

Proactive Eavesdropping in Relaying Systems

Xin Jiang, *Student Member, IEEE*, Hai Lin, *Senior Member, IEEE*, Caijun Zhong, *Senior Member, IEEE*, Xiaoming Chen, *Senior Member, IEEE*, and Zhaoyang Zhang, *Member, IEEE*

Abstract

This paper investigates the performance of a legitimate surveillance system, where a legitimate monitor aims to eavesdrop on a dubious decode-and-forward relaying communication link. In order to maximize the effective eavesdropping rate, two strategies are proposed, where the legitimate monitor adaptively acts as an eavesdropper, a jammer or a helper. In addition, the corresponding optimal jamming beamformer and jamming power are presented. Numerical results demonstrate that the proposed strategies attain better performance compared with intuitive benchmark schemes. Moreover, it is revealed that the position of the legitimate monitor plays an important role on the eavesdropping performance for the two strategies.

I. INTRODUCTION

With rapid advancements in wireless technologies, wireless communications infrastructure and services have brought great convenience to our daily lives. However, the benefits of wireless communication may be exploited by potential malicious users to commit crimes or terror attacks [1], [2]. Therefore, there is a growing need for the authorized parties such as government agencies to legitimately monitor any suspicious communications to ensure public safety and prevent terrorism.

Responding to this, a new paradigm shift in wireless security by investigating how a legitimate monitor performs legitimate information surveillance, was proposed in [3]–[5]. In particular, the authors proposed a novel approach, namely, proactive eavesdropping via jamming, where the

Copyright (c) 2017 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

Manuscript received March 23, 2017, revised April 9, 2017, accepted April 17, 2017. The associate editor coordinating the review of this paper and approving it for publication was Prof. Yong Xiang.

X. Jiang, C. Zhong, X. Chen and Z. Zhang are with the Institute of Information and Communication Engineering, Zhejiang University, China. (email: caijunzhong@zju.edu.cn).

H. Lin is with the Department of Electrical and Information Systems, Osaka Prefecture University, Osaka 599-8531, Japan (email: lin@eis.osakafuu.ac.jp).

legitimate monitor operates in a full-duplex manner, and purposely transmits jamming signals to interfere with the suspicious link while performs eavesdropping. Later in [6], another spoofing-relay based proactive eavesdropping approach was proposed.

Note that all the aforementioned works focus on the three-node point-to-point communication setup. Thus far, how to perform proactive eavesdropping in relaying systems remains largely an uncharted area. Motivated by this, in this paper, we propose a novel legitimate surveillance approach for dual-hop decode-and-forward (DF) relaying communication systems. Specifically, to maximize the effective eavesdropping rate as in [6], two strategies are designed for the legitimate monitor, which acts adaptively as an information eavesdropper, a destructive jammer or a constructive helper in the two time slots. For each strategy, the optimal jamming beamformer and jamming power are derived. Numerical results reveal that the proposed strategies achieve better performance than some intuitive benchmark schemes.

Notation: We use bold upper case letters to denote matrices, bold lower case letters to denote vectors and lower case letters to denote scalars. $\|\cdot\|$, $(\cdot)^\dagger$ and $\text{tr}(\cdot)$ denote Euclidean norm, conjugate transpose operator and the trace of a matrix, respectively. $\Pi_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^\dagger\mathbf{X})^{-1}\mathbf{X}^\dagger$ represents the orthogonal projection onto the column space of \mathbf{X} and $\Pi_{\mathbf{X}}^\perp \triangleq \mathbf{I} - \Pi_{\mathbf{X}}$ denotes the orthogonal projection onto the orthogonal complement of the column space of \mathbf{X} .

II. SYSTEM MODEL

As shown in Fig. 1, we consider a four-node legitimate surveillance system, where a legitimate monitor E aims to eavesdrop the communication between a suspicious transmitter S and a suspicious receiver D, which is assisted by a DF relay R. We assume that R and E are equipped with N and M antennas, respectively, while S and D are equipped with a single antenna each. All nodes operate in the half-duplex mode and a direct link exists between S and D.

We adopt the time-sharing protocol [7], where the entire communication consists of two time slots. The relay listens to the source transmission during the first time slot, and then forwards the decoded symbol to the destination in the second time slot. In contrast, the legitimate monitor may choose to either jam, eavesdrop, or help, depending on the channel conditions during the two time slots.

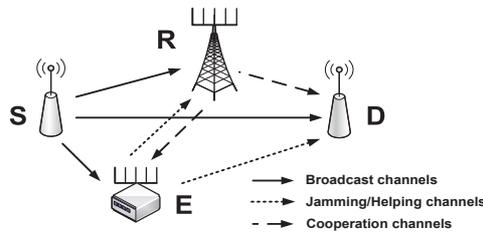


Fig. 1. A four-node legitimate surveillance system.

We assume that all the channel links are composed of large-scale path loss with exponent τ and statistically independent small-scale Rayleigh fading. We denote the inter-node distance of links $S \rightarrow R$, $S \rightarrow D$, $S \rightarrow E$, $R \rightarrow E$, $R \rightarrow D$ and $E \rightarrow D$ by d_1 , d_2 , d_3 , d_4 , d_5 and d_6 , respectively. The corresponding small-scale fading channel coefficients are denoted by $N \times 1$ vector \mathbf{h}_1 , scalar h_2 , $M \times 1$ vector \mathbf{h}_3 , $M \times N$ matrix \mathbf{H}_4 , $1 \times N$ vector \mathbf{h}_5 and $1 \times M$ vector \mathbf{h}_6 , respectively. Quasi-static fading is assumed, such that the channel coefficients remain unchanged during each transmission block but vary independently between different blocks. Each element of these complex fading channel coefficients are circular symmetric complex Gaussian random variables with zero mean and unit variance. Channel reciprocity is also assumed.

We assume that global channel state information (CSI) is available at E^1 , while S , R and D only know the channel gains of relative suspicious channels. This assumption is practical since it is difficult for the suspicious nodes to know the existence of the legitimate monitor and hence conventional physical layer security is not applied to prevent eavesdropping.

III. PROBLEM FORMULATION

In this section, we describe in detail the problem formulation. Depending on the particular action taken by E during the first time slot, we consider two separate scenarios.

A. Strategy I: Jamming First

This scenario is applicable when E is located relatively far away from S , thus E is unlikely to have a good eavesdropping performance. Therefore, in the first phase when S transmits information signal to R and D , E simultaneously transmits jamming noise to disrupt the

¹The CSI can be obtained by utilizing the methods given in paper [4], [6].

suspicious communications. The received signals at R and D can be respectively expressed as $\mathbf{y}_r^{\text{JE}} = \sqrt{\frac{P_s}{d_1^\tau}} \mathbf{h}_1 x + \sqrt{\frac{1}{d_4^\tau}} \mathbf{H}_4^\dagger \mathbf{w} s + \mathbf{n}_r$, and $y_{d1}^{\text{JE}} = \sqrt{\frac{P_s}{d_2^\tau}} h_2 x + \sqrt{\frac{1}{d_6^\tau}} \mathbf{h}_6 \mathbf{w} s + n_{d1}$, where the superscript JE stands for ‘‘jamming-then-eavesdropping’’, P_s denotes the transmit power of S, x and s denote the information and jamming symbol with unit power, respectively. \mathbf{w} is the $M \times 1$ transmit beamforming vector at E with $\mathbf{w}^\dagger \mathbf{w} \leq P$, where P denotes the maximum jamming power at E. In addition, \mathbf{n}_r and n_{d1} are the additive white Gaussian noises (AWGNs) at R and D, respectively. Without loss of generality, the elements of \mathbf{n}_r and n_{d1} follow zero mean Gaussian distribution with unit variance.

In the second phase, R first decodes the information from S using maximal ratio combining (MRC), and then forwards the re-encoded symbol to D using maximum ratio transmission (MRT), while E tries to overhear the signal. The received signals at D and E can be expressed as $y_{d2}^{\text{JE}} = \sqrt{\frac{P_r}{d_5^\tau}} \mathbf{h}_5 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + n_{d2}$, and $\mathbf{y}_e^{\text{JE}} = \sqrt{\frac{P_r}{d_4^\tau}} \mathbf{H}_4 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + \mathbf{n}_{e2}$, where P_r denotes the transmit power of R, n_{d2} and \mathbf{n}_{e2} are the AWGNs at D and E, respectively. Since D observes two copies of the signal, MRC is used to enhance the signal recovery, while E exploits the multiple antennas by using MRC for reception. Therefore, the corresponding SNRs (signal-to-interference-plus-noise ratios, SINRs) at R, D and E can be expressed as $\Gamma_r^{\text{JE}} = \frac{P_s d_4^\tau \|\mathbf{h}_1\|^2}{d_1^\tau \left| \frac{\mathbf{h}_1^\dagger}{\|\mathbf{h}_1\|} \mathbf{H}_4^\dagger \mathbf{w} \right|^2 + d_4^\tau N_0}$, $\Gamma_d^{\text{JE}} = \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2 + \frac{P_s d_6^\tau |h_2|^2}{d_2^\tau |\mathbf{h}_6 \mathbf{w}|^2 + d_2^\tau d_6^\tau N_0}$, and $\Gamma_e^{\text{JE}} = \frac{P_r}{d_4^\tau N_0} \|\mathbf{H}_4 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|}\|^2$, respectively.

B. Strategy II: Eavesdropping First

In contrast to strategy I, it is a better choice to perform eavesdropping in the first phase if the quality of S \rightarrow E link is good. In this case, S broadcasts the information signal to R and D, while E tries to eavesdrop the information. The received signals at R, D, and E can be respectively expressed as $\mathbf{y}_r^* = \sqrt{\frac{P_s}{d_1^\tau}} \mathbf{h}_1 x + \mathbf{n}_r$, $y_{d1}^* = \sqrt{\frac{P_s}{d_2^\tau}} h_2 x + n_{d1}$, and $\mathbf{y}_e^* = \sqrt{\frac{P_s}{d_3^\tau}} \mathbf{h}_3 x + \mathbf{n}_{e1}$ with $*$ \in {EH, EE, EJ}, where each superscript stands for ‘‘eavesdropping-then-helping’’, ‘‘eavesdropping-then-eavesdropping’’, ‘‘eavesdropping-then-jamming’’, respectively. Also, \mathbf{n}_{e1} is the AWGN at E. Therefore, the received SNRs at R and E can be expressed as $\text{SNR}_r^* = \frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2$ and $\text{SNR}_e^* = \frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2$.

Now, depending on the relative channel quality of the suspicious communication link and eavesdropping link, E may take different actions in order to maximize the effective eavesdropping rate in the second phase.

1) *Helping*: If $\text{SNR}_r^* \leq \text{SNR}_e^*$, E is guaranteed to successfully decode the suspicious information. Therefore, in order to further improve the effective eavesdropping rate, E acts as a helper trying to increase the rate of the suspicious link. As such, the received signal at D can be expressed as $y_{d2}^{\text{EH}} = \sqrt{\frac{P_r}{d_5^r}} \mathbf{h}_5 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + \sqrt{\frac{P_e}{d_6^r}} \mathbf{h}_6 \frac{\mathbf{h}_6^\dagger}{\|\mathbf{h}_6\|} x + n_{d2}$, where P_e denotes the transmit power of E. For fairness of comparison between different strategies, we constrain the maximum transmit power as in strategy I, i.e., $0 \leq P_e \leq P$. Therefore, the corresponding SNRs can be expressed as $\Gamma_r^{\text{EH}} = \frac{P_s}{d_1^r N_0} \|\mathbf{h}_1\|^2$, $\Gamma_d^{\text{EH}} = \frac{P_s}{d_2^r N_0} |h_2|^2 + \frac{1}{N_0} (\sqrt{\frac{P_r}{d_5^r}} \|\mathbf{h}_5\| + \sqrt{\frac{P_e}{d_6^r}} \|\mathbf{h}_6\|)^2$, and $\Gamma_e^{\text{EH}} = \frac{P_s}{d_3^r N_0} \|\mathbf{h}_3\|^2$, respectively.

2) *Eavesdropping*: If E is not able to decode the information in the first phase, E may choose to either continue eavesdropping the suspicious link or switch to jamming in the second phase², then the received signals at D and E can be expressed as $y_{d2}^{\text{EE}} = \sqrt{\frac{P_r}{d_5^r}} \mathbf{h}_5 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + n_{d2}$, and $\mathbf{y}_e^{\text{EE}} = \sqrt{\frac{P_r}{d_4^r}} \mathbf{H}_4 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + \mathbf{n}_{e2}$. To strengthen the signal detection, E employs MRC to combine the signals from two time slots. Therefore, the corresponding SNRs can be expressed as $\Gamma_r^{\text{EE}} = \frac{P_s}{d_1^r N_0} \|\mathbf{h}_1\|^2$, $\Gamma_d^{\text{EE}} = \frac{P_s}{d_2^r N_0} |h_2|^2 + \frac{P_r}{d_5^r N_0} \|\mathbf{h}_5\|^2$, and $\Gamma_e^{\text{EE}} = \frac{P_s}{d_3^r N_0} \|\mathbf{h}_3\|^2 + \frac{P_r}{d_4^r N_0} \|\mathbf{H}_4 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|}\|^2$, respectively.

3) *Jamming*: In this case, E performs jamming in an effort to degrade the rate of the suspicious link, so that the probability of the successful eavesdropping can be improved. Therefore, the received signal at D can be expressed as $y_{d2}^{\text{EJ}} = \sqrt{\frac{P_r}{d_5^r}} \mathbf{h}_5 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|} x + \sqrt{\frac{P_e}{d_6^r}} \mathbf{h}_6 \frac{\mathbf{h}_6^\dagger}{\|\mathbf{h}_6\|} s + n_{e2}$. The corresponding SNRs (SINRs) can be expressed as $\Gamma_r^{\text{EJ}} = \frac{P_s}{d_1^r N_0} \|\mathbf{h}_1\|^2$, $\Gamma_d^{\text{EJ}} = \frac{P_s}{d_2^r N_0} |h_2|^2 + \frac{P_r d_5^r \|\mathbf{h}_5\|^2}{P_e d_5^r \|\mathbf{h}_6\|^2 + d_5^r d_6^r N_0}$, and $\Gamma_e^{\text{EJ}} = \frac{P_s}{d_3^r N_0} \|\mathbf{h}_3\|^2$, respectively.

C. Problem Formulation

Depending on the different strategies, the maximum achievable rate of the suspicious link and eavesdropping link can be respectively expressed as $C_{\text{SD}} = \frac{1}{2} \min \left(\log(1 + \Gamma_r^\zeta), \log(1 + \Gamma_d^\zeta) \right)$ and $C_{\text{SE}} = \frac{1}{2} \log(1 + \Gamma_e^\zeta)$, where $\zeta \in \{\text{JE}, \text{EH}, \text{EE}, \text{EJ}\}$. Note that the factor $\frac{1}{2}$ is due to the fact that the entire communication occupies two slots.

²The mode selection criterion will be specified in the next section.

If $C_{SE} \geq C_{SD}$, E can reliably decode the suspicious information with arbitrarily small error probability. As such, the effective eavesdropping rate is given by $R = C_{SD}$ [6]. On the other hand, if $C_{SE} < C_{SD}$, it is impossible for E to decode the information without any error. In this case, the effective eavesdropping rate is defined as $R = 0$. Therefore, the main objective is to optimize the transmit beamforming vector \mathbf{w} for strategy I or the transmit power P_e for strategy II at E, so that the effective eavesdropping rate is maximized. The corresponding optimization problem can be formulated as

$$\begin{aligned}
(\text{P1}) \quad & \max \quad C_{SD} \\
& \text{s.t.} \quad C_{SE} \geq C_{SD} \\
& \quad \quad \mathbf{w}^\dagger \mathbf{w} \leq P \quad \text{or} \quad 0 \leq P_e \leq P.
\end{aligned} \tag{1}$$

IV. OPTIMAL BEAMFORMER AND TRANSMIT POWER DESIGN

In this section, we study the optimal beamformer and transmit power design of optimization problem (P1).

A. Strategy I: Jamming first

Since logarithm is a monotonically increasing function, problem (P1) can be reformulated as

$$\begin{aligned}
(\text{P2}) \quad & \max_{\mathbf{w}} \quad f(\mathbf{w}) \\
& \text{s.t.} \quad \Theta_6 \geq f(\mathbf{w}) \quad \text{and} \quad \mathbf{w}^\dagger \mathbf{w} \leq P,
\end{aligned} \tag{2}$$

where $f(\mathbf{w}) = \min(\Theta_1 + \frac{\Theta_2}{|\mathbf{h}_6 \mathbf{w}|^2 + \Theta_3}, \frac{\Theta_4}{\frac{|\mathbf{h}_1^\dagger \mathbf{H}_4^\dagger \mathbf{w}|^2 + \Theta_5}{\|\mathbf{h}_1\|}})$, $\Theta_1 = \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2$, $\Theta_2 = \frac{P_s d_6^\tau}{d_2^\tau} |h_2|^2$, $\Theta_3 = d_6^\tau N_0$, $\Theta_4 = \frac{P_s d_4^\tau}{d_1^\tau} \|\mathbf{h}_1\|^2$, $\Theta_5 = d_4^\tau N_0$, and $\Theta_6 = \frac{P_r}{d_4^\tau N_0} \|\mathbf{H}_4 \frac{\mathbf{h}_5^\dagger}{\|\mathbf{h}_5\|}\|^2$. It is easy to observe that the maximum value of $f(\mathbf{w})$ equals to $f_{\max}(\mathbf{w}) = \min(\Theta_1 + \frac{\Theta_2}{\Theta_3}, \frac{\Theta_4}{\Theta_5})$, which can be achieved when $\mathbf{w} = \mathbf{0}$. Then we have the following important observation:

Lemma 1: The optimal transmit beamformer that minimizes $f(\mathbf{w})$ can be expressed as

$$\mathbf{w}_{\text{opt}} = \sqrt{x} \frac{\Pi_{\mathbf{h}_6^\dagger} \mathbf{H}_4 \mathbf{h}_1}{\|\Pi_{\mathbf{h}_6^\dagger} \mathbf{H}_4 \mathbf{h}_1\|} + \sqrt{P - x} \frac{\Pi_{\mathbf{h}_6^\dagger}^\perp \mathbf{H}_4 \mathbf{h}_1}{\|\Pi_{\mathbf{h}_6^\dagger}^\perp \mathbf{H}_4 \mathbf{h}_1\|}, \tag{3}$$

with $0 \leq x \leq P$. *Proof:* The proof of Lemma 1 can be referred to [8].

Substituting \mathbf{w}_{opt} into $f(\mathbf{w})$, and define $g(x) = \min(\Theta_1 +$

$\frac{\Theta_2}{x\|\mathbf{h}_6\|^2+\Theta_3}, \frac{\Theta_4}{(\sqrt{x}\frac{\|\Pi_{\mathbf{h}_6^\dagger}\mathbf{H}_4\mathbf{h}_1\|}{\|\mathbf{h}_1\|} + \sqrt{P-x}\frac{\|\Pi_{\mathbf{h}_6^\dagger}\mathbf{H}_4\mathbf{h}_1\|}{\|\mathbf{h}_1\|})^2+\Theta_5})$. It is easy to show that the minimum value of $g(x)$

can be achieved when $x = P$ or $x = \frac{\|\Pi_{\mathbf{h}_6^\dagger}\mathbf{H}_4\mathbf{h}_1\|^2}{\|\mathbf{H}_4\mathbf{h}_1\|^2}P$, and we have $f_{\min}(\mathbf{w}) = \min(\Theta_1 + \frac{\Theta_2}{P\|\mathbf{h}_6\|^2+\Theta_3}, \frac{\Theta_4}{P\frac{\|\mathbf{H}_4\mathbf{h}_1\|^2}{\|\mathbf{h}_1\|^2}+\Theta_5})$.

We now consider three separate cases:

- 1) If $\Theta_6 > f_{\max}(\mathbf{w})$, i.e., the eavesdropping channel is sufficiently good that E is able to decode the information successfully without any help. As such, it is better for E to eavesdrop rather than to jam, i.e., $\mathbf{w} = \mathbf{0}$. Therefore, the corresponding eavesdropping rate is $\frac{1}{2} \log(1 + f_{\max}(\mathbf{w}))$.
- 2) If $\Theta_6 < f_{\min}(\mathbf{w})$, i.e., the eavesdropping channel is too weak that even jamming with full-power is insufficient, thus there is no need to waste jamming power. Therefore, we set $\mathbf{w} = \mathbf{0}$, the resulting eavesdropping rate is 0.
- 3) Otherwise, since $f(\mathbf{w})$ is a continuous function of \mathbf{w} , there exists \mathbf{w} satisfying $f(\mathbf{w}) = \Theta_6$. As such, the corresponding eavesdropping rate is $\frac{1}{2} \log(1 + \Theta_6)$, where the optimal \mathbf{w} can be obtained with the help of semidefinite programming (SDP) technique [9]. Specifically, let $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$ and ignore the rank-one constraint, \mathbf{W} can be found by

$$\begin{aligned}
 \text{(P3)} \quad & \min_{\mathbf{W}} \quad 0 & (4) \\
 \text{s.t.} \quad & \text{tr}(\mathbf{W}\mathbf{h}_6^\dagger\mathbf{h}_6) = \frac{\Theta_2}{\Theta_6 - \Theta_1} - \Theta_3, \\
 & \text{tr}(\mathbf{W}\mathbf{H}_4\mathbf{h}_1\mathbf{h}_1^\dagger\mathbf{H}_4^\dagger) \leq \|\mathbf{h}_1\|^2\left(\frac{\Theta_4}{\Theta_6} - \Theta_5\right), \\
 & \text{tr}(\mathbf{W}) \leq P, \quad \mathbf{W} \succeq \mathbf{0},
 \end{aligned}$$

or

$$\begin{aligned}
\text{(P4)} \quad & \min_{\mathbf{W}} \quad 0 & (5) \\
\text{s.t.} \quad & \text{tr}(\mathbf{W}\mathbf{H}_4\mathbf{h}_1\mathbf{h}_1^\dagger\mathbf{H}_4^\dagger) = \|\mathbf{h}_1\|^2\left(\frac{\Theta_4}{\Theta_6} - \Theta_5\right), \\
& \text{tr}(\mathbf{W}\mathbf{h}_6^\dagger\mathbf{h}_6) \leq \frac{\Theta_2}{\Theta_6 - \Theta_1} - \Theta_3, \\
& \text{tr}(\mathbf{W}) \leq P, \quad \mathbf{W} \succeq \mathbf{0}.
\end{aligned}$$

Note that at least one of the optimization problems is feasible and the convex SDP problem can be efficiently solved using the CVX tools [9]. Due to the fact that the optimal solution may have a rank higher than one, we need to use some approximation approaches such as randomization to find the approximate beamforming vectors [10].

B. Strategy II: Eavesdropping First

In this subsection, we provide the optimal transmit power solution of problem (P1).

If $\text{SNR}_r^* \leq \text{SNR}_e^*$, E can always successfully decode the suspicious message. Hence, the effective eavesdropping rate is determined by the maximum achievable rate of the suspicious link. Since the achievable rate of the dual-hop suspicious link is limited by the rate of the weakest hop, E may act as a helper to improve the SNR of the second hop if it is inferior to the SNR of the first hop. Depending on the effective SNRs of the two hop channels, we consider three different cases:

1) If $\frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2 \leq \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2$, the effective SNR of the second hop without help from E is larger than that of the first hop, then E can remain silent, i.e., $P_e = 0$, and the corresponding eavesdropping rate is $\frac{1}{2} \log\left(1 + \frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2\right)$.

2) If $\frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2 \geq \frac{1}{N_0} \left(\sqrt{\frac{P_r}{d_5^\tau}} \|\mathbf{h}_5\| + \sqrt{\frac{P}{d_6^\tau}} \|\mathbf{h}_6\|\right)^2 + \frac{P_s}{d_2^\tau N_0} |h_2|^2$, the effective SNR of the second hop is too weak that E should help with maximum transmit power P , and the eavesdropping rate is $\frac{1}{2} \log\left(1 + \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{1}{N_0} \left(\sqrt{\frac{P_r}{d_5^\tau}} \|\mathbf{h}_5\| + \sqrt{\frac{P}{d_6^\tau}} \|\mathbf{h}_6\|\right)^2\right)$.

3) Otherwise, E can adjust its transmit power to maintain $\Gamma_r^{\text{EH}} = \Gamma_d^{\text{EH}}$, i.e., $P_e = \frac{d_6^\tau}{\|\mathbf{h}_6\|^2} \left(\sqrt{\frac{P_s}{d_1^\tau}} \|\mathbf{h}_1\|^2 - \frac{P_s}{d_2^\tau} |h_2|^2 - \sqrt{\frac{P_r}{d_5^\tau}} \|\mathbf{h}_5\|\right)^2$, and the corresponding eavesdropping rate is $\frac{1}{2} \log\left(1 + \frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2\right)$.

If $\text{SNR}_r^* > \text{SNR}_e^*$, E is not guaranteed to decode the suspicious information successfully in the first phase, thus E can act as an eavesdropper or a jammer in the second phase. Three cases are

studied:

1) If $\frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2 \geq \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2$, the effective SNR of the eavesdropping channel is larger than that of the second hop channel, then E can always successfully decode the suspicious information. Therefore, E can remain silent in the second phase, and the corresponding eavesdropping rate is $\frac{1}{2} \log(1 + \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2)$.

2) If $\frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2 < \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r d_6^\tau \|\mathbf{h}_5\|^2}{P d_5^\tau \|\mathbf{h}_6\|^2 + d_5^\tau d_6^\tau N_0}$, the effective SNR of the eavesdropping channel is too weak such that even full-power jamming does not work, E has no choice but to eavesdrop again to enhance the eavesdropping performance. Thus, the eavesdropping rate is $\frac{1}{2} \log(1 + \min(\frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2, \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2))$ when $\Gamma_e^{\text{EE}} \geq \min(\Gamma_r^{\text{EE}}, \Gamma_d^{\text{EE}})$, otherwise the eavesdropping rate is 0.

3) Otherwise, E can select to perform eavesdropping or jamming to ensure the success of decoding. Since $\frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2 > \frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2$ and $\frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2 > \frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2$, which indicates that eavesdropping provides a higher rate, we propose to use E as an eavesdropper if $\Gamma_e^{\text{EE}} \geq \min(\Gamma_r^{\text{EE}}, \Gamma_d^{\text{EE}})$, and the corresponding eavesdropping rate is $\frac{1}{2} \log(1 + \min(\frac{P_s}{d_1^\tau N_0} \|\mathbf{h}_1\|^2, \frac{P_s}{d_2^\tau N_0} |h_2|^2 + \frac{P_r}{d_5^\tau N_0} \|\mathbf{h}_5\|^2))$. If $\Gamma_e^{\text{EE}} < \min(\Gamma_r^{\text{EE}}, \Gamma_d^{\text{EE}})$, E can adjust its jamming power to maintain $\Gamma_e^{\text{EJ}} = \Gamma_d^{\text{EJ}}$, i.e., $P_e = \frac{d_6^\tau N_0}{d_5^\tau \|\mathbf{h}_6\|^2} (\frac{P_r d_2^\tau d_3^\tau \|\mathbf{h}_5\|^2}{P_s d_2^\tau \|\mathbf{h}_3\|^2 - P_s d_3^\tau |h_2|^2} - d_5^\tau)$, and the resulting eavesdropping rate is $\frac{1}{2} \log(1 + \frac{P_s}{d_3^\tau N_0} \|\mathbf{h}_3\|^2)$.

V. NUMERICAL RESULTS

In this section, we present numerical results to evaluate the performance of the proposed proactive strategies. Unless otherwise specify, we set the carrier frequency as 5 GHz, the bandwidth as 20 MHz, the noise power density as -174 dBm/Hz, and the transmit power of S and R as $P_s = P_r = 40$ dBm. The path-loss exponent is $\tau = 3$, and the numbers of the antennas at R and E are $N = M = 4$. The four nodes are located in a 2-D topology, where S, R, D, and E are located at (0, 0) km, (2, 0) km, (4, 0) km, and (2, 3) km, respectively.

Fig. 2 depicts the achievable eavesdropping rate of different strategies. For comparison, the performance of two heuristic benchmark schemes are also plotted, namely, eavesdropping-then-jamming and eavesdropping-then-eavesdropping. As expected, strategy II always outperforms the two reference schemes, since it adaptively adjusts the action of the legitimate monitor to enhance the eavesdropping rate of the system. However, the performance difference of strategy I and II

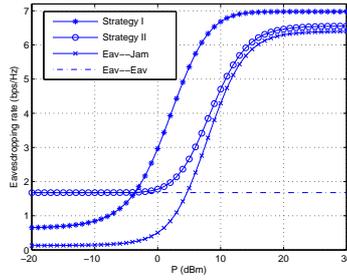


Fig. 2. Eavesdropping rate comparison of the two strategies and other benchmark schemes.

depends heavily on the network topology and operating parameters. In the current setup, strategy I is inferior in the low jamming power regime, while becomes superior when there is sufficient available jamming power.

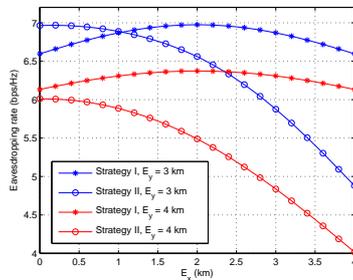


Fig. 3. Eavesdropping rate versus different positions of the legitimate monitor with $P = 40$ dBm.

In Fig. 3, we plot the eavesdropping rate as a function of the legitimate monitor's location for the two strategies where the y-coordinate (E_y) of E is fixed as 3 km or 4 km, while the x-coordinate (E_x) of E varies within the range of $[0,4]$ km. We observe that when E moves away from S, the eavesdropping rate of strategy II monotonically decreases. This is intuitive since the eavesdropping performance degrades when the distance between E and S increases. In contrast, there is an optimum position for E when adopting strategy I, i.e., the point that is most close to R. This reason is that when E is near R, it can perform jamming and eavesdropping efficiently. Therefore, as a simple criterion, E employs strategy II when it is close to S, and employs strategy I when it is close to R.

VI. CONCLUSION

This paper considered the issue of legitimate surveillance in a dual-hop DF relaying system. Specifically, two strategies aiming at maximizing the effective eavesdropping rate have been proposed, and the corresponding optimal beamformer and power allocation scheme have been obtained. It was shown that the proposed strategies significantly outperform other benchmark schemes. Moreover, the position of the legitimate monitor can be used as a simple criterion to determine the appropriate strategy.

REFERENCES

- [1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
- [2] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," to appear in *IEEE Access*.
- [3] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.
- [4] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," in *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
- [5] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," submitted to *IEEE Trans. Wireless Commun.*, 2017.
- [6] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.
- [7] A. A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.
- [8] J. Y. Ryu, J. Lee, and T. Q. Quek, "Trust degree based beamforming for MISO cooperative communication system," *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 1957–1960, Nov. 2015.
- [9] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [10] N. D. Sidiropoulos, T. N. Davidson, and Z. Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, June 2006.