Hindawi
Mobile Information Systems
Volume 2020, Article ID 7847623, 6 pages
https://doi.org/10.1155/2020/7847623

Research Article

Rate Maximization for Suspicious Multicast Communication Networks with Full-Duplex Proactive Monitoring

Dongsheng Liu,[1] Sai Zhao,[2] Quanzhong Li,[3] and Jiayin Qin[1]

[1]*School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, Guangdong, China*
[2]*School of Mechanical and Electrical Engineering, Guangzhou University, Guangzhou 510006, Guangdong, China*
[3]*School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, Guangdong, China*

Correspondence should be addressed to Quanzhong Li; liquanzh@mail.sysu.edu.cn

Received 5 January 2020; Revised 11 June 2020; Accepted 19 June 2020; Published 10 July 2020

Academic Editor: Adrian Kliks

In this paper, we investigate the optimization of the monitoring rate for a suspicious multicast communication network with a legitimate full-duplex (FD) monitor, where the FD monitor is proactive to jam suspicious receivers and eavesdrop from the suspicious transmitter simultaneously. To effectively monitor the suspicious communication over multicast networks, we maximize the monitoring rate under the outage probability constraint of the suspicious multicast communication network and the jamming power constraint at the FD monitor. The formulated optimization problem is nonconvex, and its global optimal solution is hard to obtain. Thus, we propose a constrained concave convex procedure- (CCCP-) based iterative algorithm, which is able to achieve a local optimal solution. Simulation results demonstrate that the proposed proactive eavesdropping scheme with optimal jamming power outperforms the conventional passive eavesdropping scheme.

1. Introduction

With dramatical development in wireless communication technologies, wireless networks have been widely used owing to the advantages such as mobility and flexibility. However, the openness of wireless information makes wireless networks face serious security challenges. Physical layer security has recently received significantly considerable attention to enhance the quality of secure communication, and therefore, it has been recognized as a new design paradigm to provide information security in wireless networks. In this new design paradigm, the propagation characteristics of wireless channels are taken into consideration against conventional (i.e., passive) eavesdroppers and novel (i.e., proactive) eavesdroppers.

The ubiquitous accessibility of wireless communication channels makes it more vulnerable to be misused by malicious users, causing latent danger to public security. Fortunately, suspicious communications could be discovered and prevented through passive monitoring when the channel quality of legitimate monitoring agencies is better than that of the suspicious users. However, in practice, this is not always possible, resulting in limited legitimate monitoring performance. Therefore, legitimate agencies should employ advanced effective measures to proactively monitor these suspicious communications for various purposes in order to circumvent the performance limitations caused by the disadvantageous channels.

Recently, some works have proposed different legitimate monitoring methods for suspicious wireless networks. In [1–3], Xu et al. proposed a legitimate monitoring scheme for a point-to-point suspicious wireless communication link via jamming over Rayleigh fading channels. In [4], Mobini et al. proposed a proactive eavesdropping scheme, wherein an FD monitor eavesdropped suspicious communication while sending the collected information to the unmanned aerial vehicle (UAV). In [5], Moon et al. considered a proactive eavesdropping scenario, where a central monitor tried to intercept the information exchanged between a pair of suspicious entities through amplify-and-forward FD relays and a cooperative jammer. In [6], Huang et al. proposed a wiretap channel with a transmitter, a receiver, and an eavesdropper. In this paper, the eavesdropper operates in an FD mode so as to reduce the secrecy rate of the transmitter-receiver pair through simultaneous wiretapping and jamming. In [7], Jiang et al. investigated the effective eavesdropping rate maximization problem in a legitimate surveillance relaying system, in which the legitimate monitor adaptively acted as an eavesdropper, a jammer, or a helper. In [8], Zeng and Zhang proposed a new proactive eavesdropping approach via a spoofing relay between a suspicious transmitter and a suspicious receiver to vary the source transmission rate. In [9], Cumanan et al. studied optimization frameworks for a multicast network where a transmitter broadcasted the same information to a group of legitimate users in the presence of multiple eavesdroppers.

However, to the best of our knowledge, research on the legitimate monitoring performance optimization for suspicious multicast communication networks is still missing. Therefore, in this paper, we investigate the monitoring rate maximization problem for a suspicious multicast communication network with a legitimate FD monitor. To effectively monitor the suspicious communication over multicast networks, the FD monitor is proactive to jam suspicious receivers and eavesdrop from the suspicious transmitter by operating in the FD mode. We first derive the average proactive eavesdropping rate of the monitor and the outage probability of the suspicious multicast communication network and then formulate the monitoring rate maximization problem. However, the optimization problem is nonconvex, and its global optimal solution is very difficult to obtain. Therefore, we propose a local optimal solution based on the CCCP. Simulation results show that the proposed proactive eavesdropping scheme is better than the conventional passive eavesdropping scheme.

The rest of this paper is organized as follows. In Section 2, the system model for a suspicious multicast communication network is described, and the monitoring rate maximization problem is formulated. In Section 3, we propose the CCCP-based iterative algorithm. In Section 4, we provide the simulation results to verify our proposed scheme. We conclude our paper in Section 5.

2. System Model and Problem Formulation

Consider a wireless multicast network as in Figure 1 which consists of a suspicious transmitter, N suspicious receivers, denoted by D_i, $i \in N$, $N = \{1, 2, \cdots, N\}$, and a legitimate FD monitor. An example is that criminalities would be monitored since they are usually taken by a terroristic team where a commanding director center sends wireless information to several implementation units. We consider that all the suspicious nodes (i.e., the transmitter and N receivers) are equipped with a single antenna, and the legitimate monitor is equipped with two antennas for the FD operating mode; i.e., the legitimate FD monitor can jam suspicious receivers and eavesdrop from the suspicious transmitter simultaneously [10]. The above settings are reasonable in those implementations including both separate-antenna and shared-antenna architectures [11], which use either two separate antennas or one shared antenna to transmit and receive simultaneously. This concurrent reception and transmission entails a potential coupling between the monitor's receiving and transmitting ends, inducing, thus, self-interference which is known as "echo interference," and its magnitude depends on the isolation between the transmit and receive antennas. The small-scale fading in the link is assumed to follow the Rayleigh distribution. With FD operation, the residual self-interference (RSI) is commonly modeled as a statistical fading distribution, such as Rayleigh fading [12]. Therefore, in this paper, the Rayleigh fading model is adopted to characterize the effects of RSI on the legitimate monitoring performance.

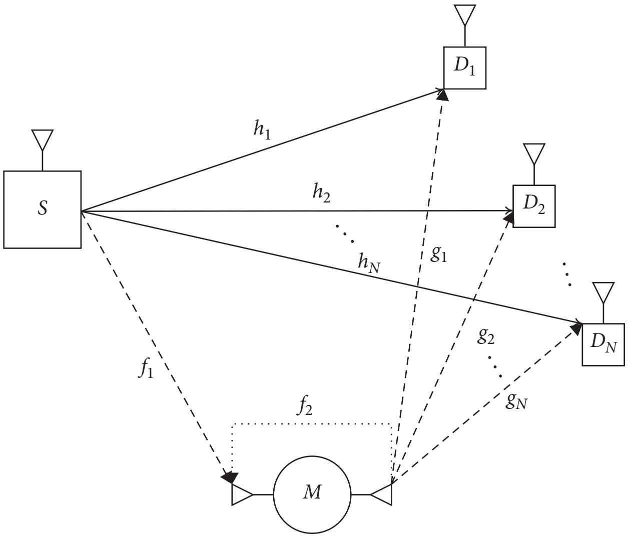

Figure 1: The system model.

We consider a block Rayleigh fading for wireless channels, where the wireless channels remain constant over one transmission block but may change during the other transmission blocks. The channel from the transmitter to the ith receiver, from the transmitter to the receiving antenna of the legitimate monitor, from the transmitting antenna of the legitimate monitor to the ith receiver, and from the transmitting antenna to the receiving antenna at the legitimate monitor is denoted as h_i, f_1, g_i, and f_2, respectively. Thus, $|h_i|^2$, $|f_1|^2$, $|g_i|^2$, and $|f_2|^2$ are modeled as independent exponential distributed random variables with parameters λ_i, ρ_1, μ_i, and ρ_2, respectively. It is assumed that the legitimate monitor does not know the channel state information (CSI) at each time block, while it knows their channel distribution information (CDI) [1]. In a given time slot, the suspicious transmitter employs a constant power P to broadcast a signal $\sqrt{P}\,x$ with $E[|x|^2] = 1$ ($E[\cdot]$ is the expectation operator), to all N suspicious receivers, while the legitimate monitor employs a jamming power Q, which is able to be adjusted according to the predefined outage probability constraint and the RSI level, to broadcast an interference signal $\sqrt{Q}\,z$ with $E[|z|^2] = 1$, to all N suspicious receivers. Then, the received signal at the legitimate monitor and the ith suspicious receiver can be expressed as

$$y_0 = f_1\sqrt{P}x + f_2\sqrt{KQ}z + n_0, \quad (1)$$

$$y_i = h_i\sqrt{P}x + g_i\sqrt{Q}z + n_i, \quad (2)$$

respectively, where K denotes the RSI level at the legitimate monitor after cancellation and $0 \leq K \leq 1$, depending on the self-interference cancellation technique at the legitimate monitor. For example, $K = 0$ means that the legitimate monitor is able to perfectly cancel the self-interference, and $K = 1$ means that the legitimate monitor cannot cancel any self-interference.

The additive noise at the legitimate monitor and the ith suspicious receiver is denoted as n_0 and n_i, respectively. Without loss of generality, the additive noises are all assumed with zero mean and unit variance, i.e., $n_0 \sim CN(0, 1)$ and $n_i \sim CN(0, 1)$. Therefore, the achievable rate at the legitimate monitor and the ith suspicious receiver can be expressed as

$$\tau_0 = \log_2 \left(1 + \gamma_0\right), \tag{3}$$

$$\tau_i = \log_2 \left(1 + \gamma_i\right), \tag{4}$$

respectively, where

$$\begin{aligned} \gamma_0 &= \frac{P\left|f_1\right|^2}{KQ\left|f_2\right|^2 + 1}, \\ \gamma_i &= \frac{P\left|h_i\right|^2}{Q\left|g_i\right|^2 + 1}. \end{aligned} \tag{5}$$

Since the suspicious transmitter is not aware of the instantaneous CSI of the suspicious links, we assume that the suspicious transmitter employs a fixed transmission rate, denoted as τ, for signal transmission [1]. As a consequence, the outage probability at the legitimate monitor and the ith suspicious receiver can be, respectively, expressed as

$$p_0^{\text{out}} = \Pr\left(\tau_0 < \tau\right) = 1 - \frac{\exp\left[-\left(2^\tau - 1\right)\rho_1/P\right]}{\left(2^\tau - 1\right)\rho_1 KQ/\left(\rho_2 P\right) + 1}, \tag{6}$$

$$p_i^{\text{out}} = \Pr\left(\tau_i < \tau\right) = 1 - \frac{\exp\left[-\left(2^\tau - 1\right)\lambda_i/P\right]}{\left(2^\tau - 1\right)\lambda_i Q/\left(\mu_i P\right) + 1}. \tag{7}$$

From equation (6), the average proactive eavesdropping rate τ_{avg} at the legitimate monitor is [1]

$$\tau_{\text{avg}} = \tau\left(1 - p_0^{\text{out}}\right) = \frac{\tau \exp\left[-\left(2^\tau - 1\right)\rho_1/P\right]}{\left(2^\tau - 1\right)\rho_1 KQ/\left(\rho_2 P\right) + 1}. \tag{8}$$

Then, the outage probability of the suspicious multicast communication network can be expressed as

$$p_D^{\text{out}} = 1 - \prod_{i=1}^{N}\left(1 - p_i^{\text{out}}\right) = 1 - \prod_{i=1}^{N} \frac{\exp\left[-\left(2^\tau - 1\right)\lambda_i/P\right]}{\left(2^\tau - 1\right)\lambda_i Q/\left(\mu_i P\right) + 1}. \tag{9}$$

In this paper, we aim to maximize the average proactive eavesdropping rate τ_{avg} at the legitimate monitor under the outage probability constraint of the suspicious multicast communication network and the jamming power constraint at the FD monitor, which is formulated as

$$\max_{\tau, Q} \quad \tau_{\text{avg}}, \tag{10a}$$

$$\text{s.t.} \quad p_D^{\text{out}} = \varepsilon, \tag{10b}$$

$$0 \leq Q \leq Q_{\max}, \tag{10c}$$

where $Q_{\max}$ denotes the maximum available jamming power budget at the legitimate monitor. In problem (10), the first constraint ensures that the outage probability of the suspicious multicast communication network cannot exceed the predefined threshold after jammed by the legitimate monitor with the power Q, and the second constraint ensures that the jamming power employed at the legitimate monitor cannot exceed the maximum available budget.

3. Local Optimal Solution to Problem (10)

The objective (10a) and the constraint (10b) are nonconvex, thus problem (10) is nonconvex, and its global optimal solution is very hard to find. In this section, we will develop a local optimal solution for solving problem (10).

Combining (9) with (10b) and after some mathematical manipulation, we can obtain

$$\sum_{i=1}^{N}\left\{\ln\left[1 + \left(2^\tau - 1\right)\frac{\lambda_i Q}{\mu_i P}\right] + \left(2^\tau - 1\right)\frac{\lambda_i}{P}\right\} = -\ln\left(1 - \varepsilon\right). \tag{11}$$

However, (11) is intractable to obtain a closed-form expression of τ due to its hybridization of the logarithm in the summarization computation. Note that τ is a monotonically decreasing function in Q. Then, combining with the jamming power budget constraint (10c), we have

$$\tau\left(Q_{\max}\right) \leq \tau \leq \tau(0), \tag{12}$$

where

$$\tau(0) = \log_2\left(1 + \frac{-P\ln\left(1 - \epsilon\right)}{\sum_{i=1}^{N}\lambda_i}\right). \tag{13}$$

On the other hand, it is easy to observe that the left hand side of (11) increases as τ varies from $\tau(Q_{\max})$ to $\tau(0)$. Therefore, we can obtain $\tau(Q_{\max})$ under the maximum available jamming power $Q_{\max}$ by solving the following optimization problem [13]:

$$\min_{\tau} \quad \tau, \tag{14a}$$

$$\text{s.t.} \quad \sum_{i=1}^{N}\left\{\ln\left[1 + \left(2^\tau - 1\right)\frac{\lambda_i Q_{\max}}{\mu_i P}\right] + \left(2^\tau - 1\right)\frac{\lambda_i}{P}\right\} \geq -\ln\left(1 - \epsilon\right). \tag{14b}$$

Based on the obtained $\tau(Q_{\max})$, the optimization problem (10) can be rewritten as

$$\max_{\tau, Q} \quad \frac{\tau \exp\left[-\left(2^\tau - 1\right)\rho_1/P\right]}{\left(2^\tau - 1\right)\rho_1 KQ/\left(\rho_2 P\right) + 1}, \tag{15a}$$

$$\text{s.t.} \quad (12). \tag{15b}$$

By introducing the slack variables t and x, the optimization problem (15) can be equivalently recast as

$$\max_{\tau,Q,t,x} \quad t, \tag{16a}$$

$$\text{s.t.} \quad \tau \exp\left(-(2^{\tau}-1)\frac{\rho_1}{P}\right) \geq tx, \tag{16b}$$

$$(2^{\tau}-1)\frac{\rho_1 K Q}{\rho_2 P} + 1 \leq x, \tag{16c}$$

$$\tau(Q_{\max}) \leq \tau \leq \tau(0). \tag{16d}$$

The equivalence between problems (15) and (16) can be guaranteed as the constraints (16b) and (16c) hold with equality at the optimum. Otherwise, we can increase t and decrease x to obtain a larger objective value without violating the constraints. In the following, we focus on solving the optimization problem (16).

Taking the advantages of monotonicity and concavity of the function $\ln(\cdot)$, (16b) and (16c) can be converted into difference of convex (DC) forms. Thus, the optimization problem (16) can be transformed to a DC programming problem [14, 15]. In the following, we propose a CCCP-based iterative algorithm to solve the DC programming [16, 17].

We first define a function $h(z) = \ln(z)$, whose first-order Taylor expansion around the current point $\hat{z}$ is

$$\hat{h}(z,\hat{z}) = \ln(\hat{z}) + \frac{z-\hat{z}}{\hat{z}}. \tag{17}$$

Then, in the $(n+1)$th iteration of the proposed iterative algorithm, given $\{\tau^{(n)}, Q^{(n)}, t^{(n)}, x^{(n)}\}$, which is optimal in the nth iteration, we solve the following convex optimization problem [13]:

$$\max_{\tau,Q,t,x} \quad t, \tag{18a}$$

$$\text{s.t.} \quad \hat{h}\left(t,t^{(n)}\right) + \hat{h}\left(x,x^{(n)}\right) - \ln(\tau) + (2^{\tau}-1)\frac{\rho_1}{P} \leq 0, \tag{18b}$$

$$\hat{h}\left(2^{\tau}-1, 2^{\tau^{(n)}}-1\right) + \ln\left(\frac{\rho_1 K}{\rho_2 P}\right) + \hat{h}\left(Q,Q^{(n)}\right) - \ln(x-1) \leq 0, \tag{18c}$$

$$(12). \tag{18d}$$

Now, we summarize the proposed CCCP-based iterative algorithm as given in Algorithm 1.

For Algorithm 1, its convergence result is given as below.

Proposition 1. *Algorithm 1 converges to a local optimal point of problem (16).*

Proof. The proof of Proposition 1 can be directly found in [16] and omitted for brevity. □

To implement Algorithm 1, we need to solve the convex problem (18), which can be done effectively by using the gradient projection (GP) algorithm with computational complexity $O(\varepsilon^{-2})$ when the GP iterations are set to stop under the condition that the magnitude of the gradient is less or equal to ε [18]. Accordingly, the computational complexity of Algorithm 1 is $O(L\varepsilon^{-2})$, where L is the iteration number for the convergence of Algorithm 1.

After finding t^* by Algorithm 1, we can obtain the maximum proactive eavesdropping rate at the legitimate monitor as

$$\tau_{\text{avg}}^{\text{opt}} = \max\left(\min\left(\tau_{avg}(\tau(0)), t^*\right), \tau_{avg}\left(\tau(Q_{\max})\right)\right). \tag{19}$$

4. Simulation Results

In this section, we numerically evaluate the maximum achievable proactive eavesdropping rate $\tau_{\text{avg}}^{\text{opt}}$ at the legitimate monitor. The average channel power gain parameters are set to be $\lambda_i = 0.5$, $\rho_1 = 50$, $\mu_i = 50$, and $\rho_2 = 0.02$, respectively [10]. Furthermore, we set the outage probability threshold and the maximum jamming power budget at the legitimate monitor as $\epsilon = 0.05$ and $Q_{\max} = 20$ dB, respectively [1].

In Figure 2, we present the maximum achievable average eavesdropping rate $\tau_{\text{avg}}^{\text{opt}}$ at the legitimate monitor versus the RSI level, K, under the imperfect self-interference cancellation (ISIC) scheme, compared with the perfect self-interference cancellation (PSIC) scheme in [1]. From Figure 2, we can see that with the increase in the RSI level, the maximum achievable eavesdropping rate will decrease, until to a certain value, which means that the RSI level has significant importance on the maximum achievable average eavesdropping rate of the legitimate monitor. Proactive eavesdropping strategy brings better monitoring performance than the passive eavesdropping strategy at the legitimate monitor. However, the proactive eavesdropping strategy can be only proposed under a certain RSI level. When the RSI level exceeds a threshold value, the passive eavesdropping strategy should be proposed at the legitimate monitor. Moreover, the more the power employed by the suspicious transmitter and the more the suspicious receivers, the greater the maximum achievable average eavesdropping rate can be obtained by the legitimate monitor under proactive and passive monitoring strategies.

In Figure 3, we present the optimal jamming power Q at the legitimate monitor versus the RSI level, K, under the ISIC scheme, compared with the PSIC scheme in [1]. From Figure 3, we can see that when the legitimate monitor is not able to operate sufficient SIC [19], e.g., the RSI level, $K > -60$ dB while $N = 6$ and $K > -30$ dB while $N = 1$, less jamming power should be employed at the legitimate monitor to obtain optimal monitoring performance. Especially, if K exceeds a certain threshold value, e.g., $K = -35$ dB while $N = 6$ or $K = -25$ dB while $N = 1$, respectively, the legitimate monitor should employ no jamming power to jam the suspicious receivers any more, which means that the legitimate monitoring strategy degenerates from proactive eavesdropping to passive eavesdropping, resulting in worse monitoring performance. This is because when K exceeds a

```
(1) Input: $N$, $\lambda_i$, $\rho_1$, $\mu_i$, $\rho_2$, $P$, $Q_{\max}$, $K$
(2) Initialization: set the iteration number $n := 1$ and a feasible point $\{\tau^{(0)}, Q^{(0)}, t^{(0)}, x^{(0)}\}$;
(3) Repeat:
      Obtain $\{\tau^{(n)}, Q^{(n)}, t^{(n)}, x^{(n)}\}$ by solving the convex problem (18);
      Update $n := n + 1$;
(4) Until: convergence.
```

Algorithm 1: The proposed CCCP-based iterative algorithm for solving problem (16).

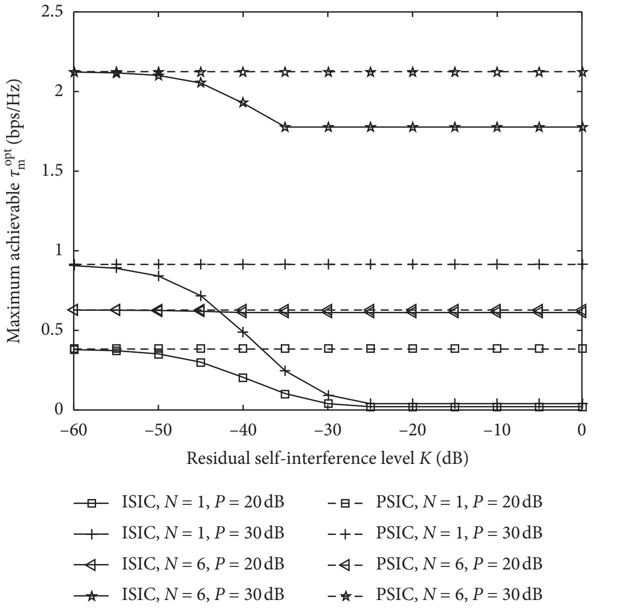

Figure 2: The maximal achievable average eavesdropping rate $\tau_{\mathrm{avg}}^{\mathrm{opt}}$ at the legitimate monitor versus the RSI level K.

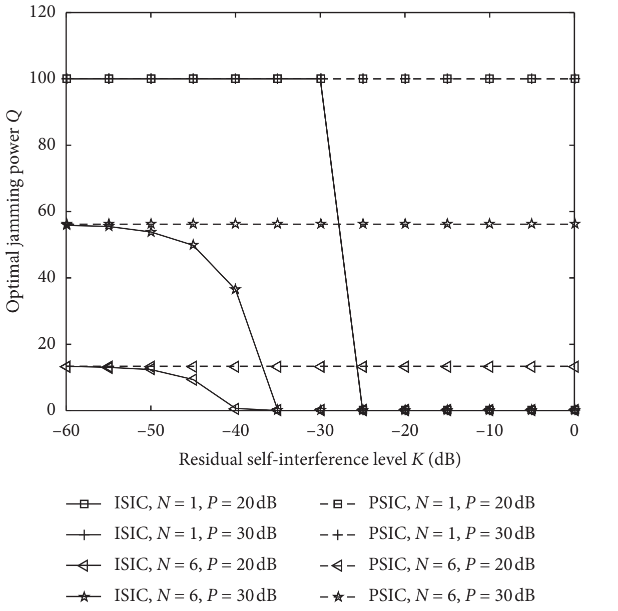

Figure 3: The optimal jamming power Q at the legitimate monitor versus the RSI level K.

certain threshold value, the jamming power will cause more damage to the legitimate monitor than the suspicious receivers. Moreover, the more the power employed by the suspicious transmitter and the less the suspicious receivers, the more the jamming power should be employed by the legitimate monitor under the proactive monitoring strategy.

5. Conclusions

In this paper, we propose an effective legitimate monitoring scheme for suspicious multicast communication networks, where an FD monitor is proactive to jam suspicious receivers and eavesdrop from the suspicious transmitter simultaneously. We formulate the monitoring rate maximization problem and develop a CCCP-based iterative algorithm to find a local optimal solution. Numerical results demonstrate the relationship between the optimal monitoring performance of the legitimate monitor and the RSI levels. The RSI level has significant importance on the monitoring strategy, jamming power, and maximum achievable average eavesdropping rates of the legitimate monitor. As the RSI level is sufficiently small, namely, the legitimate monitor is able to perform PSIC, the optimal monitoring strategy is proactive eavesdropping with optimum jamming power, which realizes a maximum achievable average eavesdropping rate. With the increase in the RSI level, namely, the legitimate monitor performs ISIC, the optimal monitoring strategy is still proactive eavesdropping, however, with less jamming power, which results in a smaller maximum achievable average eavesdropping rate. When the RSI level exceeds a certain threshold value, the jamming power causes more damage to the legitimate monitor than the suspicious receivers, which means that the optimal monitoring strategy is passive eavesdropping with no jamming power.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China, under Grants 61802447 and 61902084, in part by the Guangdong Natural Science

Foundation, under Grants 2014A030310374 and 2018B0303110016, in part by the Guangzhou Science and Technology Program, under Grant 201804010445, and in part by the Featured Innovation Project of the Guangdong Education Department, under Grant 2018KTSCX174.

References

[1] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 80–83, 2016.

[2] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2790–2806, 2017.

[3] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," in *Proceedings of the 2016 IEEE International Conference on Communications*, pp. 2790–2806, Kuala Lumpur, Malaysia, May 2016.

[4] Z. Mobini, B. k. Chalise, M. Mohammadi, H. A. Suraweera, and Z. Ding, "Proactive eavesdropping using UAV systems with full-duplex ground terminals," in *Proceedings of the 2018 IEEE International Conference on Communications Workshops*, pp. 1–6, Kansas City, MO, USA, May 2018.

[5] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6707–6719, 2018.

[6] W. Huang, W. Chen, B. Bai, and Z. Han, "Wiretap channel with full-duplex proactive eavesdropper: a game theoretic approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7658–7663, 2018.

[7] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in relaying systems," *IEEE Signal Processing Letters*, vol. 24, no. 6, pp. 917–921, 2017.

[8] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1449–1461, 2016.

[9] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, 2016.

[10] B. Li, Y. Yao, H. Chen, Y. Li, and S. Huang, "Wireless information surveillance and intervention over multiple suspicious links," *IEEE Signal Processing Letters*, vol. 25, no. 8, pp. 1131–1135, 2018.

[11] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, 2014.

[12] T. K. Baranwal, D. S. Michalopoulos, and R. Schober, "Outage analysis of multihop full duplex relaying," *IEEE Communications Letters*, vol. 17, no. 1, pp. 63–66, 2013.

[13] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, UK, 2004.

[14] R. Horst and N. V. Thoai, "Dc programming: overview," *Journal of Optimization Theory and Applications*, vol. 103, no. 1, pp. 1–43, 1999.

[15] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 130–143, 2020.

[16] A. J. Smola, S. V. N. Vishwanathan, and T. Hofmann, "Kernel methods for missing variables," in *Proceedings of the 10th International Workshop on Artificial Intelligence and Statistics*, pp. 325–332, Bridgetown, Barbados, March 2005.

[17] Q. Li and L. Yang, "Robust optimization for energy efficiency in MIMO two-way relay networks with SWIPT," *IEEE Systems Journal*, vol. 14, no. 1, pp. 196–207, 2020.

[18] Y. Nesterov, *Introductory Lectures on Convex Optimization, Applied Optimization*, Kluwer Academic Publishers, Dordrecht, Netherlands, 2004.

[19] J. R. Krier and I. F. Akyildiz, "Active self-interference cancellation of passband signals using gradient descent," in *Proceedings of the IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, pp. 1212–1216, London, UK, September 2013.