Secure Communication in Multiple Relay Networks Through Decode-and-Forward Strategies

Raef Bassily and Sennur Ulukus

Abstract: **In this paper, we study the role of cooperative relays to provide and improve secure communication rates through decode-and-forward (DF) strategies in a full-duplex multiple relay network with an eavesdropper. We consider the DF scheme as a basis for cooperation and propose several strategies that implement different versions of this scheme suited for cooperation with multiple relays. Our goal is to give an efficient cooperation paradigm based on the DF scheme to provide and improve secrecy in a multiple relay network. We first study the DF strategy for secrecy in a single relay network. We propose a suboptimal DF with zero forcing (DF/ZF) strategy for which we obtain the optimal power control policy. Next, we consider the multiple relay problem. We propose three different strategies based on DF/ZF and obtain their achievable secrecy rates. The first strategy is a single hop strategy whereas the other two strategies are multiple hop strategies. In the first strategy, we show that it is possible to eliminate all the relays' signals from the eavesdropper's observation (full ZF), however, the achievable secrecy rate is limited by the worst source-relay channel. Our second strategy overcomes the drawback of the first strategy, however, with the disadvantage of enabling partial ZF only. Our third strategy provides a reasonable compromise between the first two strategies. That is, in this strategy, full ZF is possible and the rate achieved does not suffer from the drawback of the first strategy. We conclude our study by a set of numerical results to illustrate the performance of each of the proposed strategies in terms of the achievable rates in different practical scenarios.**

Index Terms: **Decode-and-forward (DF) scheme, information theoretic security, multiple hop strategies, relay networks, secrecy rate.**

I. INTRODUCTION

Recently, there has been considerable attention devoted to the role of cooperation in wireless networks to improve the achievable secrecy rates. In the context of secrecy, there have been two main types of cooperating relays considered in the literature. The first type is the untrusted relay where the relay helps improve the communication between the source and the destination while the relay itself is regarded as an eavesdropper from which the source message has to be concealed. This model has been considered in several papers, e.g., [1], [2], [3], and [4]. The second type, which we consider in this paper, is the trusted relay where the is no security requirement imposed against the relay whereas there is an external eavesdropper from which the source message has to be concealed. Henceforth, whenever we mention a cooperating relay, we will be referring to a trusted relay.

In general, one can distinguish between two modes of cooperation via a trusted relay in the context of secrecy. The first mode is an active mode of cooperation in which a relay listens to the source transmissions and uses its observation to improve the achievable secrecy rate. This mode is based on the well-known strategies, e.g., decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF) strategies, devised originally for cooperative models with no secrecy constraints. Reference [5] was the first to introduce the basic relay channel without secrecy constraints where most of these strategies were first proposed. In [6], the basic relay-eavesdropper channel was introduced and achievable secrecy rates were obtained based on extended versions of these strategies as well as new strategies that fit the secrecy model. The second mode of cooperation for secrecy is a passive mode in which the relay transmits a signal that is independent of the source message in order to confuse the eavesdropper and hence improve the achievable secrecy rate; see [7]. This mode is usually referred to as deaf cooperation. There have been several schemes for deaf cooperation proposed in the literature, for example, deaf cooperation using Gaussian noise [8], [9], and [10], deaf cooperation using Gaussian codebooks [6], and deaf cooperation using structured codes [11]. There are two schemes of deaf cooperation based on Gaussian signaling. In the first scheme [8], [9], and [10], a helping interferer transmits white Gaussian noise when it is closer to the eavesdropper than it is to the legitimate receiver. This scheme is usually referred to as cooperative jamming with Gaussian noise. For brevity, we will henceforth refer to this scheme as the cooperative jamming (CJ) scheme.[1] The second scheme of deaf cooperation based on Gaussian signaling is usually referred to as noise forwarding (NF) and is first introduced in [6]. In a NF scheme, the relay transmits a dummy Gaussian codeword that is independent from the source message to introduce helpful interference that would hurt the eavesdropper more than the legitimate receiver. Recently, reference [12] has proposed a scheme that combines the novel technique of noisy network coding [13] with a deaf cooperation scheme to improve over the secrecy rate achievable by deaf cooperation only.

In multiple relay networks, the roles of active and passive (deaf) modes of cooperation have been investigated in some recent works. For deaf cooperation with Gaussian signaling, the

Manuscript received January 30, 2012.

This work was supported by NSF Gants CCF 07-29127, CNS 09-64632, CCF 09-64645, CCF 10-18185, and CNS 11-47811.

R. Bassily is with the Department of Computer Science and Engineering, Pennsylvania State University, University Park , PA 16802, USA, email: bassily@umd.edu.

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, email: ulukus@umd.edu.

[1] We stress that the notion of cooperative jamming can be understood in general as a class of deaf cooperation schemes that aim at improving the achievable secrecy rate by creating less favorable conditions at the eavesdropper than those at the legitimate receiver. This class includes, as a special case, cooperative jamming with Gaussian noise.

role of CJ is studied in several papers, e.g., [14], [15], and [16]. The role of combined CJ and NF is studied in [17]. On the other hand, the role of active cooperation of beamforming relays in improving secrecy is investigated in [18] and [19]. In both [18] and [19], a two-stage cooperative secrecy protocol is proposed in which a set of multiple relays decode the source's message in the first stage, then the relays forward the source's message to the destination using beamforming. Reference [18] proposes an iterative strategy, when the global channel state information (CSI) is perfectly available, to design the beamforming coefficients either to maximize the secrecy rate for a fixed transmit power or to minimize the transmit power for a fixed secrecy rate. The same reference proposes a suboptimal zero-forcing (ZF) strategy in which an additional constraint of canceling out the signals from the eavesdropper's observation is imposed. In [19], the problem of maximizing the secrecy rate achieved by the collaborative beamforming of the relays when the global CSI is perfectly available is investigated under both total and individual relay power constraints where a closed-form solution is obtained in the first case and a numerical solution is devised for the second case. The work in [18] and [19] appears to be closely related to the beamforming strategy presented in this paper. However, there is a major difference between their model and the model presented here. In particular, both [18] and [19] assume that the communication occurs in two stages where in the first stage (source to relays) neither the destination nor the eavesdropper can hear the source and hence no secrecy requirement is involved in this stage, whereas in the second stage only the relays (but not the source) send the source's message by beamforming to the destination and hence their model becomes similar to a MISO wiretap channel [20], [21], [22], [23]. This assumption is not made in the work presented in this paper. In particular, any node in the system can hear any other transmitting node (s) at any time during the message is being communicated.

In this paper, we study the DF scheme in the secrecy context and propose DF-based strategies for secrecy in multiple relay networks. First, we consider the single relay problem. The problem of maximizing the achievable secrecy rate under individual average power constraints at the source and the relay is, in general, analytically intractable. Hence, we propose a suboptimal DF with ZF (DF/ZF) strategy for which we obtain the optimal power control policy. Next, we consider the multiple relay problem. We propose three different strategies based on DF/ZF and obtain the achievable secrecy rate by each of them. In the first strategy, all the relays decode the source message at the same time, then perform beamforming by transmitting scaled versions of the same signal to the destination, i.e., in this strategy each message block is transmitted to the destination in a single hop.[2] Moreover, we show that all the relays' signal components can be eliminated from the eavesdropper's observation, i.e., *full* ZF can be achieved. Although this strategy is simple and allows for full ZF, it has an obvious drawback. That is, the relays which are far from the source could possibly create a bottleneck that limits the achievable rate. To overcome this drawback, we propose another strategy that is based on the one in [24] (see also [25]) for the case with no secrecy constraints. In this strategy, the relays are ordered with respect to their distance from the source and they perform DF in a multi-hop fashion, i.e., the closest relay decodes the source message first, forwards it (with the help of the source) to the second closest relay and so forth till it reaches the destination. Thus, if the total number of the relays is T, then the transmission of each message block is done in T hops. We show that this strategy overcomes the bottleneck drawback of the first strategy. However, given that all the relays transmit fresh information in every transmission block, it is shown that only half of the relays' signal components can be forced to zero in the eavesdropper's observation. That is, only *partial* ZF is possible in the second strategy. We observe that to achieve full ZF in the second strategy, we need to set half of the relays' signal components (that represent the fresh information transmitted by these relays in a given transmission block) to zero. Based on this observation, we propose a $T/2$-hop strategy that, to some extent, combines the advantages of the two aforementioned strategies in an efficient way. That is, the achievable rate is not limited by the worst source-relay channel as in the first strategy, yet we can eliminate all the relays' signals from the eavesdropper's observation. In this strategy, the relays are ordered with respect to their distance from the source and then grouped into clusters of two relays per cluster. The source transmits the message to the relays in the first cluster (closest to the source) which decode the message and forward it (with the help of the source) to the relays in the second cluster and so on so forth till the message is forwarded to the destination. The relays in each clusters are not assumed to have any kind of direct communication among them. We show that by properly adjusting the signal coefficients at the relays, we can zero-force all the relays' signals at the eavesdropper. Hence, in typical situations, this strategy provides a reasonable compromise between the first two strategies.

Finally, we give numerical results to compare the performance of the proposed strategies in terms of the achievable rates when a constant power allocation is used at all the relays. Our results show that the second (multi-hop) strategy yields higher rates than the first (single-hop) strategy when the variation in the distance between the source and each relay is large whereas the first strategy yields higher rates when such variation is small, i.e., when the relays are at about the same distance from the source. Our simulation results also show that in a typical situation where each relay has a close neighbor relay, the third strategy outperforms the first two strategies.

II. DECODE-AND-FORWARD WITH A SINGLE RELAY

We consider the Gaussian relay-eavesdropper channel consisting of a source (node 0), a relay (node 1), a destination (node 2), and an eavesdropper (node 3); see Fig. 1. Without loss of generality, one can normalize the channel gains from the source and the relay to the destination by proper scaling of the power constraints at the source and the relay. Hence, the outputs at the relay, the destination, and the eavesdropper are, respectively, given by

$$Y_1 = h_{01}X_0 + N_1 \tag{1}$$

[2]Here, we define the number of hops as the number of transmission blocks required for all the relays to decode a single block of the source's message.

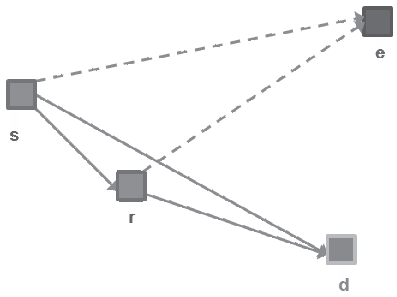

Fig. 1. A single relay network with an eavesdropper.

$$Y_2 = X_0 + X_1 + N_2 \tag{2}$$
$$Y_3 = h_{03}X_0 + h_{13}X_1 + N_3 \tag{3}$$

where $h_{k\ell}$ denotes the complex channel gain from node k to node ℓ, $k \in \{0,1\}$ and $\ell \in \{1,3\}$, X_k denotes the channel input at node $k \in \{0,1\}$, and N_ℓ denotes the Gaussian noise at node $\ell \in \{1,2,3\}$ which is circularly symmetric complex Gaussian random variable with zero mean and unit variance. We assume that all nodes have perfect knowledge of all the channel gains. The average power constraints at the source and the relay are given by

$$E[|X_0|^2] \triangleq P_0 \le \bar{P}_0, \text{ and } E[|X_1|^2] \triangleq P_1 \le \bar{P}_1. \tag{4}$$

We confine our attention to the DF scheme which is given in its original setting without secrecy constraints in [5] and [26] and extended in the secrecy context in [6]. The achievable secrecy rate using the DF scheme R^{DF} for any discrete memoryless relay-eavesdropper channel given by some conditional distribution $p(y_1, y_2, y_3|x_0, x_1)$ and for some input distribution $p(x_0, x_1)$ is given by (see [6])

$$R^{DF} = \min\{I(X_0; Y_1|X_1), I(X_0, X_1; Y_2)\} - I(X_0, X_1; Y_3). \tag{5}$$

For the Gaussian channel given by (1)–(3) above, as proposed in [5] as well as in [6], we choose X_0 and X_1 to be circularly symmetric Gaussian random variables with zero mean and variances P_0 and P_1, respectively. Moreover, X_0 and X_1 are related as $X_0 = \tilde{X}_0 + \alpha_0 X_1$ where α_0 is some complex number to be determined later, $\tilde{X}_0$ is circularly symmetric Gaussian random variable with zero mean and variance $\tilde{P}_0$, and $\tilde{X}_0$ is independent of X_1. Hence, X_0 and X_1 are arbitrarily correlated and their covariance depends on the value of α_0. Moreover, from the average power constraints (4), we must have

$$\tilde{P}_0 + |\alpha_0|^2 P_1 \le \bar{P}_0, \text{ and } P_1 \le \bar{P}_1. \tag{6}$$

It follows that the achievable secrecy rate by the DF strategy for such channel is given by

$$R^{DF} = \min\left\{ \log\left(\frac{1+|h_{01}|^2\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1}\right), \log\left(\frac{1+\tilde{P}_0+|\alpha_0+1|^2 P_1}{1+|h_{03}|^2\tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1}\right)\right\} \tag{7}$$

where α_0, $\tilde{P}_0$, and P_1 must satisfy (6). On the other hand, the secrecy capacity of the original Gaussian wiretap channel without a relay is given by

$$C^{\text{GWT}} = \left(\log\left(\frac{1+\bar{P}_0}{1+|h_{03}|^2\bar{P}_0}\right)\right)^+ \tag{8}$$

where for $x \in \mathbb{R}$, $(x)^+ = \max(0, x)$. For the DF strategy to achieve strictly larger secrecy rate than the secrecy capacity of the original Gaussian wiretap channel C^{GWT}, it is clear from (7) and (8) that we must have $|h_{01}| > \max\{1, |h_{03}|\}$. In other words, a necessary condition for the DF strategy to be useful is to have $|h_{01}| > \max\{1, |h_{03}|\}$.

The problem of finding the optimal power control policy (including finding the optimal value of α_0) is in general analytically intractable and closed form solution could not be obtained. However, we present here a suboptimal strategy for which we analytically derive the optimal power control policy. Here, we can only zero-force the relay signal X_1 but not the independent component of the source signal $\tilde{X}_0$. In particular, we set $\alpha_0 = \alpha^{\text{ZF}} \triangleq -h_{13}/h_{03}$. We denote the achievable rate in this case as $R^{\text{DF/ZF}}$ which, as a function of $(\tilde{P}_0, P_1)$, is given by

$$R^{\text{DF/ZF}} = \min\left\{ \log\left(\frac{1+|h_{01}|^2\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+|\alpha^{\text{ZF}}+1|^2 P_1}{1+|h_{03}|^2\tilde{P}_0}\right)\right\} \tag{9}$$

In the following theorem, we give the optimal power control policy $(\tilde{P}_0^\star, P_1^\star)$ that maximizes $R^{\text{DF/ZF}}$. This theorem is proved in Appendix A.

Theorem 1 *If $|h_{01}| \le \max\{1, |h_{03}|\}$, then the optimal power control policy that maximizes $R^{\text{DF/ZF}}$ is given by $\tilde{P}_0^\star = P_1^\star = 0$ when $|h_{01}| \le |h_{03}|$, whereas by $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$ when $|h_{01}| > |h_{03}|$. In this case, the DF/ZF strategy (and even the general DF strategy) becomes useless since the optimal achievable rate is equal to the secrecy capacity of the original Gaussian wiretap channel without a relay node. On the other hand, if $|h_{01}| > \max\{1, |h_{03}|\}$, then the optimal power control policy that maximizes $R^{\text{DF/ZF}}$ is given by the following cases*:

- *If* $\bar{P}_0 \le \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2}$ *and* $\bar{P}_1 \ge \frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}$, $\tilde{P}_0^\star = \bar{P}_0$ *and* $P_1^\star = 0$.
- *If* $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2}$ *and* $\bar{P}_1 \ge \frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}$, $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{\text{ZF}}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\bar{P}_0$ *and* $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\text{ZF}}|^2}$.
- *If* $\bar{P}_0 \le \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2}$ *and* $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}$, $\tilde{P}_0^\star = \bar{P}_0$ *and* $P_1^\star = 0$.
- *If* $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2}$ *and* $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}$, *we have the following subcases*:
  - *If* $\bar{P}_1 \le \min\left\{\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{\text{ZF}}|^2}, \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}\right\}$, $\tilde{P}_0^\star = \bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$ *and* $P_1^\star = \bar{P}_1$.

– *If* $\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{\text{ZF}}|^2} < \bar{P}_1 \leq \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\frac{\bar{P}_0}{|\alpha^{\text{ZF}}|^2}$, $\tilde{P}_0^\star = \frac{|1+\alpha^{\text{ZF}}|^2}{|h_{01}|^2-1}\bar{P}_1$ *and* $P_1^\star = \bar{P}_1$.

– *Otherwise,* $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{\text{ZF}}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\bar{P}_0$ *and* $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\text{ZF}}|^2}$.

Moreover, in cases 1 *and* 3 *above, the DF/ZF strategy is useless, i.e., it can only achieve rates as high as the secrecy capacity of the original Gaussian wiretap channel with no relay, whereas in cases* 2 *and* 4*, the DF/ZF strategy achieves a strictly larger rate than the secrecy capacity of the original Gaussian wiretap channel.*

The following corollary is a direct consequence of the above theorem.

Corollary 1 *If at least one of the following two conditions is true, then the DF/ZF strategy is useful, i.e., it achieves a higher secrecy rate than the secrecy capacity of the original Gaussian wiretap channel without a relay*:

1. $|h_{01}| > |h_{03}| > 1$.
2. $|h_{01}| > 1 > |h_{03}|$ *and* $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2}$.

III. DECODE-AND-FORWARD WITH MULTIPLE RELAYS

Let $\mathcal{T} = \{1, \cdots, T\}$ denote the set of relays. Let the source be denoted as node 0, the destination as node $T+1$, and the eavesdropper as node $T+2$. The outputs at the relays, the destination, and the eavesdropper are given by

$$Y_i = h_{0i}X_0 + \sum_{j\in\mathcal{T}\setminus\{i\}} h_{ji}X_j + N_i,\ i \in \mathcal{T} \tag{10}$$

$$Y_{T+1} = X_0 + \sum_{i\in\mathcal{T}} X_i + N_{T+1} \tag{11}$$

$$Y_{T+2} = h_{0,T+2}X_0 + \sum_{i\in\mathcal{T}} h_{i,T+2}X_i + N_{T+2} \tag{12}$$

where, for $i,\ j \in \{0, 1, \cdots, T+2\}$, h_{ij} is the complex channel gain from node i to node j, X_i is the channel input at node i, and N_i is the complex circularly symmetric zero mean unit variance Gaussian noise at node i. We assume perfect knowledge of all channel gains at all the nodes. The average power constraints are given by

$$E[|X_0|^2] \triangleq P_0 \leq \bar{P}_0 \quad \text{and} \quad E[|X_i|^2] \triangleq P_i \leq \bar{P}_r,\ i \in \mathcal{T} \tag{13}$$

where we assume that all the relays have equal power constraints for simplicity.

A. Multiple Relay Single Hop DF (MRSH-DF) Strategy

In this strategy, all the relays decode the source message at a given block at the same time and forward it to the destination; see Fig. 2. In the case of the general discrete memoryless multiple relay channel given by some conditional distribution $p(y_1, \cdots, y_{T+1}, y_{T+2}|x_0, \cdots, x_T)$, the DF scheme of [6] can be extended to obtain an analogous scheme for the multiple relay case. It is not difficult to see that the achievable secrecy rate R^{DF} by such scheme is given by

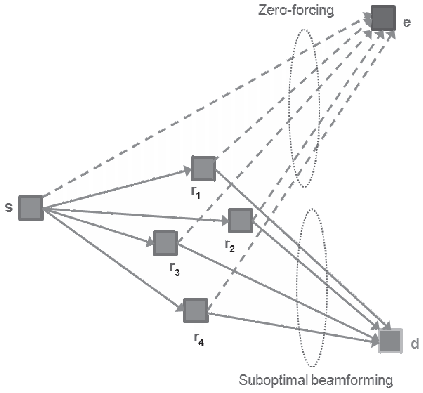

Fig. 2. Multiple relay single hop strategy for a multiple relay network with an eavesdropper.

$$R^{\text{DF}} = \min\left\{\min_{i\in\mathcal{T}}\{I(X_0;Y_i|X_r)\}, I(X_0,X_r;Y_{T+1})\right\} - I(X_0,X_r;Y_{T+2}) \tag{14}$$

for some auxiliary random variable X_r where $p(x_r, x_0, \cdots, x_T)$ factors as $p(x_0|x_r)p(x_r)\prod_{j=1}^{T} p(x_j|x_r)$. For the Gaussian channel, our strategy requires that all the relays perform signal beamforming as they forward the source message to the destination. In particular, we choose $X_0 = \tilde{X}_0 + \alpha_0 X_r$ and $X_i = \alpha_i X_r,\ i \in \mathcal{T}$ where $\tilde{X}_0,\ X_r$ are independent circularly symmetric complex Gaussian random variables with zero mean and variances $\tilde{P}_0$ and P_r, respectively, and $\alpha_0, \alpha_i,\ i \in \mathcal{T}$ are some complex numbers. From (13), we must have

$$\tilde{P}_0 + |\alpha_0|^2 P_r \leq \bar{P}_0 \ \text{ and } \ |\alpha_i|^2 P_r \leq \bar{P}_r,\ i \in \mathcal{T} \tag{15}$$

Consequently, the achievable secrecy rate R^{DF} is given by (16) at the top of the next page. It is clear that a necessary condition for this strategy to be useful is to have $\min_{i\in\mathcal{T}}|h_{0,i}| > \max\{1, |h_{0,T+2}|\}$. Again, finding the optimal values for $\tilde{P}_0, P_r$, and $\alpha_i,\ i \in \mathcal{T}\cup\{0\}$ is analytically intractable. As in the previous section, we propose a suboptimal strategy in which α_0 is chosen to force the term of the eavesdropper's observation that depends on X_r to zero. This goal can be attained for any values of $\alpha_j,\ j \in \mathcal{T}$, by choosing $\alpha_0 = \alpha^{\text{ZF}} \triangleq -\frac{\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}}{h_{0,T+2}}$. Hence, the achievable rate becomes

$$R^{\text{DF/ZF}} = \min\left\{\log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+|\sum_{j\in\mathcal{T}}\alpha_j\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)|^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\} \tag{17}$$

where $i^\star = \arg\min_{i\in\mathcal{T}}|h_{0i}|$. However, the problem of maximizing (17) under the constraints $\tilde{P}_0 + |\alpha^{\text{ZF}}|^2 P_r \leq \bar{P}_0$ and $|\alpha_j|^2 P_r \leq \bar{P}_r,\ j \in \mathcal{T}$ is still intractable since α^{ZF} (and hence the first constraint) depends on $\alpha_j,\ j \in \mathcal{T}$ and is not merely a constant as in the previous section. Thus, we resort to

$$R^{\mathrm{DF}} = \min\left\{ \min_{i\in\mathcal{T}} \log\left(\frac{1+|h_{0i}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0+|\alpha_0 h_{0,T+2}+\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}|^2 P_r}\right), \right.$$
$$\left. \log\left(\frac{1+\tilde{P}_0+|\alpha_0+\sum_{j\in\mathcal{T}}\alpha_j|^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0+|\alpha_0 h_{0,T+2}+\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}|^2 P_r}\right)\right\} \tag{16}$$

a suboptimal procedure to obtain a tractable solution. Specifically, we first find a set of suboptimal beamforming coefficients $\alpha_j,\ j\in\{\mathcal{T}\}$, then, for this choice of coefficients, we maximize the achievable rate under the corresponding set of constraints. In particular, we ignore the constraint $\tilde{P}_0+|\alpha^{\mathrm{ZF}}|^2P_r\le\bar{P}_0$, assume $\tilde{P}_0$ to be fixed, and find $\alpha_j,\ j\in\mathcal{T}$ that maximize (17) for every P_r that satisfies the constraints $|\alpha_j|^2P_r\le\bar{P}_r,\ j\in\mathcal{T}$. For this set of coefficients, the problem of maximizing the achievable rate under the resulting set of constraints is tractable and can be solved in a way similar to that of the previous section.

Now, we claim that if $\tilde{P}_0$ is fixed, then, for every P_r that satisfies $|\alpha_j|^2P_r\le\bar{P}_r,\ j\in\mathcal{T}$, the rate in (17) is maximized by choosing $\alpha_j=\frac{\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)^*}{\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|},\ \forall j\in\mathcal{T}$, where a^* denotes the complex conjugate of the complex number a. To see this, we first note that, from the triangle inequality, we have $\left|\sum_{j\in\mathcal{T}}\alpha_j\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)\right|\le\sum_{j\in\mathcal{T}}|\alpha_j|\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|$. This upper bound can be attained by selecting the phase of α_j to be the negative of the phase of $\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right),\ j\in\mathcal{T}$. Hence, we can replace the objective function of (17) with

$$R^{\mathrm{DF/ZF}} = \min\left\{ \log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \right.$$
$$\left. \log\left(\frac{1+\tilde{P}_0+\left(\sum_{j\in\mathcal{T}}|\alpha_j|\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|\right)^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\}. \tag{18}$$

Define $\hat{\beta}\triangleq\max\{|\alpha_j|,\ j\in\mathcal{T}\}$, $\beta_j\triangleq\frac{\alpha_j}{\hat{\beta}},\ j\in\mathcal{T}$, and $Q_r\triangleq\hat{\beta}^2P_r$. Hence, the objective function in (18) can be written as

$$R^{\mathrm{DF/ZF}} = \min\left\{ \log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \right.$$
$$\left. \log\left(\frac{1+\tilde{P}_0+\left(\sum_{j\in\mathcal{T}}|\beta_j|\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|\right)^2 Q_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\} \tag{19}$$

where $|\beta_j|\le 1,\ j\in\mathcal{T}$, and $Q_r\le\bar{P}_r$. Finally, we note that, for every $Q_r\le\bar{P}_r$, (19) is maximized by choosing $|\beta_j|=1\ \forall j\in\mathcal{T}$.

Thus, the achievable rate by this set of coefficients $\alpha_j,\ j\in\mathcal{T}$ is given by

$$R^{\mathrm{DF/ZF}} = \min\left\{ \log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \right.$$
$$\left. \log\left(\frac{1+\tilde{P}_0+\left(\sum_{j\in\mathcal{T}}\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|\right)^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\} \tag{20}$$

where $\tilde{P}_0$ and P_r satisfy

$$\tilde{P}_0+|\alpha^{\mathrm{ZF}}|^2P_r\le\bar{P}_0,\ \ P_r\le\bar{P}_r \tag{21}$$

and $\alpha^{\mathrm{ZF}}=-\sum_{j\in\mathcal{T}}\frac{h_{j,T+2}}{h_{0,T+2}}\frac{\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)^*}{|1-\frac{h_{j,T+2}}{h_{0,T+2}}|}$. Indeed from the similarity between (20) and (9), we can easily modify Theorem 1 to obtain the optimal power control policy $(\tilde{P}_0^\star,P_r^\star)$ that maximizes (20) under constraints (21). In particular, if $|h_{0i^\star}|\le\max\{1,|h_{0,T+2}|\}$, then this strategy is useless, i.e., it can achieve at most the secrecy capacity of the original wiretap channel with no relays. On the other hand, if $|h_{0i^\star}|>\max\{1,|h_{0,T+2}|\}$, then the optimal power control policy that maximizes (20) is given by the following cases:

1. If $\bar{P}_0\le\frac{|\alpha^{\mathrm{ZF}}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{\mathrm{ZF}}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$ and $\bar{P}_r\ge\frac{\bar{P}_0}{|\alpha^{\mathrm{ZF}}|^2}$, $\tilde{P}_0^\star=\bar{P}_0$ and $P_r^\star=0$.
2. If $\bar{P}_0>\frac{|\alpha^{\mathrm{ZF}}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{\mathrm{ZF}}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$ and $\bar{P}_r\ge\frac{\bar{P}_0}{|\alpha^{\mathrm{ZF}}|^2}$, $\tilde{P}_0^\star=\frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2\bar{P}_0}{|\alpha^{\mathrm{ZF}}|^2(|h_{0i^\star}|^2-1)+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$ and $P_r^\star=\frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\mathrm{ZF}}|^2}$.
3. If $\bar{P}_0\le\frac{|\alpha^{\mathrm{ZF}}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{\mathrm{ZF}}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$ and $\bar{P}_r<\frac{\bar{P}_0}{|\alpha^{\mathrm{ZF}}|^2}$, $\tilde{P}_0^\star=\bar{P}_0$ and $P_r^\star=0$.
4. If $\bar{P}_0>\frac{|\alpha^{\mathrm{ZF}}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{\mathrm{ZF}}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$ and $\bar{P}_r<\frac{\bar{P}_0}{|\alpha^{\mathrm{ZF}}|^2}$, we have the following subcases:
   - If $\bar{P}_r\le\min\left\{\frac{1-|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2},\ \frac{|h_{0i^\star}|^2-1}{|\alpha^{\mathrm{ZF}}|^2|h_{0i^\star}|^2-|\alpha^{\mathrm{ZF}}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0\right\}$, $\tilde{P}_0^\star=\bar{P}_0-|\alpha^{\mathrm{ZF}}|^2\bar{P}_r$ and $P_r^\star=\bar{P}_r$.
   - If $\frac{1-|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}<\bar{P}_r\le\frac{|h_{0i^\star}|^2-1}{|\alpha^{\mathrm{ZF}}|^2|h_{0i^\star}|^2-|\alpha^{\mathrm{ZF}}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0$, $\tilde{P}_0^\star=\frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}{|h_{0i^\star}|^2-1}\bar{P}_r$ and $P_r^\star=\bar{P}_r$.

- Otherwise,

$$\tilde{P}_0^\star = \frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}{|\alpha^{\text{ZF}}|^2|h_{0i^\star}|^2-|\alpha^{\text{ZF}}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0 \quad \text{and}$$

$$P_r^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\text{ZF}}|^2}.$$

As in Theorem 1, cases 1 and 3 above can only achieve rates as high as the secrecy capacity of the original Gaussian wiretap channel with no relays, whereas in cases 2 and 4, the DF/ZF strategy achieves a strictly larger rate than the secrecy capacity of the original Gaussian wiretap channel.

B. Multiple Relay Multiple Hop DF (MRMH-DF) Strategy

One clear drawback of the above strategy is the requirement that all relays must decode the source message in a single hop at the same time and thus the furthest relay from the source creates a bottleneck in the achievable secrecy rate. To overcome this drawback, we propose another strategy that is based on the multi-hop DF strategy introduced in [24] for the multiple relay model without an eavesdropper. In this strategy, the relays in $\mathcal{T}$ are given a certain order. In any given transmission block b of the source message, the first relay decodes the current message block and forwards it (with the help of the source) to the second relay in the transmission block $b+1$ which decodes it and then forwards it (with the help of the source and the first relay) to the third relay in the transmission block $b+2$ and so on so forth till the last relay decodes the source message block and forwards it (with the help of the source and all the other relays) to the destination in the transmission block $b+T$. Hence, the transmission of each message block occurs over T hops before it reaches the destination; see Fig. 3. Since the multi-hop transmission is pipelined, we only have an initial delay (overhead) of T blocks before the first message block reaches the destination, however, no further delay is involved between source message blocks. Under the usual assumption that the source message is composed of sufficiently large number of blocks $B >> T$, the achievable rate loss due to such overhead is negligible. Without loss of generality, assume that the relays are ordered according to their label in $\mathcal{T}$, i.e., each relay $i \in \mathcal{T}$ is the ith relay in the multi-hop order. In the case of the general discrete memoryless multiple relay channel with external eavesdropper given by some conditional distribution $p(y_1,\cdots,y_{T+1},y_{T+2}|x_0,\cdots,x_T)$, the multi-hop DF scheme of [24] can be extended by applying stochastic encoding at the source and every relay in the usual manner to obtain an analogous secure scheme for the multiple relay with an external eavesdropper problem. By noting that the eavesdropper intercepts the signal transmitted in each of the T hops, it is not difficult to see that the achievable secrecy rate R^{DF} by such scheme for some input distribution $p(x_0,\cdots,x_T)$ is given by

$$\begin{aligned} R^{\text{DF}} = \min\Big\{ & I(X_0;Y_1|X_1,X_2,\cdots,X_T),\cdots, \\ & I(X_0,X_1,\cdots,X_i;Y_{i+1}|X_{i+1},\cdots,X_T),\cdots, \\ & I(X_0,X_1,\cdots,X_T;Y_{T+1})\Big\} \\ & -I(X_0,X_1,\cdots,X_T;Y_{T+2}). \end{aligned} \tag{22}$$

For the Gaussian channel (10)–(12), we choose the channel inputs as follows. $X_i = \tilde{X}_i + \alpha_i X_{i+1},\ i = 0,\cdots,T-1$ and $X_T = \tilde{X}_T$ where all $\tilde{X}_i,\ i = 0,\cdots,T$ are independent circularly symmetric complex Gaussian random variables with zero mean and variances $\tilde{P}_i,\ i = 0,\cdots,T$, respectively, and $\alpha_i, i = 0,\cdots,T-1$, are some complex numbers. Equivalently, we have $X_i = \tilde{X}_i + \sum_{j=i+1}^{T}\prod_{\ell=i}^{j-1}\alpha_\ell X_j,\ i = 0,\cdots,T-1$ and $X_T = \tilde{X}_T$. From (13), we must have

$$\tilde{P}_i + \sum_{j=i+1}^{T}\prod_{\ell=i}^{j-1}|\alpha_\ell|^2\tilde{P}_j \le \bar{P}_i,\ \ i\in\mathcal{T}\cup\{0\} \tag{23}$$

where $\bar{P}_i = \bar{P}_r\ \forall i \in \mathcal{T}$. Hence, the achievable rate R^{DF} is given by (24) at the top of the next page. For example, when $T=3$, the achievable rate is given by (25) at the top of the next page.

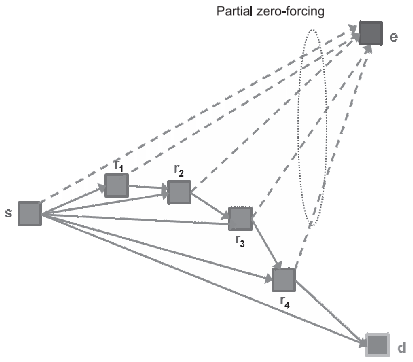

Fig. 3. Multiple relay T-hop strategy for a multiple relay network with an eavesdropper.

Recall that this rate corresponds to the aforementioned ordering of the relays. In general, there are $T!$ of such orderings each of which giving a different rate. In this strategy, we choose to order the relays according to their distances from the source, i.e., the closer the relay to the source comes first in the multi-hop order. Hence, without loss of generality, we assume that $|h_{01}| \ge |h_{02}| \ge \cdots \ge |h_{0T}|$ and hence the ordering of the relays gives the rate in (24). Clearly, a necessary condition for this DF strategy to be useful (i.e., to give a rate higher than the secrecy capacity of the original Gaussian wiretap channel) is to have $\max_{i\in\mathcal{T}}|h_{0i}| > \max\{1,|h_{0,T+2}|\}$ which shows that the relays far from the source do not necessarily limit the achievable rate as in the MRSH-DF strategy.

Clearly, in the Gaussian case, the MRSH-DF strategy is a special case of the MRMH-DF strategy when all the relays' independent signal components $\tilde{X}_i,\ i \in \mathcal{T}$ are set to zero. This makes the MRMH-DF strategy potentially better than the MRSH-DF strategy in terms of the achievable secrecy rate if appropriate power allocation is used for the source and the relays. On the other hand, finding the optimal power allocation for the MRMH-DF strategy is analytically intractable and seeking numerical solution for this problem is not a practical choice especially if the number of relays is large. Hence, as a viable practical alternative, we may want to have some guarantees on the information rate leaked to the eavesdropper by zero-forcing the relays' signals at the eavesdropper as we did in the MRSH-DF strategy. In this case, even if the relays used a simple fixed power

$$R^{\text{DF}} = \min\left\{\min_{j\in\mathcal{T}} \log\left(1+|h_{0j}|^2\tilde{P}_0+\sum_{i=1}^{j-1}|h_{ij}+\sum_{\ell=0}^{i-1}h_{\ell j}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right), \log\left(1+\tilde{P}_0+\sum_{i\in\mathcal{T}}|1+\sum_{\ell=0}^{i-1}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0+\sum_{i\in\mathcal{T}}|h_{i,T+2}+\sum_{\ell=0}^{i-1}h_{\ell,T+2}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right) \tag{24}$$

$$\begin{aligned}R^{\text{DF}} = \min\Bigg\{ &\log\left(1+|h_{01}|^2\tilde{P}_0\right), \log\left(1+|h_{02}|^2\tilde{P}_0+|h_{12}+h_{02}\alpha_0|^2\tilde{P}_1\right),\\ &\log\left(1+|h_{03}|^2\tilde{P}_0+|h_{13}+h_{03}\alpha_0|^2\tilde{P}_1+|h_{23}+h_{13}\alpha_1+h_{03}\alpha_0\alpha_1|^2\tilde{P}_2\right),\\ &\log\left(1+\tilde{P}_0+|1+\alpha_0|^2\tilde{P}_1+|1+\alpha_1+\alpha_0\alpha_1|^2\tilde{P}_2+|1+\alpha_2+\alpha_1\alpha_2+\alpha_0\alpha_1\alpha_2|^2\tilde{P}_3\right)\Bigg\}\\ -\log\big(&1+|h_{0,5}|^2\tilde{P}_0+|h_{15}+h_{05}\alpha_0|^2\tilde{P}_1+|h_{25}+h_{15}\alpha_1+h_{05}\alpha_0\alpha_1|^2\tilde{P}_2\\ &+|h_{35}+h_{25}\alpha_2+h_{15}\alpha_1\alpha_2+h_{05}\alpha_0\alpha_1\alpha_2|^2\tilde{P}_3\big)\end{aligned} \tag{25}$$

$$Y_5 = h_{05}\tilde{X}_0+(h_{15}+h_{05}\alpha_0)\tilde{X}_1+(h_{25}+(h_{15}+h_{05}\alpha_0)\,\alpha_1)\,\tilde{X}_2+(h_{35}+(h_{25}+(h_{15}+h_{05}\alpha_0)\,\alpha_1)\,\alpha_2)\,\tilde{X}_3+N_5 \tag{26}$$

$$R^{\text{DF/PZF}} = \min\left\{\min_{j\in\mathcal{T}} \log\left(1+|h_{0j}|^2\tilde{P}_0+\sum_{i=1}^{j-1}\left|h_{i,j}+\sum_{\ell=0}^{i-1}h_{\ell j}\prod_{k=\ell}^{i-1}\alpha_k\right|^2\tilde{P}_i\right), \log\left(1+\tilde{P}_0+\sum_{i\in\mathcal{T}}\left|1+\sum_{\ell=0}^{i-1}\prod_{k=\ell}^{i-1}\alpha_k\right|^2\tilde{P}_i\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0+\sum_{\text{even } i\in\mathcal{T}}\left|h_{i,T+2}+\sum_{\ell=0}^{i-1}h_{\ell,T+2}\prod_{k=\ell}^{i-1}\alpha_k\right|^2\tilde{P}_i\right) \tag{27}$$

strategy, we would guarantee that none of the relays' signals would leak to the eavesdropper. However, unlike the MRSH-DF/ZF strategy, here, we cannot eliminate all the components of the relays signals from the eavesdropper's observation unless we set some of the relays' independent signal components $\tilde{X}_i$ to zero. More precisely, if $\tilde{P}_i > 0,\ \forall\, i \in \mathcal{T}$, then we can only eliminate half of the relays' signals from the eavesdropper's observation. In contrast, in the MRSH-DF strategy, we were able to achieve full ZF because all the relays' independent signal components $\tilde{X}_i,\ i \in \mathcal{T}$ were zero in that strategy. However, here if we insist that all the relays must transmit fresh information in each block, i.e., $\tilde{P}_i > 0,\ \forall\, i \in \mathcal{T}$, then only the signal components from either the odd (or the even) relays in the multi-hop ordering can be eliminated from the eavesdropper's observation but not both. Hence, we obtain a MRMH-DF strategy with partial ZF (MRMH-PZF). The reason for this is that whenever we want to eliminate the signal X_i from the eavesdropper's observation, we adjust the correlation between X_i and X_{i-1} through choosing the proper value for α_{i-1}. However, this will necessarily give rise to a non-zero coefficient of X_{i-1} in the eavesdropper's observation. For example, when $T = 3$, the eavesdropper's observation Y_5 is given by (26) shown above in this page. Here, we can either force the coefficients of $\tilde{X}_1$ and $\tilde{X}_3$ only to zero by setting $\alpha_0 = \alpha_0^{\text{ZF}} \triangleq -\frac{h_{15}}{h_{05}}$ and $\alpha_2 = \alpha_2^{\text{ZF}} \triangleq -\frac{h_{35}}{h_{25}}$, or we can force the coefficient of $\tilde{X}_2$ only to zero by setting $\alpha_1 = \alpha_1^{\text{ZF}} \triangleq -\frac{h_{25}}{h_{15}+h_{05}\alpha_0}$ where $\alpha_0 \neq \alpha_0^{\text{ZF}}$.

One can choose to force either the odd or the even terms of the relay signals in the eavesdropper's observation to zero. In general, one should make the choice such that the coefficients with higher channel gains are forced to zero. Without loss of generality, we force the odd terms to zero by choosing $\alpha_{2i} = \alpha_{2i}^{\text{ZF}} \triangleq -\frac{h_{2i+1,T+2}}{h_{2i,T+2}},\ \forall i \in \{0,\cdots,\lfloor\frac{T}{2}\rfloor\}$. The rest of the coefficients must be chosen such that the power constraints (23) are satisfied. Hence, in this case, the achievable rate $R^{\text{DF/PZF}}$ is given by (27) shown above in this page. Thus, we conclude that in order to achieve full ZF in this strategy, we must set half of the independent signal components of the relays to zero, e.g., $\tilde{X}_i = 0$ (and hence $\tilde{P}_i = 0$) for all even i in $\mathcal{T}$. However, it would be inefficient to use a DF strategy with T hops where half of the relays transmit the same signals (except for a scaling factor) that the other half of the relays transmit. Based on this observation, we propose below a multi-hop DF strategy using T relays but with only $T/2$ hops and show that full ZF is possible in this case. Indeed, for the Gaussian model, the strategy proposed below is a practical realization of the T-hop strategy discussed here with full ZF, i.e., when half of the relays independent signal components are set to zero in the T-hop strategy. It is clear now that the first MRSH-DF strategy represents one extreme case of the MRMH-DF strategy with T hops where all the relays' independent signals components $\tilde{X}_i,\ i \in \mathcal{T}$ are set to zero. As discussed earlier, this leads to the drawback of having the achievable rate limited by the furthest relay from the

$$R^{\text{DF}} = \min\Bigg\{ \min_{j\in\{1,2\}} I(X_0;Y_j|X_{1,2},\cdots,X_{T-1,T}),\cdots, \min_{j\in\{2i-1,2i\}} I(X_0,X_{1,2},\cdots,X_{2i-3,2i-2};Y_j|X_{2i-1,2i},\cdots,X_{T-1,T}),\cdots,$$
$$I(X_0,X_{1,2},\cdots,X_{T-1,T};Y_{T+1})\Bigg\} - I(X_0,X_{1,2},\cdots,X_{T-1,T};Y_{T+2}) \tag{28}$$

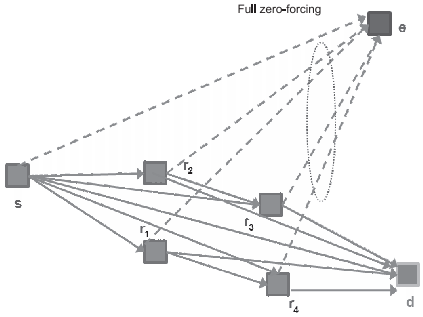

Fig. 4. Multiple relay $T/2$-hop strategy for a multiple relay network with an eavesdropper.

source. On the other hand, the other extreme is to have a T-hop strategy where we insist that all the relays transmit fresh information (represented by the independent signals $\tilde{X}_i$) in every transmission block. In this case, although the bottleneck problem is solved, only partial ZF is possible and without optimal power allocation (which is analytically intractable) there will be no guarantees on the information rate leaked to the eavesdropper. Hence, we propose next a multi-hop strategy that sits somewhere in the middle between these two extremes and provides an efficient and practical compromise where the achievable rate is not limited by the worst source-relay channel as in the MRSH-DF strategy but rather limited by the second best source-relay channel and all the relays' signals can be fully eliminated from the eavesdropper's observation.

C. Multiple Relay Multiple Hop DF with Full Zero-Forcing (MRMH-DF/FZF) Strategy

First, we discuss the general strategy without imposing the ZF constraint. Then, in the Gaussian case, we show how to achieve full ZF. In this strategy, we assume for simplicity that the number of relays T is even. We also take the number of the message blocks B to be even. The transmission of each message block takes place in $T/2$ hops; see Figure 4. This is done as follows. In any given transmission block b of the source message, the closest pair of relays to the source decodes the bth message block transmitted by the source and forwards it (with the help of the source) to the second closest pair of relays in the transmission block $b+1$ which decodes it and then forwards it (with the help of the source and the first pair of relays) to the third closest pair of relays[3] in the transmission block $b+2$ and so on so forth till the furthest pair of relays from the source decodes the bth message block and forwards it (with the help of the source and all the other relays) to the destination in the transmission block $b+T/2$. As in the previous subsection, since the multi-hop transmission is pipelined, the overhead is $T/2$ blocks. Hence, the loss in the achievable rate due to this overhead since $B >> T$. According to scenario described above, let the relays in the ith pair be labeled as $2i-1$ and $2i$, $1 \le i \le T/2$. In the case of the general discrete memoryless multiple relay channel with external eavesdropper given by some conditional distribution $p(y_1,\cdots,y_{T+1},y_{T+2}|x_0,\cdots,x_T)$, by combining the results of the two previous subsections, it can be shown that the achievable secrecy rate R^{DF} by such strategy for is given by (28) shown above in this page for some auxiliary random variables $X_{1,2},\cdots,X_{T-1,T}$ where $p(x_{1,2},\cdots,x_{T-1,T},x_0,x_1,\cdots,x_T)$ factors as $p(x_0|x_{1,2},\cdots,x_{T-1,T})\prod_{j=1}^{\frac{T}{2}} p(x_{2j-1}|x_{2j-1,2j})\, p(x_{2j}|x_{2j-1,2j})$. For the Gaussian channel (10)–(12), we choose the channel inputs as follows. $X_0 = \tilde{X}_0 + \alpha_0 X_{1,2}$, $X_1 = X_{1,2}$, $X_2 = \beta_{1,2}X_{1,2}$, $X_{1,2} = \tilde{X}_{1,2} + \alpha_{1,2}X_{3,4}$, $X_3 = X_{3,4}$, $X_4 = \beta_{3,4}X_{3,4}$, $X_{3,4} = \tilde{X}_{3,4} + \alpha_{3,4}X_{5,6}$ and so on so forth, till $X_{T-1} = X_{T-1,T}$, $X_T = \beta_{T-1,T}X_{T-1,T}$, and $X_{T-1,T} = \tilde{X}_{T-1,T}$ where $\tilde{X}_0$ and all $\tilde{X}_{2i-1,2i}$, $i = 1,\cdots,T/2$ are independent circularly symmetric complex Gaussian random variables with zero mean an variances $\tilde{P}_0$ and $\tilde{P}_{2i-1,2i}$, $i = 1,\cdots,T/2$, respectively, and α_0, $\alpha_{2i-1,2i}$, $i = 1,\cdots,T/2-1$, and $\beta_{2i-1,2i}$, $i = 1,\cdots,T/2$ are some complex numbers.

Equivalently, we have

$$X_0 = \tilde{X}_0 + \alpha_0 \sum_{i=0}^{\frac{T}{2}-1} \left(\prod_{j=1}^{i} \alpha_{2j-1,2j} \right) \tilde{X}_{2j+1,2j+2} \tag{29}$$

and, for $\ell = 1,\cdots,T/2$, we have

$$X_{2\ell-1} = \sum_{i=\ell-1}^{\frac{T}{2}-1} \left(\prod_{j=1}^{i} \alpha_{2j-1,2j} \right) \tilde{X}_{2i+1,2i+2} \tag{30}$$

$$X_{2\ell} = \beta_{2\ell-1,2\ell} X_{2\ell-1} \tag{31}$$

where, whenever $i < j$, the product $\prod_{t=j}^{i}$ is set to 1 and the sum $\sum_{t=j}^{i}$ is set to 0. From (13), we must have

$$\tilde{P}_0 + |\alpha_0|^2 \sum_{i=0}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \le \bar{P}_0 \tag{32}$$

and, for $\ell = 1,\cdots,T/2$,

$$\sum_{i=\ell-1}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \le \bar{P}_{2\ell-1} \tag{33}$$

$$|\beta_{2\ell-1,2\ell}| \sum_{i=\ell-1}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \le \bar{P}_{2\ell} \tag{34}$$

[3]Here, we mean closest to the source.

$$R^{\mathrm{DF}} = \min\left\{ \min_{t\in\{1,\cdots,\frac{T}{2}\}} \left\{ \min_{i\in\{2t-1,2t\}} \log\left(1+|h_{0i}|^2\tilde{P}_0 + \sum_{\ell=1}^{t-1}\left|\alpha_0 h_{0i}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}(h_{2k-1,i}+\beta_{2k-1,2k}h_{2k,i})\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right|^2\tilde{P}_{2\ell-1,2\ell}\right)\right\},\right.$$
$$\left.\log\left(1+|h_{0,T+1}|^2\tilde{P}_0 + \sum_{\ell=1}^{\frac{T}{2}}\left|\alpha_0 h_{0,T+1}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}(h_{2k-1,T+1}+\beta_{2k-1,2k}h_{2k,T+1})\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right|^2\tilde{P}_{2\ell-1,2\ell}\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0 + \sum_{\ell=1}^{\frac{T}{2}}\left|\alpha_0 h_{0,T+2}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}(h_{2k-1,T+2}+\beta_{2k-1,2k}h_{2k,T+2})\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right|^2\tilde{P}_{2\ell-1,2\ell}\right) \tag{35}$$

$$Y_{T+2} = h_{0,T+2}\tilde{X}_0 + \sum_{\ell=1}^{\frac{T}{2}}\left(\alpha_0 h_{0,T+2}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}(h_{2k-1,T+2}+\beta_{2k-1,2k}h_{2k,T+2})\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right)\tilde{X}_{2\ell-1,2\ell} + N_{T+2} \tag{36}$$

It follows that the achievable rate R^{DF} is given by (35) shown above in this page.

Now, we show that one can adjust the parameters in this strategy to fully eliminate all the relays' signals from the eavesdropper observation and hence obtain a MRMH-DF strategy with full ZF (MRMH-DF/FZF). First, we observe that the eavesdropper's observation is given by (36) above in this page. Let ζ_ℓ denote the coefficient of $\tilde{X}_{2\ell-1,2\ell}$ in (36). One can verify that, for $\ell = 2,\cdots,T/2$, ζ_ℓ can be obtained recursively from $\zeta_{\ell-1}$ as follows

$$\zeta_\ell = \alpha_{2\ell-3,2\ell-1}\zeta_{\ell-1} + h_{2\ell-1,T+2} + \beta_{2\ell-1,2\ell}h_{2\ell,T+2} \tag{37}$$

Thus, by setting $\beta_{2\ell-1,2\ell} = -\frac{h_{2\ell-1,T+2}}{h_{2\ell,T+2}}$, one can eliminate all the relays' signals from the eavesdropper observation. The rest of the parameters, i.e., α_0, $\alpha_{2\ell-1,2\ell}$, $1 \le \ell \le T/2$ and the power values $\tilde{P}_0$, $\tilde{P}_{2\ell-1,2\ell}$, $1 \le \ell \le T/2$ should then be chosen to maximize the achievable secrecy rate which is now given by (38) shown at the top of the next page.

IV. NUMERICAL RESULTS

First, we consider the single relay DF strategy. We set $\bar{P}_1 = 10$, $h_{01} = \sqrt{2}$, and $h_{13} = h_{12} = h_{02} = 1$. In Fig. 5, we plot both the achievable secrecy rate $R^{\mathrm{DF/ZF}}$ by the DF/ZF strategy and the secrecy capacity C^{GWT} of the channel without a relay as functions of the source total power $\bar{P}_0$. We do this for two cases of the channel gain h_{03}, namely, $h_{03} = \sqrt{1.2}$ and $h_{03} = \sqrt{0.8}$. It is clear that, as Corollary 1 suggests, when $h_{01} > h_{03} > 1$, we have $R^{\mathrm{DF/ZF}} > C^{\mathrm{GWT}} = 0$ for all $\bar{P}_0$. On the other hand, when $h_{01} > 1 > h_{03}$, the DF/ZF strategy becomes useful when $\bar{P}_0$ is large enough.

Next, we consider the multiple relay model with T relays. We devise a simulation for the following experiment. Consider a two-dimensional coordinate system where the source (node 0) is located at the origin. The channel gain $h_{\ell k}$ between any two nodes ℓ and k is given by $h_{\ell k} = d_{\ell k}^{-\gamma}e^{j\theta_{\ell k}}$ where $d_{\ell k}$ is the distance between ℓ and k, $\gamma > 1$ is the path loss coefficient, and $\theta_{\ell k}$ accounts for independent phase fading and is uniformly and independently distributed over $[0, 2\pi)$ for all ℓ, k. We choose $d_{0,T+1} = d_{0,T+2} = 1$ km and take $\gamma = 3$. We use a constant power allocation policy at all the relays where the transmit powers of all the relays are set to $\bar{P}_r = 10$ and accordingly power is allocated at the source to maximize the achievable rate where the total average power at the source is set to $\bar{P}_0 = 50$. All the channel gains are assumed to be fixed for the whole transmission duration and assumed to be known at all the nodes. We consider two scenarios. In the first scenario, all the T relays are uniformly spread over a disc of radius 0.75 km centered at the source. In the second scenario, all the T relays are at the same distance of 0.5 km from the source.

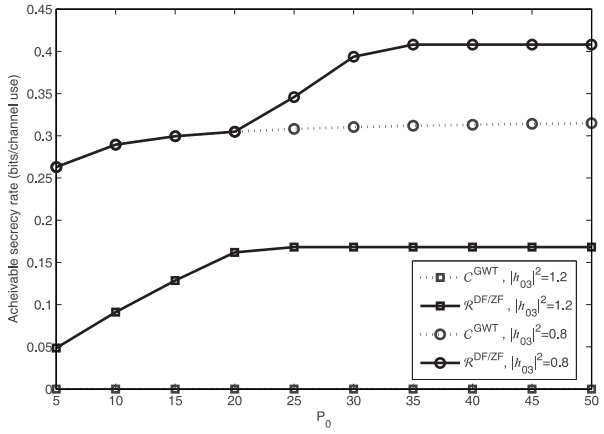

Fig. 5. The achievable secrecy rate, $R^{\mathrm{DF/ZF}}$, and the secrecy capacity of the original wiretap channel, C^{GWT}, versus the source's total power, $\bar{P}_0$, for two cases: $h_{03} = \sqrt{1.2}$ and $h_{03} = \sqrt{0.8}$.

$$R^{\text{DF/FZF}} = \min\left\{ \min_{t\in\{1,\cdots,\frac{T}{2}\}} \left\{ \min_{i\in\{2t-1,2t\}} \log\Big(1+|h_{0i}|^2\tilde{P}_0 + \sum_{\ell=1}^{t-1}\Big|\alpha_0 h_{0i}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}\left(h_{2k-1,i} - \frac{h_{2k-1,T+2}}{h_{2k,T+2}}h_{2k,i}\right)\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\Big|^2\tilde{P}_{2\ell-1,2\ell}\Big)\right\}, \right.$$
$$\log\Big(1+|h_{0,T+1}|^2\tilde{P}_0 + \sum_{\ell=1}^{\frac{T}{2}}\Big|\alpha_0 h_{0,T+1}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}\left(h_{2k-1,T+1} - \frac{h_{2k-1,T+2}}{h_{2k,T+2}}h_{2k,T+1}\right)\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\Big|^2\tilde{P}_{2\ell-1,2\ell}\Big)\Bigg\}$$
$$\left. - \log\Big(1+|h_{0,T+2}|^2\tilde{P}_0\Big)\right\} \tag{38}$$

In Fig. 6, we plot the achievable secrecy rate by each of the proposed multiple-relay strategies, the MRSH-DF/ZF, the MRMH-DF/PZF, and the MRMH-DF/FZF strategies, for $T = 1, \cdots, 10$. Fig. 6 shows that the MRMH-DF/PZF strategy usually achieves higher rates than the MRSH-DF/ZF strategy when there is a noticeable variation in the magnitudes of the channel gains $h_{0,k},\ k \in \mathcal{T}$ between the source and the relays which is the case captured by the first scenario. However, since in the MRMH-DF/PZF strategy, we can eliminate only half of the signal terms from the eavesdropper's observation, as T increases, the MRMH-DF/PZF strategy becomes less efficient due to the increase in the number of signal components observed at the eavesdropper. One can also see that the MRSH-DF/ZF strategy is usually better than the MRMH-DF/PZF strategy when the amount of variation in the magnitudes of the channel gains between the source and the relays is small. This is clearly captured by the second scenario, where all such channel gains have the same magnitude. On the other hand, one can see the superiority of the rate achieved by the MRMH-DF/FZF strategy in both of the examples. This indeed is due to the fact that the MRMH-DF/FZF strategy enjoys the advantages of the two previous strategies with almost insignificant loss in the achievable rate in the typical situations.

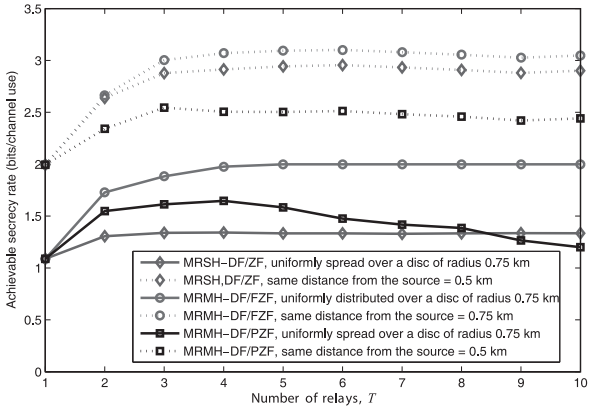

Fig. 6. The achievable secrecy rate, $R^{\text{DF/ZF}}$, by the MRSH-DF, the MRMH-DF/PZF, and the MRMH-DF/FZF strategies versus the number of relays, T, for two cases: When the relays are uniformly spread over a disc 0.75 km centered at the source, and when all the relays are the same distance (0.5 km) from the source.

V. CONCLUSIONS

In this paper, we considered the role of active cooperation for secrecy in multiple relay networks through DF strategies. We proposed and studied several alternatives to implement an efficient cooperation paradigm to provide and improve secrecy in multiple relay networks based on the DF scheme. We first studied the DF strategy for secrecy in a single relay network. We proposed a suboptimal DF/ZF strategy for which we obtained the optimal power control policy. For the multiple relay problesm, we proposed three different strategies based on DF/ZF technique and obtained the achievable secrecy rate by each strategy. In the first strategy, which is a single hop strategy, we showed that all the relays' signals can be eliminated at the eavesdropper (full ZF), however, the rate achieved by this strategy suffers from a bottleneck created by the worst source-relay channel. The second strategy is a multiple hop strategy that was shown to overcome the drawback of the first strategy, however, with the disadvantage of enabling only partial ZF assuming that all the relays are required to transmit fresh information in every transmission block. To provide a reasonable compromise between these two strategies, we proposed a third strategy, which is also a multiple hop strategy, for which we showed that full ZF is possible and the rate achieved does not suffer from the drawback of the first strategy. Finally, we gave numerical examples to illustrate the performance of each of the proposed strategies in terms of the achievable rates. The numerical results showed the sensitivity of the first two strategies to the amount of variation in the distance between the source and each relay. The numerical results also verified that, in typical conditions, the third strategy combines the advantages of the first two strategies and hence is considered a practical solution to provide a reasonable compromise between the first two strategies. It is important to note that our results rely on the standard assumption that global CSI, including the eavesdropper's CSI, is available at all the nodes. Providing security when nothing is known about the eavesdropper's CSI is an interesting problem that could be considered in future work.

APPENDICES

I. PROOF OF THEOREM 1

Define

$$R_1^{\text{DF/ZF}} = \log\left(\frac{1+|h_{01}|^2\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right) \tag{39}$$

$$R_2^{\text{DF/ZF}} = \log\left(\frac{1+\tilde{P}_0+|\alpha^{\text{ZF}}+1|^2P_1}{1+|h_{03}|^2\tilde{P}_0}\right) \tag{40}$$

Hence, from (9), we have $R^{\text{DF/ZF}} = \min\left\{R_1^{\text{DF/ZF}}, R_2^{\text{DF/ZF}}\right\}$. Let $\bar{R}^{\text{DF/ZF}}$ denote the maximum value of $R^{\text{DF/ZF}}$ over the constraint set given by (6) where $\alpha_0 = \alpha^{\text{ZF}} = -\frac{h_{13}}{h_{03}}$. Recall that the secrecy capacity of the original Gaussian wiretap channel without a relay C^{GWT} is given by (8). First, we observe that if $|h_{01}| \leq |h_{03}|$ then the maximum value of $R_1^{\text{DF/ZF}}$ is zero and is attained at $\tilde{P}_0 = 0$. Hence, $\bar{R}^{\text{DF/ZF}} = 0 \leq C^{\text{GWT}}$ and in this case, we can set $P_1 = 0$. On the other hand, if $|h_{03}| < |h_{01}| \leq 1$, then for all $\tilde{P}_0$ and P_1, we have $R^{\text{DF/ZF}} = R_1^{\text{DF/ZF}} \leq C^{\text{GWT}} = \log\left(\frac{1+\bar{P}_0}{1+|h_{03}|^2\bar{P}_0}\right)$ with equality attained if and only if $\tilde{P}_0 = \bar{P}_0$ and $P_1 = 0$.

Next, we turn to the case where $|h_{01} > \max\{1, |h_{03}|\}|$ which will be assumed in the rest of the proof. One can easily note that $R_1^{\text{DF/ZF}}$ (which does not depend on P_1) is a strictly increasing function in $\tilde{P}_0$ and that for every $\tilde{P}_0$, $R_2^{\text{DF/ZF}}$ is strictly increasing in P_1. However, the behavior of $R_2^{\text{DF/ZF}}$ as a function of $\tilde{P}_0$ for fixed P_1 depends on the power constraints $\bar{P}_0$, $\bar{P}_1$, and the channel gains $|h_{01}|$, $|h_{03}|$, and $|h_{13}|$. Since both $R_1^{\text{DF/ZF}}$ and $R_2^{\text{DF/ZF}}$ are non-decreasing in P_1, then so is $R^{\text{DF/ZF}}$. Hence, from (6), for every $\tilde{P}_0$, one can express the optimal power P_1 as a function of $\tilde{P}_0$, namely,

$$P_1^\star\left(\tilde{P}_0\right) = \min\left\{\bar{P}_1, \frac{\bar{P}_0-\tilde{P}_0}{|\alpha^{\text{ZF}}|^2}\right\} \tag{41}$$

Hence, $R_2^{\text{DF/ZF}}$ could be written, without loss of optimality, as a function of $\tilde{P}_0$ only as follows

$$R_2^{\text{DF/ZF}} = \log\left(\frac{1+\tilde{P}_0+|1+\alpha^{\text{ZF}}|^2\bar{P}_1}{1+|h_{03}|^2\tilde{P}_0}\right) \quad \text{if } 0 \leq \tilde{P}_0 \leq \left(\bar{P}_0-|\alpha^{\text{ZF}}|^2\bar{P}_1\right)^+ \tag{42}$$

$$R_2^{\text{DF/ZF}} = \log\left(\frac{1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2\bar{P}_0+\left(1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2\right)\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right) \quad \text{if } \left(\bar{P}_0-|\alpha^{\text{ZF}}|^2\bar{P}_1\right)^+ \leq \tilde{P}_0 \leq \bar{P}_0 \tag{43}$$

where $(x)^+$ denotes $\max\{0, x\}$ for any real number x. Consequently, the derivative of $R_2^{\text{DF/ZF}}$ with respect to $\tilde{P}_0$ is given by

$$\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} = \frac{1-|h_{03}|^2-|h_{03}|^2|1+\alpha^{\text{ZF}}|^2\bar{P}_1}{\left(1+\tilde{P}_0+|1+\alpha^{\text{ZF}}|^2\bar{P}_1\right)\left(1+|h_{03}|^2\tilde{P}_0\right)} \quad \text{whenever } 0 \leq \tilde{P}_0 \leq \left(\bar{P}_0-|\alpha^{\text{ZF}}|^2\bar{P}_1\right)^+ \tag{44}$$

$$\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} = \frac{1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2-|h_{03}|^2-|h_{03}|^2|1+\frac{1}{\alpha^{\text{ZF}}}|^2\bar{P}_0}{\left(1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2\bar{P}_0+\left(1-|1+\frac{1}{\alpha^{\text{ZF}}}|^2\right)\tilde{P}_0\right)\left(1+|h_{03}|^2\tilde{P}_0\right)} \quad \text{whenever } \left(\bar{P}_0-|\alpha^{\text{ZF}}|^2\bar{P}_1\right)^+ \leq \tilde{P}_0 \leq \bar{P}_0 \tag{45}$$

This leads to the four cases in Theorem 1 which we will prove below.

- Case (1): The second condition of this case implies that for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$, $R_2^{\text{DF/ZF}}$ and $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0}$ are given by (43) and (45), respectively. The first condition of this case implies that $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} \geq 0$. Thus, both $R_1^{\text{DF/ZF}}$ and $R_2^{\text{DF/ZF}}$ are increasing in $\tilde{P}_0$ and hence $\bar{R}^{\text{DF/ZF}}$ is attained at $\tilde{P}_0 = \tilde{P}_0^\star = \bar{P}_0$ which, by (41), implies that $P_1^\star = 0$. Moreover, in this case, it is clear that at the optimal power values $\bar{R}^{\text{DF/ZF}} = R_2^{\text{DF/ZF}} = C^{\text{GWT}}$.
- Case (2): Similar to case (1), the second condition of this case implies that for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$, $R_2^{\text{DF/ZF}}$ and $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0}$ are given by (43) and (45), respectively. However, the first condition of this case implies that $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} < 0$. Thus, $R_1^{\text{DF/ZF}}$ is strictly increasing in $\tilde{P}_0$ whereas $R_2^{\text{DF/ZF}}$ is strictly decreasing in $\tilde{P}_0$. Therefore, $\bar{R}^{\text{DF/ZF}}$ is attained at when $R_1^{\text{DF/ZF}} = R_2^{\text{DF/ZF}}$ which gives the optimal power values $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{\text{ZF}}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\bar{P}_0$ and $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\text{ZF}}|^2}$. We also note that at $\tilde{P}_0 = \bar{P}_0$, we have $R_2^{\text{DF/ZF}} = C^{\text{GWT}}$. This together with the fact that $R_2^{\text{DF/ZF}}$ is strictly decreasing in $\tilde{P}_0$ implies that $\bar{R}^{\text{DF/ZF}}$ is strictly larger than C^{GWT}.
- Case (3): In this case, one can easily verify from (44) and (45) that $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} \geq 0$ for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$. Hence, both $R_1^{\text{DF/ZF}}$ and $R_2^{\text{DF/ZF}}$ are increasing in $\tilde{P}_0$. Thus, $\tilde{P}_0^\star$, $P_1^\star$, and $\bar{R}^{\text{DF/ZF}}$ are the same as in case (1).
- Case (4):
  - Case (4-a): In this case, one can verify from (44) and (45) that $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} > 0$ whenever $0 \leq \tilde{P}_0 \leq \bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$ and $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} < 0$ whenever $\bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$. This implies that $R_2^{\text{DF/ZF}}$ attains its local maximum at $\tilde{P}_0 = \bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$. Moreover, in this case, $R_2^{\text{DF/ZF}} < R_1^{\text{DF/ZF}}$ at $\tilde{P}_0 = \bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$. Hence, $\bar{R}^{\text{DF/ZF}}$ is attained at $\tilde{P}_0^\star = \bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$ and at such point $R_2^{\text{DF/ZF}} = \bar{R}^{\text{DF/ZF}}$. Since $R_2^{\text{DF/ZF}}$ is strictly decreasing in $\tilde{P}_0$ for $\bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$ and since $R_2^{\text{DF/ZF}} = C^{\text{GWT}}$ at $\tilde{P}_0 = \bar{P}_0$, then we must have $\bar{R}^{\text{DF/ZF}} > C^{\text{GWT}}$.
  - Case (4-b): In this case, from (44) and (45), we have $\frac{\partial R_2^{\text{DF/ZF}}}{\partial \tilde{P}_0} < 0$ for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$. It follows that the optimal power value $\tilde{P}_0^\star$ is obtained by solving $R_1^{\text{DF/ZF}} = R_2^{\text{DF/ZF}}$ in $\tilde{P}_0$. In this case, we note that $R_1^{\text{DF/ZF}} = R_2^{\text{DF/ZF}}$ happens when $R_2^{\text{DF/ZF}}$ is given by (42), and hence $\tilde{P}_0^\star = \frac{|1+\alpha^{\text{ZF}}|^2}{|h_{01}|^2-1}\bar{P}_1$. It follows from (41) that $P_1^\star = \bar{P}_1$. At the optimal power values, we have $R_2^{\text{DF/ZF}} = \bar{R}^{\text{DF/ZF}}$. This together with the fact that $R_2^{\text{DF/ZF}}$ is strictly decreasing in $\tilde{P}_0$ for $0 \leq \tilde{P}_0 \leq \bar{P}_0$ and the fact that at $\tilde{P}_0 = \bar{P}_0$, we have $R_2^{\text{DF/ZF}} = C^{\text{GWT}}$, it follows that $\bar{R}^{\text{DF/ZF}} > C^{\text{GWT}}$.

– Case (4-c): In this case, one can easily verify that $R_2^{\text{DF/ZF}}$ is strictly decreasing in $\tilde{P}_0$ for $\bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$ and that $R_1^{\text{DF/ZF}} = R_2^{\text{DF/ZF}}$ happens when $R_2^{\text{DF/ZF}}$ is given by (43), i.e., the value of $\tilde{P}_0$ at which $R_1^{\text{DF/ZF}} = R_2^{\text{DF/ZF}}$ is greater than or equal to $\bar{P}_0 - |\alpha^{\text{ZF}}|^2\bar{P}_1$. Hence, this value of $\tilde{P}_0$ must be the optimal power value $\tilde{P}_0^\star$. As in case (2), this optimal value is given by $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{\text{ZF}}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{\text{ZF}}}|^2}\bar{P}_0$ which, by (41), implies that $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{\text{ZF}}|^2}$. Again, like in cases (2),(4-a), and (4-b), one can show that $\bar{R}^{\text{DF/ZF}} > C^{\text{GWT}}$.

REFERENCES

[1] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. ISIT*, Nice, France, June 2007, pp. 926–930.

[2] Y. Oohama and S. Watanabe. (2010, Sept.). Capacity results for relay channels with confidential messages. [Online]. Available: http://arxiv.org/pdf/1009.5829.pdf

[3] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3801–3827, Aug. 2010.

[4] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, pp. 137–155, Jan. 2011.

[5] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, pp. 572–584, Sept. 1979.

[6] L. Lai and H. E. Gamal, "Cooperation for secrecy: The relay-eavesdropper channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[7] X. He and A. Yener, "Cooperative jamming: The tale of friendly interference for secrecy," *Securing Wireless Communications at the Physical Layer.* W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[8] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC*, Sept. 2005.

[9] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[10] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 5747–5755, Dec. 2008.

[11] X. He and A. Yener. (2009, July). Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels. [Online]. Available: http://arxiv.org/pdf/0907.5388.pdf

[12] P. Xu, Z. Ding, X. Dai, and K. Leung. (2012, May). On the application of noisy network coding to the relay-eavesdropper channel. [Online]. Available: http://arxiv.org/abs/1203.5602

[13] S. H. Lim, Y.-H. Kim, A. E. Gamal, and S.-Y. Chung, "Noisy network coding," *IEEE Trans. Inf. Theory*, vol. 57, pp. 3132–3152, May 2011.

[14] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.

[15] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010, pp. 1–6.

[16] J. Huang and A. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *Proc. IEEE GlobeCom*, Miami, FL, Dec. 2010.

[17] R. Bassily and S. Ulukus, "Deaf cooperation for secrecy in mutiple-relay networks," in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011.

[18] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. Allerton Conf. Commun., Control, Comput., Monticello*, IL, Sept. 2008.

[19] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," *EURASIP J. Advances Signal Process.*, Aug. 2010. Submitted.

[20] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033–4039, Sept. 2009.

[21] A. Khisti and G. Wornell, "Secure transmission with multiple antenna: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, July 2010.

[22] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[23] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.

[24] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3037–3063, Sept. 2005.

[25] P. Gupta and P. R. Kumar, "Towards an information theory of large networks: An achievable rate region," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1877–1894, Aug. 2003.

[26] T. M. Cover and J. A. Thomas, *Elements of Information theory*. John Wiley and Sons, 1991.

Raef Bassily received the B.S. degree in Electrical and Computer Engineering and the M.S. degree in Engineering Mathematics from Cairo University, Giza, Egypt in 2003 and 2006, respectively. He received the Ph.D. degree in Electrical and Computer Engineering from the University of Maryland, College Park in 2011. He was a Research Associate in the Department of Computer Science at the University of Maryland, College Park, from January to August 2012. Since August 2012, he has been a Research Associate in the Department of Computer Science and Engineering at the Pennsylvania State University. His research interests include information theory, wireless communications, cryptography, network security, statistical data privacy, and machine learning.

Sennur Ulukus is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, physical-layer information-theoretic security for wireless networks, and energy-harvesting wireless communications.

She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, and the 2010–2011 ISR Outstanding Systems Engineering Faculty Award. She served as an Associate Editor for the IEEE Transactions on Information Theory between 2007–2010, as an Associate Editor for the IEEE Transactions on Communications between 2003-2007, and as a Guest Editor for the Journal of Communications and Networks for the special issue on energy harvesting in wireless networks, as a Guest Editor for the IEEE Transactions on Information Theory for the special issue on interference networks, as a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issue on multiuser detection for advanced communication systems and networks. She served as the TPC co-chair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, the Medium Access Control (MAC) Track at the 2008 IEEE Wireless Communications and Networking Conference, the Wireless Communications Symposium at the 2010 IEEE International Conference on Communications, the 2011 Communication Theory Workshop, and the Physical-Layer Security Workshop at the 2011 IEEE International Conference on Communications, the Physical-Layer Security Workshop at the 2011 IEEE Global Telecommunications Conference. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007-2009.