log_2\left(1 + \frac{\rho_{i,j} p_i g_{i,j}}{\sigma^2}\right). \tag{3}$$

Two scenario are considered for the eavesdroppers. The first scenario assumes that the eavesdroppers are collusive and the achieved eavesdropping rate for the suspicious source node i is written as

$$r_1^i = \log_2\left(1 + \frac{\sum_{j=1}^{M} \rho_{i,j} p_i g_{i,j}}{\sigma^2}\right). \tag{4}$$

The second scenario assumes that the eavesdroppers are not collusive and the achieved eavesdropping rate for the suspicious source node i is written as

$$r_1^i = \log_2\left(1 + \frac{p_i \max_j \ \rho_{i,j} g_{i,j}}{\sigma^2}\right). \tag{5}$$

We assume that as long as $r_1^i \geq r_0^i$, the eavesdroppers can successfully eavesdrop the information from the suspicious source node i, and the successful eavesdropping probability for the suspicious source node i is defined as $\Pr(r_1^i \geq r_0^i)$.

Our aim is to maximize the average successful eavesdropping probability by optimizing the power splitting ratio $\{\rho_{i,j}\}$ under the minimum harvested energy constraint. The optimization problem is formulated as

$$(\text{P1}): \max_{\{\rho_{i,j}\}} \frac{1}{N}\sum_{i=1}^{N} \Pr(r_1^i \geq r_0^i) \tag{6}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, i = 1, \ldots, N, j = 1, \ldots, M, \tag{7}$$

$$\mathbb{E}\left\{\xi \sum_{i=1}^{N} (1 - \rho_{i,j}) p_i g_{i,j}\right\} \geq Q_j, j = 1, \ldots, M. \tag{8}$$

3 Proposed Algorithms

In this section, we investigate P1 with collusive eavesdroppers or non-collusive eavesdroppers. P1 may be infeasible due to the constraint in (8). The feasibility condition for P1 is given as follows. If $\mathbb{E}\left\{\xi \sum_{i=1}^{N} p_i g_{i,j}\right\} \geq Q_j$ is satisfied for all $j = 1, \ldots, M$, then P1 is feasible.

To solve P1, we rewrite $\Pr(r_1^i \geq r_0^i)$ as $\Pr(r_1^i \geq r_0^i) = \mathbb{E}\{X_i\}$, where

$$X_i = \begin{cases} 1, & \text{if } r_1^i \geq r_0^i, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

We optimally solve P1 using convex optimization theory [15], since the time-sharing condition can be verified to be satisfied by P1 [16]. The Lagrangian of P1 can be written as

$$L(\{\lambda_j\}, \{\rho_{i,j}\}) = \frac{1}{N}\sum_{i=1}^{N} \mathbb{E}\{X_i\} + \sum_{j=1}^{M} \lambda_j \left(\mathbb{E}\left\{\xi \sum_{i=1}^{N} (1 - \rho_{i,j}) p_i g_{i,j}\right\} - Q_j\right), \tag{10}$$

where $\lambda_j, j = 1, \ldots, M$ are the non-negative dual variables with respect to the constraint in (8). The dual function $G(\{\lambda_j\})$ is defined as

$$G(\{\lambda_j\}) = \max_{\{\rho_{i,j}\}} L(\{\lambda_j\}, \{\rho_{i,j}\}) \tag{11}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, i = 1, \ldots, N, j = 1, \ldots, M. \tag{12}$$

Then, the dual problem to optimize $\{\lambda_j\}$ is given by

$$\max_{\{\lambda_j\}} G(\{\lambda_j\}) \tag{13}$$

$$\text{s.t. } 0 \leq \lambda_j \leq 1, j = 1, \ldots, M, \tag{14}$$

which can be solved with the subgradient method [15]. Thus, what remains is to solve the problem in (11), which is given in what follows.

The problem in (11) can be decoupled into subproblems, each for a suspicious source node in a transmission block as given by

$$\max_{\{\rho_{i,j}\}} \frac{X_i}{N} - \xi p_i \sum_{j=1}^{M} \lambda_j \rho_{i,j} g_{i,j} \tag{15}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, j = 1, \ldots, M, \tag{16}$$

for $i = 1, \ldots, N$.

3.1 Collusive Eavesdroppers

For collusive eavesdroppers, we discuss the problem in (15) in the following two cases.

Case 1: $X_i = 1$. In this case, we have to satisfy $\sum_{j=1}^{M} \rho_{i,j} g_{i,j} \geq h_i$ in order to let $X_i = 1$. The problem in (15) is thus rewritten as

$$\max_{\{\rho_{i,j}\}} \frac{1}{N} - \xi p_i \sum_{j=1}^{M} \lambda_j \rho_{i,j} g_{i,j} \tag{17}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, j = 1, \ldots, M, \tag{18}$$

$$\sum_{j=1}^{M} \rho_{i,j} g_{i,j} \geq h_i. \tag{19}$$

The above problem belongs to linear programming and thus can be efficiently solved.

Case 2: $X_i = 0$. In this case, we have to satisfy $\sum_{j=1}^{M} \rho_{i,j} g_{i,j} < h_i$ in order to let $X_i = 0$. The problem in (15) is thus rewritten as

$$\max_{\{\rho_{i,j}\}} -\xi p_i \sum_{j=1}^{M} \lambda_j \rho_{i,j} g_{i,j} \tag{20}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, j = 1, \ldots, M, \tag{21}$$

$$\sum_{j=1}^{M} \rho_{i,j} g_{i,j} < h_i. \tag{22}$$

It is easy to verify that the optimal solution of the above problem is $\rho_{i,j} = 0, j = 1, \ldots, M$ and the optimal objective function value is 0.

Algorithm 1. Proposed algorithm to solve P1 with collusive eavesdroppers.

1: Initialize: $\lambda_j, j = 1, \ldots, M$.
2: **repeat**
3: **for** $i = 1$ to N **do**
4: Obtain $\rho_{i,j}, j = 1, \ldots, M$ by solving the problem in (17) using linear programming and denote its optimal objective function value as O.
5: **if** $O < 0$ **then**
6: Set $\rho_{i,j} = 0, j = 1, \ldots, M$.
7: **end if**
8: **end for**
9: Update $\lambda_j, j = 1, \ldots, M$ by the subgradient method.
10: **until** $\lambda_j, j = 1, \ldots, M$ converge to a desired accuracy.

Based on the above discussion on the problem in (15) with collusive eavesdroppers, its optimal solution is obtained by the following steps: Firstly, the problem in (17) is solved with linear programming. Then, if the optimal objective function value in (17) is larger than or equal to 0, the optimal solution the problem in (17) is the optimal solution of the problem in (17). Otherwise, the optimal solution of the problem in (17) is $\rho_{i,j} = 0, j = 1, \ldots, M$.

The algorithm to solve P1 with collusive eavesdroppers is summarized in Algorithm 1.

3.2 Non-collusive Eavesdroppers

For non-collusive eavesdroppers, we discuss the problem in (15) in the following two cases.

Case 1: $X_i = 1$. In this case, we have to satisfy $\max_j \rho_{i,j} g_{i,j} \geq h_i$ in order to let $X_i = 1$. The problem in (15) is thus rewritten as

$$\max_{\{\rho_{i,j}\}} \frac{1}{N} - \xi p_i \sum_{j=1}^{M} \lambda_j \rho_{i,j} g_{i,j} \tag{23}$$

$$\text{s.t. } 0 \leq \rho_{i,j} \leq 1, j = 1, \ldots, M, \tag{24}$$

$$\max_j \rho_{i,j} g_{i,j} \geq h_i. \tag{25}$$

Define the set $\mathbb{J}_i = \{j | \frac{h_i}{g_{i,j}} \leq 1, j = 1, \ldots, M\}$. Suppose that $\rho_{i,j} = \frac{h_i}{g_{i,j}}, j \in \mathbb{J}_i$, then we have $\lambda_j \rho_{i,j} g_{i,j} = \lambda_j h_i$. Thus, the optimal solution of the above problem is

$$\rho_{i,j} = \begin{cases} \frac{h_i}{g_{i,j}}, & j = \arg\min_{k \in \mathbb{J}_i} \lambda_k, \\ 0, & j \neq \arg\min_{k \in \mathbb{J}_i} \lambda_k. \end{cases} \tag{26}$$

The optimal objective function value in (23) is thus $\frac{1}{N} - \xi p_i \lambda_{j^*} h_i$, where $j^* = \arg\min_{k \in \mathbb{J}_i} \lambda_k$.

Algorithm 2. Proposed algorithm to solve P1 with non-collusive eavesdroppers.

1: Initialize: $\lambda_j, j = 1, \ldots, M$.
2: **repeat**
3: Obtain $\rho_{i,j}, i = 1, \ldots, N, j = 1, \ldots, M$ from (30).
4: Update $\lambda_j, j = 1, \ldots, M$ by the subgradient method.
5: **until** $\lambda_j, j = 1, \ldots, M$ converge to a desired accuracy.

Case 2: $X_i = 0$. In this case, we have to satisfy $\max_j \rho_{i,j} g_{i,j} < h_i$ in order to let $X_i = 0$. The problem in (15) is thus rewritten as

$$\max_{\{\rho_{i,j}\}} \; -\xi p_i \sum_{j=1}^{M} \lambda_j \rho_{i,j} g_{i,j} \tag{27}$$

$$\text{s.t. } 0 \le \rho_{i,j} \le 1, j = 1, \ldots, M, \tag{28}$$

$$\max_j \; \rho_{i,j} g_{i,j} < h_i. \tag{29}$$

It is easy to verify that the optimal solution of the above problem is $\rho_{i,j} = 0, j = 1, \ldots, M$ and the optimal objective function value is 0.

Based on the above discussion on the problem in (15) with non-collusive eavesdroppers, its optimal solution is obtained as

$$\rho_{i,j} = \begin{cases} \frac{h_i}{g_{i,j}}, & j = \arg\min_{k \in \mathbb{J}_i} \lambda_k, \\ & \frac{1}{N} - \xi p_i \lambda_j h_i \ge 0, \\ 0, & \text{otherwise}, \end{cases} \tag{30}$$

for $j = 1, \ldots, M$.

The algorithm to solve P1 with non-collusive eavesdroppers is summarized in Algorithm 2.

4 Simulation Results

This section provides simulation results to verify the proposed algorithm with collusive eavesdroppers or non-collusive eavesdroppers. In the simulation, all the channel power gains are assumed to follow exponential distribution with unit mean and we set $\sigma^2 = 1$, $N = 2$, $M = 2$ and $p_i = p, i = 1, \ldots, N$. For performance comparison, a reference algorithm which sets $\rho_{i,j} = 0.5$ for all $i = 1, \ldots, N, j = 1, \ldots, M$ is adopted. Besides, an upper bound for the proposed algorithm which ignores the minimum harvested energy constraint and sets $\rho_{i,j} = 1$ for all $i = 1, \ldots, N, j = 1, \ldots, M$ is also adopted.

Figure 2 plots the average successful eavesdropping probability against ξ with $Q = 2\,\text{W}$ and $p = 5\,\text{W}$ for different algorithms. Note that zero average successful eavesdropping probability means P1 is infeasible for the adopted algorithm. It is shown that the average successful eavesdropping probability increases as ξ increases. This is because a higher ξ leads to higher energy harvested by

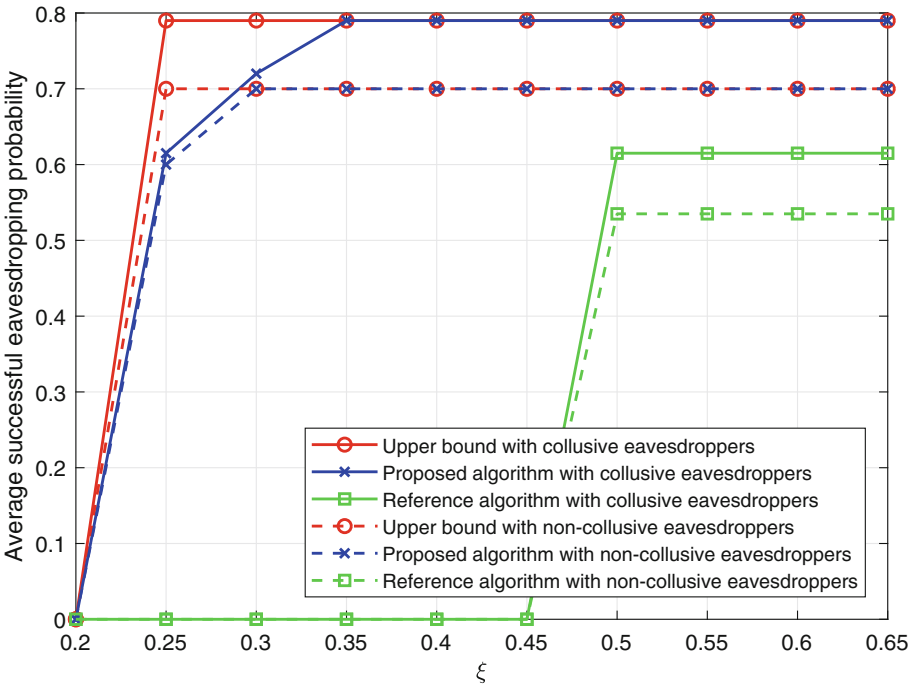

Fig. 2. Average successful eavesdropping probability against ξ ($Q = 2\,\mathrm{W}$ and $p = 5\,\mathrm{W}$).

the eavesdroppers and thus can leave more signal power for information eavesdropping. It is also shown that the average successful eavesdropping probability saturates when ξ is high. This is because in this case, the performance is not restricted by the minimum harvested energy constraint. Besides, it is seen that the average successful eavesdropping probability achieved by the proposed algorithm with collusive eavesdroppers is higher than that with non-collusive eavesdroppers, and the proposed algorithm with collusive/non-collusive eavesdroppers outperforms the reference algorithm with collusive/non-collusive eavesdroppers. It is also seen that the average successful eavesdropping probability achieved by the proposed algorithm with collusive/non-collusive eavesdroppers is lower than the upper bound with collusive/non-collusive eavesdroppers when ξ is small and overlaps with the upper bound with collusive/non-collusive eavesdroppers when ξ is large. This indicates that the proposed algorithm can achieve the upper bound when ξ is large.

Figure 3 plots the average successful eavesdropping probability against Q with $\xi = 0.35$ and $p = 5\,\mathrm{W}$ for different algorithms. It is shown that the average successful eavesdropping probability decreases as Q increases. This is because a higher Q means the eavesdroppers need to harvest more energy and thus leaves less signal power for information eavesdropping. It is also shown that

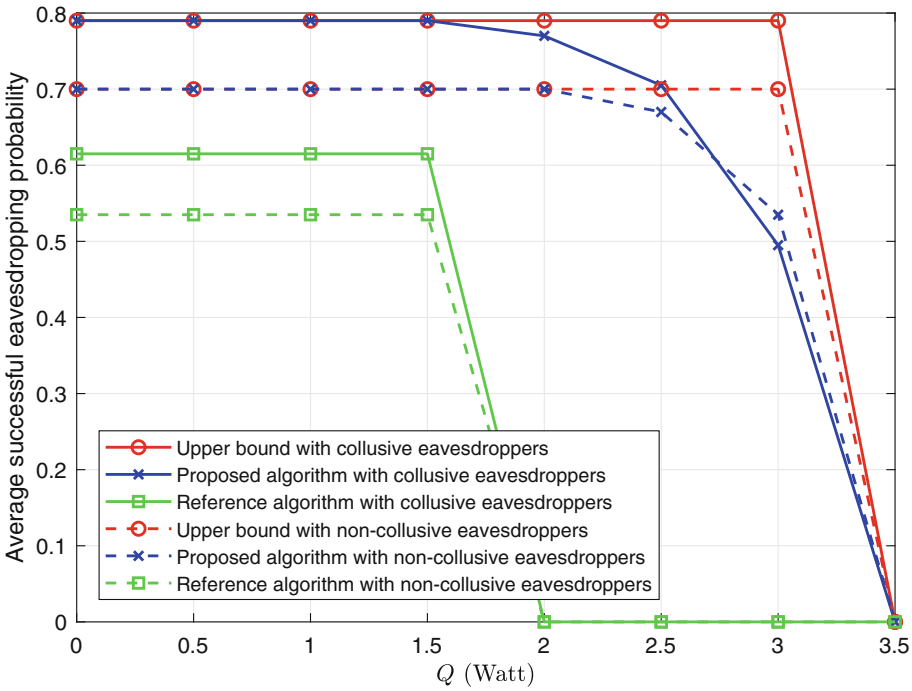

Fig. 3. Average successful eavesdropping probability against Q ($\xi = 0.35$ and $p = 5\,\mathrm{W}$).

the average successful eavesdropping probability is unchanged as Q increases when Q is low. This is because in this case, the performance is not restricted by the minimum harvested energy constraint. Besides, it is seen that the average successful eavesdropping probability achieved by the proposed algorithm with collusive/non-collusive eavesdroppers overlaps with the upper bound with collusive/non-collusive eavesdroppers when Q is small and is lower than the upper bound with collusive/non-collusive eavesdroppers when Q is large. This indicates that the proposed algorithm can achieve the upper bound when Q is small.

Figure 4 plots the average successful eavesdropping probability against p with $\xi = 0.3$ and $Q = 1.5\,\mathrm{W}$ for different algorithms. It is shown that the average successful eavesdropping probability increases as p increases. This is because a higher p leads to higher energy harvested by the eavesdroppers and thus can leave more signal power for information eavesdropping. It is also shown that the average successful eavesdropping probability saturates when p is high. This means the performance is not restricted by the minimum harvested energy constraint when p is high. Besides, it is seen that the average successful eavesdropping probability achieved by the proposed algorithm with collusive/non-collusive eavesdroppers is lower than the upper bound with collusive/non-collusive eavesdroppers when

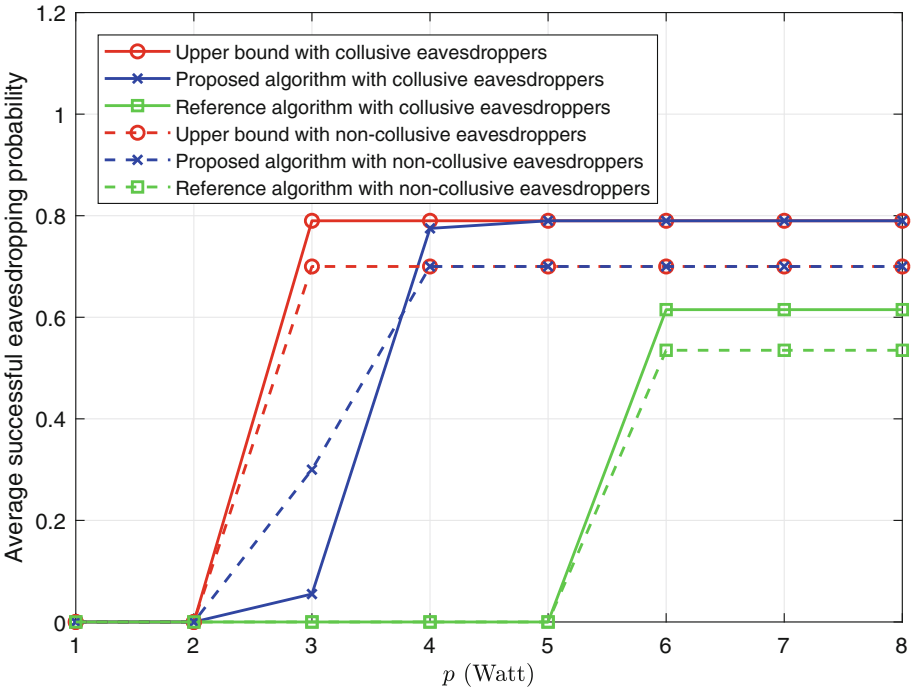

Fig. 4. Average successful eavesdropping probability against p ($\xi = 0.3$ and $Q = 1.5\,\mathrm{W}$).

p is small and overlaps with the upper bound with collusive/non-collusive eavesdroppers when p is large. This indicates that the proposed algorithm can achieve the upper bound when p is large.

5 Conclusions

We investigate legitimate eavesdropping in a suspicious communication network with multiple suspicious source-destination nodes and multiple wireless powered legitimate eavesdroppers, where the legitimate eavesdroppers are assumed to be collusive or non-collusive. The aim is to maximize the average successful eavesdropping probability by optimizing the power splitting ratio at each eavesdropper under the minimum harvested energy constraint. We derive the optimal algorithm to solve the optimization problem for both collusive eavesdroppers and non-collusive eavesdroppers. It is shown that the proposed algorithm achieves the upper bound of the successful eavesdropping probability when the energy harvesting energy is large, the required minimum harvested energy is small, or the transmit power of the suspicious source node is high.

References

1. Xu, J., Duan, L., Zhang, R.: Proactive eavesdropping via cognitive jamming in fading channels. IEEE Trans. Wirel. Commun. **16**(5), 2790–2806 (2017)
2. Zhong, C., Jiang, X., Qu, F., Zhang, Z.: Multi-antenna wireless legitimate surveillance systems: design and performance analysis. IEEE Trans. Wirel. Commun. **16**(7), 4585–4599 (2017)
3. Hu, D., Zhang, Q., Yang, P., Qin, J.: Proactive monitoring via jamming in amplify-and-forward relay networks. IEEE Signal Process. Lett. **24**(11), 1714–1718 (2017)
4. Xu, J., Li, K., Duan, L., Zhang, R.: Proactive eavesdropping via jamming over HARQ-based communications. In: Proceedings of the IEEE Global Communications Conference, pp. 1–6 (2017)
5. Li, B., Yao, Y., Zhang, H., Lv, Y., Zhao, W.: Energy efficiency of proactive eavesdropping for multiple links wireless system. IEEE Access **6**, 26081–26090 (2018)
6. Xu, D., Li, Q.: Proactive eavesdropping through a third-party jammer. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **101**(5), 878–882 (2018)
7. Zeng, Y., Zhang, R.: Wireless information surveillance via proactive eavesdropping with spoofing relay. IEEE J. Sel. Top. Sign. Process. **10**(8), 1449–1461 (2016)
8. Xu, D., Li, Q.: Resource allocation for secure communications in cooperative cognitive wireless powered communication networks. IEEE Syst. J. **13**(3), 2431–2442 (2019)
9. Zeng, Y., Clerckx, B., Zhang, R.: Communications and signals design for wireless power transmission. IEEE Trans. Commun. **65**(5), 2264–2290 (2017)
10. Xu, D., Zhu, H.: Secure transmission for SWIPT IoT systems with full-duplex IoT devices. IEEE IoT J. **6**, 10915–10933 (2019)
11. Zhang, H., Huang, S., Jiang, C., Long, K., Leung, V.C., Poor, H.V.: Energy efficient user association and power allocation in millimeter-wave-based ultra dense networks with energy harvesting base stations. IEEE J. Sel. Areas Commun. **35**(9), 1936–1947 (2017)
12. Xu, D., Li, Q.: Legitimate surveillance with a wireless powered monitor in rayleigh fading channels. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **101**(1), 293–297 (2018)
13. Xu, D.: Legitimate surveillance with battery-aided wireless powered full-duplex monitor. IEEE Syst. J. (Accepted for publication)
14. Xu, D., Zhu, H., Li, Q.: Jammer-assisted legitimate eavesdropping in wireless powered suspicious communication networks. IEEE Access **7**, 20363–20380 (2019)
15. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)
16. Yu, W., Lui, R.: Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans. Commun. **54**(7), 1310–1322 (2006)