Decode-and-Forward Based Strategies for Secrecy in Multiple-Relay Networks

Raef Bassily Sennur Ulukus

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
bassily@umd.edu *ulukus@umd.edu*

***Abstract*—In this paper, we first study the Decode-and-Forward strategy for secrecy in a single-relay network. We propose a suboptimal Decode-and-Forward 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. The first strategy is a single-hop strategy in which all the relays decode the source message at the same time, then perform beamforming such that all the relays' signals are eliminated from the eavesdropper's observation (full zero-forcing). We give the achievable rate by this strategy and derive the optimal power control policy. We show that, in this strategy, the relays which are far from the source create a bottleneck and limit the achievable rate. The second strategy is a multiple hop strategy that overcomes the drawback of the first strategy, however, with the disadvantage of enabling partial zero-forcing only, assuming that all the relays are required to transmit fresh information in every transmission block. The third strategy is also a multiple hop strategy in which full zero-forcing is possible and the rate achieved does not suffer from the drawback of the first strategy.**

I. Introduction

Recently, there has been considerable attention devoted to the role of cooperation in wireless networks to improve the achievable secrecy rates. In general, one can distinguish between two types of cooperation in the secrecy context. The first type of cooperation for secrecy is passive (deaf) cooperation, 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, e.g., [1], [2], [3]. Whereas the second type of cooperation is active cooperation in which the relay listens to the source transmissions and uses its observation to improve the achievable secrecy rate. A well-known active cooperation strategy is the Decode-and-Forward (DF) strategy devised originally for the cooperative models with no secrecy constraint [4]. In [5], the basic relay-eavesdropper channel was introduced and achievable secrecy rates were obtained based on extended version of this strategy.

The role of active cooperation of beamforming relays in improving secrecy was investigated in [6] and [7]. In both [6] and [7], a half-duplex cooperative secrecy protocol is proposed in which the communication occurs in two stages where in the first stage 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) forward the source's message by beamforming to the destination. Reference [6] proposes a suboptimal zero-forcing strategy for the half-duplex model in which an additional constraint of canceling out the signals from the eavesdropper's observation is enforced.

In this paper, we consider the *full-duplex* relay channel with an eavesdropper where every node in the system can hear all the other transmitting node(s) at any time during the message is being communicated. 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 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. In the first strategy, all the relays decode the source message at the same time, then perform beamforming to the destination, i.e., in this strategy each message block is transmitted to the destination in a single hop[1]. We give the achievable rate using this strategy and derive the optimal power control policy for both the source and the relays. This strategy has an obvious drawback, namely, 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 proposed in [8] for the case with no secrecy constraints. In this strategy, the transmission of each message block occurs in a number of hops that is equal to the number of relays. We show that this strategy overcomes the bottleneck drawback of the first strategy, however, only partial zero-forcing is enabled by this strategy if all the relays transmit fresh information in every transmission block. We observe that to achieve full zero-forcing in the second strategy, we need to set half of the relays' signal components to zero. Based on this observation, we propose another multi-hop strategy that, in the Gaussian case, represents a practical realization of the second strategy with full zero-forcing and hence it combines

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

[1]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.

the advantages of the two aforementioned strategies in an efficient way. In the third strategy, the relays form clusters of two relays per cluster and the number of hops is half that of the second strategy. Finally, we give numerical results to compare the performance of the proposed strategies in terms of the achievable rates.

II. Decode-and-Forward with Single Relay

We consider the usual Gaussian relay-eavesdropper channel consisting of a source (node 0), a relay (node 1), a destination (node 2), and an eavesdropper (node 3). 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

$$Y_1 = h_{01}X_0 + N_1 \tag{1}$$
$$Y_2 = X_0 + X_1 + N_2 \tag{2}$$
$$Y_3 = h_{03}X_0 + h_{13}X_1 + N_3 \tag{3}$$

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

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

We confine our attention to the DF scheme which was introduced in its original setting without secrecy constraints in [4] and extended in the secrecy context in [5]. 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 $R^{DF} = \min\{I(X_0; Y_1|X_1), I(X_0, X_1; Y_2)\} - I(X_0, X_1; Y_3)$ (see [5]). For the Gaussian channel given by (1)-(3) above, as proposed in [4] as well as in [5], 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

$$\tilde{P}_0 + |\alpha_0|^2 P_1 \leq \bar{P}_0 \qquad \text{and} \qquad P_1 \leq \bar{P}_1 \tag{5}$$

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

$$R^{DF} = \min\left\{ \log\left(\frac{1 + |h_{01}|^2\tilde{P}_0}{1 + |h_{03}|^2\tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1}\right), \log\left(\frac{1 + \tilde{P}_0 + |\alpha_0 + 1|^2 P_1}{1 + |h_{03}|^2\tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1}\right)\right\} \tag{6}$$

where α_0, $\tilde{P}_0$, and P_1 must satisfy (5). For the DF strategy to achieve strictly larger secrecy rate than the secrecy capacity of the original Gaussian wiretap channel when the relay is not involved, it is clear from (6) 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 $\alpha_0 = \alpha^{ZF} \triangleq -\frac{h_{13}}{h_{03}}$. We denote the achievable rate in this case as $R^{DF/ZF}$ which, as a function of $(\tilde{P}_0, P_1)$, is given by

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

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

Theorem 1 If $|h_{01}| \leq \max\{1, |h_{03}|\}$, then the optimal power control policy that maximizes $R^{DF/ZF}$ is given by $\tilde{P}_0^\star = P_1^\star = 0$ when $|h_{01}| \leq |h_{03}|$ whereas $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$ 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 $R^{DF/ZF}$ is given by the following cases:

1) If $\bar{P}_0 \leq \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$.
2) If $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0$, $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.
3) If $\bar{P}_0 \leq \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$.
4) If $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then we have the following subcases:

- If $\bar{P}_1 \leq \min\left\{\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{ZF}|^2},\ \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\frac{\bar{P}_0}{|\alpha^{ZF}|^2}\right\}$, then $\tilde{P}_0^\star = \bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1,\ P_1^\star = \bar{P}_1$.
- If $\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{ZF}|^2} < \bar{P}_1 \leq \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \frac{|1+\alpha^{ZF}|^2}{|h_{01}|^2-1}\bar{P}_1,\ P_1^\star = \bar{P}_1$.
- Otherwise, then $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0,\ P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.

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 without a relay.

III. Decode-and-Forward with Multiple Relays

Let $\mathcal{T} = \{1, ..., T\}$ 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

$$Y_i = h_{0i}X_0 + \sum_{j\in\mathcal{T}\setminus\{i\}} h_{ji}X_j + N_i,\ i \in \mathcal{T} \tag{8}$$

$$Y_{T+1} = X_0 + \sum_{i\in\mathcal{T}} X_i + N_{T+1} \tag{9}$$

$$Y_{T+2} = h_{0,T+2}X_0 + \sum_{i\in\mathcal{T}} h_{i,T+2}X_i + N_{T+2} \tag{10}$$

where, for $i,\ j \in \{0, 1, ..., T+2\}$, 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

$$E[|X_0|^2] \triangleq P_0 \leq \bar{P}_0 \quad \text{and} \quad E[|X_i|^2] \triangleq P_i \leq \bar{P}_r,\ i \in \mathcal{T} \tag{11}$$

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. In the case of the general discrete memoryless multiple relay channel given by some conditional distribution $p(y_1, ..., y_{T+1}, y_{T+2}|x_0, ..., x_T)$, the DF scheme of [5] 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

$$R^{DF} = \min\left\{\min_{i\in\mathcal{T}}\{I(X_0; Y_i|X_r)\}, I(X_0, X_r; Y_{T+1})\right\} - I(X_0, X_r; Y_{T+2}) \tag{12}$$

for some auxiliary random variable X_r where $p(x_r, x_0, ..., x_T)$ 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 (11), we must have

$$\tilde{P}_0 + |\alpha_0|^2 P_r \leq \bar{P}_0 \qquad \text{and} \qquad |\alpha_i|^2 P_r \leq \bar{P}_r,\ i \in \mathcal{T} \tag{13}$$

Consequently, the achievable secrecy rate R^{DF} is given by (14) 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 (MRSH-DF/ZF) 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 $\alpha_0 = \alpha^{ZF} \triangleq -\frac{\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}}{h_{0,T+2}}$. Hence, the achievable rate becomes

$$R^{DF/ZF} = \min\left\{\log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+|\sum_{j\in\mathcal{T}}\alpha_j\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)|^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\} \tag{15}$$

where $i^\star = \arg\min_{i\in\mathcal{T}}|h_{0i}|$. We choose $\alpha_j = \frac{\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)^*}{\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|},\ \forall j \in \mathcal{T}$, where a^* denotes the complex conjugate of the complex number a, then, maximize the resulting rate

$$R^{DF/ZF} = \min\left\{\log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+\left(\sum_{j\in\mathcal{T}}\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|\right)^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right)\right\} \tag{16}$$

over all $\tilde{P}_0,\ P_r$ that satisfy $\tilde{P}_0 + |\alpha^{ZF}|^2 P_r \leq \bar{P}_0$ and $P_r \leq \bar{P}_1$. Indeed from the similarity between (16) and (7), we can easily modify Theorem 1 to obtain the optimal power control policy $(\tilde{P}_0^\star, P_r^\star)$ for this strategy.

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 and 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 [8] for the multiple relay model without an eavesdropper. In this strategy, the relays in $\mathcal{T}$ are ordered according to their distance from the source. The transmission of each message block occurs over T hops as follows. In any given transmission block b of the source message, the first relay decodes the current message block and forwards it to the second relay in the transmission block $b+1$ and so on so forth till the last relay decodes the source message block and forwards it to

$$R^{DF} = \min\left\{ \min_{i\in\mathcal{T}} \log\left(\frac{1+|h_{0i}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0+|\alpha_0 h_{0,T+2}+\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}|^2 P_r}\right), \right.$$
$$\left. \log\left(\frac{1+\tilde{P}_0+|\alpha_0+\sum_{j\in\mathcal{T}}\alpha_j|^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0+|\alpha_0 h_{0,T+2}+\sum_{j\in\mathcal{T}}\alpha_j h_{j,T+2}|^2 P_r}\right)\right\} \quad (14)$$

the destination in the transmission block $b+T$. 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. 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. In the case of the general discrete memoryless multiple relay channel with external eavesdropper given by some conditional distribution $p(y_1,...,y_{T+1},y_{T+2}|x_0,...,x_T)$, the multi-hop DF scheme of [8] 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. It is not difficult to see that the achievable secrecy rate R^{DF} by such scheme for some input distribution $p(x_0,...,x_T)$ is given by

$$R^{DF} = \min\Big\{ I(X_0;Y_1|X_1,X_2,...,X_T),...,$$
$$I(X_0,X_1,...,X_i;Y_{i+1}|X_{i+1},...,X_T),...,$$
$$I(X_0,X_1,...,X_T;Y_{T+1})\Big\}$$
$$-I(X_0,X_1,...,X_T;Y_{T+2}) \quad (17)$$

For the Gaussian channel (8)-(10), we choose the channel inputs as follows: $X_i = \tilde{X}_i + \alpha_i X_{i+1},\ i=0,...,T-1$ and $X_T = \tilde{X}_T$ where all $\tilde{X}_i,\ i=0,...,T$ are independent circularly symmetric complex Gaussian random variables with zero mean an variances $\tilde{P}_i,\ i=0,...,T$, respectively, and $\alpha_i, i=0,...,T-1$, are some complex numbers. Equivalently, we have $X_i = \tilde{X}_i + \sum_{j=i+1}^{T}\prod_{\ell=i}^{j-1}\alpha_\ell X_j,\ i=0,...,T-1$ and $X_T = \tilde{X}_T$. From (11), we must have

$$\tilde{P}_i + \sum_{j=i+1}^{T}\prod_{\ell=i}^{j-1}|\alpha_\ell|^2\tilde{P}_j \le \bar{P}_i,\ i\in\mathcal{T}\cup\{0\} \quad (18)$$

where $\bar{P}_i = \bar{P}_r\ \forall i\in\mathcal{T}$. Hence, the achievable rate R^{DF} is given by (19) at the top of the next page. Clearly, a necessary condition for this DF strategy to be useful 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.

Unlike the MRSH-DF/ZF strategy, here we cannot eliminate all the components of the relays signals from the eavesdropper's observation. More precisely, we can only eliminate the signals of either the odd (or the even) relays in the multi-hop ordering from the eavesdropper's observation but not both. The reason for that is that whenever we want to eliminate the signal X_i from the eavesdropper's observation, we adjust the covariance 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. Hence, we obtain a MRMH-DF strategy with partial zero-forcing (MRMH-DF/PZF). In general, one should make the choice such that the coefficients with higher channel gains are forced to zero. Here, we force the odd terms to zero by choosing $\alpha_{2i} = \alpha_{2i}^{ZF} \triangleq -\frac{h_{2i+1,T+2}}{h_{2i,T+2}},\ \forall i\in\{0,...,\lfloor\frac{T}{2}\rfloor\}$. The rest of the coefficients must be chosen such that the power constraints (18) are satisfied. Hence, in this case, the achievable rate $R^{DF/PZF}$ is given by (20) at the top of the next page.

C. MRMH-DF with Full Zero-Forcing (MRMH-DF/FZF)

In order to achieve full zero-forcing in the strategy above, 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 do not have fresh information to transmit. Based on this observation, we propose a multi-hop DF strategy using T relays but with only $\frac{T}{2}$ hops where full zero-forcing is possible. In this strategy, the relays are grouped in pairs which are ordered according to their distance from the source. The source message flows from the source to the first pair then to the second pair and so forth till it reaches the destination. Each pair of relays adjust their beamforming coefficients to ensure full zero-forcing at the eavesdropper. Hence, the achievable secrecy rate, $R^{DF/FZF}$ is given by (21) 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 Figure 1, we plot both the achievable secrecy rate $R^{DF/ZF}$ by the DF/ZF strategy and the secrecy capacity C^{GWT} of the channel without a relay as functions of the source total power $\bar{P}_0$. It is clear that, as Theorem 1 suggests, when $h_{01} > h_{03} > 1$, we have $R^{DF/ZF} > C^{GWT} = 0$ 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, consider a two-dimensional coordinate system of T relays where the source 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

$$R^{DF} = \min\left\{\min_{j\in\mathcal{T}} \log\left(1+|h_{0j}|^2\tilde{P}_0+\sum_{i=1}^{j-1}|h_{ij}+\sum_{\ell=0}^{i-1}h_{\ell j}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right), \log\left(1+\tilde{P}_0+\sum_{i\in\mathcal{T}}|1+\sum_{\ell=0}^{i-1}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0+\sum_{i\in\mathcal{T}}|h_{i,T+2}+\sum_{\ell=0}^{i-1}h_{\ell,T+2}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right) \quad (19)$$

$$R^{DF/PZF} = \min\left\{\min_{j\in\mathcal{T}} \log\left(1+|h_{0j}|^2\tilde{P}_0+\sum_{i=1}^{j-1}|h_{i,j}+\sum_{\ell=0}^{i-1}h_{\ell j}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right), \log\left(1+\tilde{P}_0+\sum_{i\in\mathcal{T}}|1+\sum_{\ell=0}^{i-1}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0+\sum_{\text{even } i\in\mathcal{T}}|h_{i,T+2}+\sum_{\ell=0}^{i-1}h_{\ell,T+2}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right) \quad (20)$$

$$R^{DF/FZF} = \min\left\{\min_{j\in\mathcal{T}} \log\left(1+|h_{0j}|^2\tilde{P}_0+\sum_{i=1}^{j-1}|h_{i,j}+\sum_{\ell=0}^{i-1}h_{\ell j}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right), \log\left(1+\tilde{P}_0+\sum_{i\in\mathcal{T}}|1+\sum_{\ell=0}^{i-1}\prod_{k=\ell}^{i-1}\alpha_k|^2\tilde{P}_i\right)\right\}$$
$$-\log\left(1+|h_{0,T+2}|^2\tilde{P}_0\right) \quad (21)$$

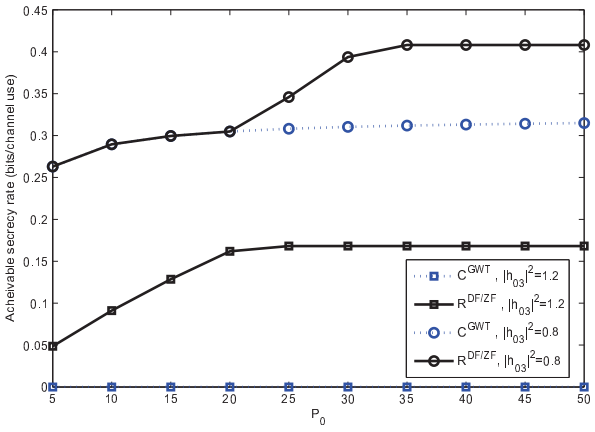

Fig. 1. The achievable secrecy rate, $R^{DF/ZF}$, and the secrecy capacity of the original wiretap channel, C^{GWT}, versus the source's total power, $\bar{P}_0$.

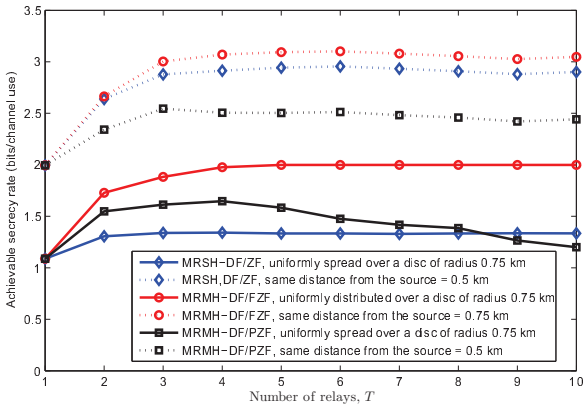

Fig. 2. The achievable secrecy rate, $R^{DF/ZF}$, by the MRSH-DF and the MRMH-DF strategies versus the number of relays, T.

at all the relays where $\bar{P}_r = 10$ and the source power is allocated to maximize the achievable rate where $\bar{P}_0 = 50$. We consider two scenarios. In the first, all the T relays are uniformly spread over a disc of radius 0.75 km centered at the source. Whereas in the second, all the T relays are at the same distance of 0.5 km from the source. Figure 2 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 $h_{0,k},\ k\in\mathcal{T}$ and vice versa which is reflected by the first and the second scenarios, respectively. One can also see the superiority of the rate achieved by the MRMH-DF/FZF strategy in both 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.

REFERENCES

[1] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, Sep. 2005.

[2] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Friendly jamming for wireless secrecy. In *IEEE International Conference on Communications, Cape Town, South Africa*, pages 1–6, May 2010.

[3] R. Bassily and S. Ulukus. Deaf cooperation for secrecy in mutiple-relay networks. In *IEEE Globecom, Houston, TX*, Dec. 2011. To appear.

[4] T. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. on Inf. Theory*, 25:572–584, Sep. 1979.

[5] L. Lai and H. El Gamal. Cooperation for secrecy: The relay-eavesdropper channel. *IEEE Trans. on Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Secure wireless communications via cooperation. In *46th Annual Allerton Conference on Communications, Control and Computing, UIUC, IL*, Sep. 2008.

[7] J. Zhang and M. C. Gursoy. Collaborative relay beamforming for secrecy. *EURASIP Journal on Advances in Signal Processing*, Aug. 2010. Submitted.

[8] G. Kramer, M. Gastpar, and P. Gupta. Capacity theorems for wireless relay channels. In *41th Annual Allerton Conference on Communication, Control and Computing, Monticello, IL*, pages 1074–1083, Oct. 2003.