COOPERATION STRATEGIES FOR SECRECY IN MIMO RELAY NETWORKS WITH UNKNOWN EAVESDROPPER CSI

Jing Huang and A. Lee Swindlehurst
Dept. of Electrical Engineering and Computer Science
University of California, Irvine
Irvine, CA 92697
{jing.huang,swindle}@uci.edu

ABSTRACT
We investigate secure communications for a four-node relay-eavesdropper channel with multiple data stream transmission, assuming that the eavesdropper’s channel state information (ECSI) is unavailable. Our approach is to allocate part of the global transmit power to satisfy a fixed target rate for the relay link, and then use the remaining power for jamming the eavesdropper. Two cooperative jamming strategies are investigated. In the first, jamming signals are only broadcast by the terminals that are also transmitting data. In the second scheme, the normally inactive nodes in the relay network are used as cooperative jamming sources. Algorithms are proposed for allocating the transmit power and the number of signal dimensions that carry data. Simulation results show that, under a global transmit power constraint, the secrecy rate is dramatically increased when the normally inactive nodes in the relay network provide jamming support for the relayed signals.

Index Terms— relay-eavesdropper channel, cooperative jamming, secure communications

1. INTRODUCTION
Due to the vulnerability of wireless networks to eavesdropping, there has recently been considerable interest in improving wireless security through physical layer mechanisms. These approaches exploit the degrees of freedom offered by multiple antennas and the multi-path nature of the wireless channel to "hide" signals from potential eavesdroppers. The theoretical foundation for physical layer security was laid by Wyner [1], who introduced the so-called wiretap channel and demonstrated that when the eavesdropper’s channel is a degraded version of the channel of the legitimate receiver, the transmitter can send secret messages to the destination with non-zero rate while keeping the eavesdropper from learning anything about the message. The secrecy capacity of the link is defined as the maximum achievable rate for which such secret communication is possible.

Recently, the focus of much of the work on physical layer security has been on wiretap channels with multiple antennas [2–6]. In particular, the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been fully characterized in [2, 5]. Beamforming techniques have been proposed that steer information signals away from the eavesdroppers and instead steer artificial noise or jamming signals in their direction [4, 7]. The goal is to degrade the eavesdropper’s channel without impacting the signals received by legitimate users. As a natural extension, multiple antenna wiretap channels have also been investigated for cooperative relaying networks [8–13]. In these cases, relays or even destinations can be used as helpers to provide jamming signals to confuse the eavesdropper. This approach is often referred to as cooperative jamming. In [9] a four-terminal relay-eavesdropper channel is addressed and a noise-forwarding strategy is devised in which the full-duplex relay sends codewords independent of the secret message to confuse the eavesdropper. A two-stage cooperative jamming protocol is investigated in [7], where multiple relay nodes act as an extension of the single-antenna source node. In [10], three cooperative schemes are proposed for a single-antenna relay network, and the corresponding relay weights and power allocation strategy are derived to enhance the secrecy for the second hop. An optimal beamforming design for decode-and-forward (DF) relays is investigated in [11], but only the scenario where the eavesdropper wiretaps just the link between the relay and destination is considered. Jamming beamformer design and power allocation are jointly investigated in [12], where a single-antenna relay is employed and a single data stream transmission is assumed.

Unlike the aforementioned work, this paper proposes cooperative jamming strategies for a half-duplex two-hop wireless MIMO relay system in which multiple data streams are transmitted. Secure communication for both hops of the relay link will be studied. Furthermore, nearly all of the prior work on these problems assumes that the eavesdropper’s channel state information (ECSI), or at least its distribution, is known at the transmitter. While this assumption is common, it is often not practical, especially if the eavesdropper is passive and not part of the network itself. Prior work on the case with unknown ECSI includes [14,15], which respectively discuss the use of jamming for single and multiple data stream transmissions in the point-to-point MIMO case. Since without ECSI it is impossible to optimize the secrecy rate of the link, the approach taken in these papers is to first allocate resources in order to guarantee a certain quality of service for the link, and then use any remaining resources for jamming the eavesdropper. In this paper, we extend this idea to half-duplex two-hop MIMO relay networks. We propose two basic approaches, a partially cooperative jamming (PCJ) scheme where only the information sources in each hop transmit jamming signals, and a fully cooperative jamming (FCJ) strategy where all the nodes in the relay network, including those that are normally inactive, can act as helpers to transmit jamming signals.

The mathematical model assumed in this paper is presented in the next section, and the following notational conventions will be followed throughout: $E\{\cdot\}$ denotes expectation, $(\cdot)^H$ is the Hermitian transpose, $|x|^\ast$ denotes max{$0, x$}, and $I$ is an identity matrix of appropriate dimension. Section 3 presents the PCJ and FCJ algo-
2. MATHEMATICAL MODEL

We consider a two-phase four-terminal relay system composed of a source (Alice), a destination (Bob), a relay node and an eavesdropper (Eve). All nodes are assumed to be half-duplex and have multiple antennas, and we assume there is no direct link between Alice and Bob. The number of antennas at Alice, Bob, the Relay and Eve are denoted by $N_a, N_b, N_r$ and $N_e$ respectively. Decode-and-forward (DF) relaying is employed and for simplicity we will only consider repetition-based coding, i.e., the Relay encodes the received signals onto the same number of data streams as Alice when multiplexing is applied. While the CSI for the relay network is assumed to be known to everyone (including the eavesdropper), no one besides the eavesdropper is assumed to possess ECSI.

The signals transmitted by Alice in the first phase contain both information and jamming signals, and in general Bob may also transmit jamming signals at the same time. Thus the signals received by the Relay and Eve in the first phase will be given by

$$y_r = H_{ar}(T_a z_a + T'_a z'_a) + H_{br} T'_r z'_b + n_r$$

$$y_e = H_{er}(T_a z_a + T'_a z'_a) + H_{be} T'_e z'_e + n_e$$

where $H_{ij}$ $(h_{ij})$ represents the channel matrix from node $i$ to $j$, with $i, j \in \{a, b, e, r\}$ denoting which of the four terminals is involved, $z_a$ is the information signal vector transmitted by Alice with $E(z_a^H z_a) = p_a$, and $T_a, T'_a \in \mathbb{C}^{N_a \times k}$ $(1 \leq k \leq s)$ is the transmit beamformer used by Alice, where $m = rank(H_{ar})$, $n = rank(H_{er})$, $s = \min(m, n)$, and $k$ represents the number of transmitted data streams. The vectors $z_r$ and $z_e$ are jamming signal vectors transmitted by Alice and Bob, respectively, and $T_a, T'_a \in \mathbb{C}^{N_a \times N_a - k}$ and $T'_b, T'_e \in \mathbb{C}^{N_b, N_e \times min(N_a - k, N_b, N_e)}$ are the corresponding transmit beamformers. We will let $Q_{za}, Q_{z'a}, Q_{zb}, Q_{z'b}$ represent the covariance matrices of $z_a, z'_a, z_b, z'_b$, respectively. The terms $n_r$ and $n_e$ represent naturally occurring noise at the Relay and Eve.

In phase 2, Alice can jam the eavesdropper when the Relay transmits information since this will produce no interference to Bob. Accordingly, the signals received by Bob and Eve in phase 2 are

$$y_b = H_{br}(T_a z_a + T'_a z'_a) + n_b$$

$$y_e = H_{er}(T_a z_a + T'_a z'_a) + H_{be} T'_e z'_e + n_e$$

where $z_r$ is the Relay’s information signal with transmit beamformer $T_r \in \mathbb{C}^{N_r \times k}$ and $E(z_r^H z_r) = p_r$, $z'_a$ and $z'_b$ are jamming signal vectors transmitted by the Relay and Alice, respectively, $T'_r \in \mathbb{C}^{N_r \times N_r - k}$ and $T_a, T'_a \in \mathbb{C}^{N_a \times N_a}$ are their corresponding transmit beamformers, and $n_r, n_e$ represent the noise vectors at Bob and Eve, respectively. For both phase 1 and phase 2, we assume the background noise to be Gaussian with covariance $\sigma^2 I$. The covariance matrices of $z_r, z'_a$ and $z'_b$ will be denoted by $Q_{zr}, Q_{z'a}$ and $Q_{z'b}$, respectively.

Under the assumption of repetition coding, the elements of $z_r$ are simply scaled versions of those in $z_a$. In particular, we can write $z_a = D_a z$ and $z_r = D_r z$, where $E(zz^H) = I$ and $D_a, D_r$ are diagonal power loading matrices that ensure the power constraints are met. For a global power constraint in each phase, we have

$$E(z_a^H z_a + z'_a^H z'_a + z'_b^H z'_b) \leq P$$

$$E(z_r^H z_r + z'_r^H z'_r + z'_a^H z'_a) \leq P.$$

We will also investigate scenarios with individual power constraints as follows: $E(z_a^H z_a + z'_a^H z'_a) \leq P_a, E(z_r^H z_r) \leq P_b, E(z'_b^H z'_b) \leq P_e$, and $E(z'_a^H z'_a) \leq P_a$.

The achievable secrecy rate of a four-terminal half-duplex DF relay channel is given by [13]:

$$R_s = \max (I_a - I_e)$$

where $I_a$ is the mutual information from the source to the destination, $I_e$ is the mutual information from the source to the eavesdropper, and the maximum is taken over all possible input covariance matrices. Secrecy rate will be used as the performance metric in this paper.

3. SECURE RELAYING WITH COOPERATIVE JAMMING

In this section, we propose a cooperative jamming strategy similar to that proposed in [16] in which the signal space at the receiver in each phase is divided into two orthogonal subspaces, an information subspace and a jamming subspace. Two jamming strategies will be studied. For partially cooperative jamming (PCJ), any available jamming power will only be allocated to the information transmitters, while Bob (in phase 1) and Alice (in phase 2) remain inactive. For fully cooperative jamming (FCJ), both the information transmitters and the normally inactive nodes can perform cooperative jamming. The term “cooperative jamming” refers to the fact that the jamming signals will be aligned so that they lie in the jamming subspace at the desired receiver, while the information signals will lie in the orthogonal information subspace. Since Eve’s channel is different from the desired receiver, this alignment will not hold and Eve’s received signal will be degraded.

In phase 1, assume that $span\{H_{ar}\} = span\{\eta_1, ..., \eta_m\}$, where $k \leq s$ and $\eta_1, \eta_2, ..., \eta_m$ represent an orthonormal basis. The information and jamming subspaces are defined to be $S_1$ and $J_1$, respectively, where $S_1 = span\{\eta_1, \eta_2, ..., \eta_m\}$ and $J_1 = S_1^\perp$. A standard choice for these subspaces would be to let $S$ be formed from the left singular vectors of $H_{ar}$ with the largest singular values. At the relay, a prefiltering matrix $W_r = [\eta_1, \eta_2, ..., \eta_s]$ is used to null out the jamming signals:

$$\tilde{y}_r = W_r^H H_{ar}(T_a z_a + T'_a z'_a) + H_{br} T'_r z'_b + n_r$$

$$= H_{ar} z_a + \tilde{n}_r$$

where $H_{ar} = W_r^H H_{ar} T_a$, and the transmit beamformers are chosen such that $H_{ar} T_a z_a \in S_1$, and $H_{br} T'_r z'_b \in J_1, H_{br} T'_e z'_e \in J_1$. The signal received by Eve in phase 1 is

$$y_e = H_{er}(T_a z_a + T'_a z'_a) + H_{be} T'_e z'_e + n_e$$

$$= H_{er} z_a + \tilde{n}_e$$

where $\tilde{n}_e = H_{er} T'_e z'_e + H_{be} T'_e z'_e + n_e$.

In phase 2, signal $S_2$ and jamming $J_2$ subspaces are chosen from $span\{H_{er}\}$, and similar to phase 1, the signals at Bob and Eve are

$$\tilde{y}_b = W_b^H H_{br}(T_a z_a + T'_a z'_a) + n_b$$

$$= H_{br} z_a + \tilde{n}_b$$

$$y_e = H_{er}(T_a z_a + T'_a z'_a) + H_{be} T'_e z'_e + n_e$$

$$= H_{er} z_a + \tilde{n}_e$$
where $\tilde{H}_{rb} = W_b H_{rb} T_r$, $\tilde{H}_{re} = H_{re} T_r$, $\tilde{H}_{ae} = H_{ae} T_a$, $\tilde{z}_r = z_r + \tilde{H}_{rb} z_a$, and as before, $T_r$ and $T_a$ force $H_{rb} T_r z_r \in S_2$ and $H_{ae} T_a z_a \in S_1$. Since the CSI of Eve is unavailable, we will set $T_{a2}'$ to be an identity matrix and uniformly allocate the power to $Q_{z,a}'$.

Expressions for the mutual information terms in (5) can be found as follows:

$$I_d = \min \{ I(z_a;y_r), I(z_r;y_b) \}$$

where

$$I(z_a;y_r) = \frac{1}{2} \log_2 \det(I + \frac{1}{\sigma^2} \tilde{H}_{ar} Q_{za} \tilde{H}_{ar}^H)$$

and $Q_{za}$ is a block diagonal matrix $\text{diag}(Q_{z,a1}, Q_{z,a2})$, and

$$Q_{z,a1} = H_{ae} T_a' Q_{z,a} T_a^H H_{ae}^H + H_{be} T_b' Q_{z,b} T_b^H H_{be}^H + \sigma^2 I$$

and $Q_{z,a2}$ is a block diagonal matrix $\text{diag}(Q_{z,a1}, Q_{z,a2})$, and

$$Q_{z,a2} = H_{ae} T_a^H Q_{z,a} T_a'^H H_{ae} + \sigma^2 I$$

To complete development of the approach described above, an algorithm is needed for determining the power allocation and the dimension $k$ of the information signal. If the MIMO channel is rich enough, more dimensions allocated to the signal subspace increases the amount of power available for jamming, but leads to a smaller dimensional jamming subspace for both transmitters and cooperative jammers. More antennas for Eve usually requires a higher dimensional jamming subspace, especially when Eve’s CSI is unknown to the transmitters. One of the advantages of FCJ in this case is that in addition to the pre-assigned jamming subspace of dimension $N_a - k$ (for phase 1), the helpers provide jamming support in additional dimensions due to the fact they have different channels to Eve. Taking the transmission in phase 1 as an example, assuming $k$ dimensions are assigned to the information subspace, the dimension of the jamming subspace seen by Eve will be more than $N_a - k$, i.e., $N_a - k \leq \text{dim(span}(H_{ae} T_a')) \cap \text{span}(H_{ae} T_a) \leq 2(N_a - k)$.

Considering the tradeoff between power and allocation of the jamming subspace dimension, we propose to use an approach similar to that in [15] and minimize the product of the power allocated to the information signal and the dimension of the information subspace, $(p_a + p_r)k$, such that the fixed target rate is achieved. We then allocate all remaining dimensions and power for jamming. Since the ECSI is not known, the jamming power will be uniformly distributed among all available dimensions at the transmitters and cooperative jammers. Assuming the target rate for the relay transmission is $R_t$, the proposed approach for FCJ is outlined as follows:

Step 1 Initialization

- Let $\text{svd}(\tilde{H}_{ar}) = U_a r_s V_{ar}^H$, $\text{svd}(\tilde{H}_{rb}) = U_r b r_b V_{rb}^H$.

Step 2 While $i \leq s$

- Let $W_r = [u_{ar,1}, ..., u_{ar,s}], W_b = [u_{br,1}, ..., u_{br,s}]$.
- $T_a = [v_{ar,1}, ..., v_{ar,i}], T_r = [v_{rb,1}, ..., v_{rb,i}]$.
- $T_a' = [v_{ar,i+1}, ..., v_{ar,N_a}], T_r' = [v_{rb,i+1}, ..., v_{rb,N_b}]$.
- $\text{svd}(W_r^H \tilde{H}_{ar}) = U_{ar} \Sigma_{ar} V_{ar}^H$, $T_b' = V_{br}[;i+1:N_b]$, and $T_a' = U_{ar}$.

Step 3 Power allocation

- Find $k = \arg \min (p_a + p_r) i \cdot i$, and determine all beamformers for the resulting $k$.
- Allocate $p_{a,k}$ to $\text{diag}\{Q_{z,a}, Q_{z,b}\}$, and $p_{r,k}$ to $\text{diag}\{Q_{z,r}, Q_{z,t}\}$ using water filling.
- Uniformly allocate $P - p_{a,k}$ to $\text{diag}\{Q_{z,a}, Q_{z,b}\}$, and $P - p_{r,k}$ to $\text{diag}\{Q_{z,r}, Q_{z,t}\}$.

The optimization problem in step 2 can be solved with a simple line search. If the target rate cannot be met with the total given power, then the link is assumed to be in outage.

The PCJ approach is similar to FCJ, except that we will not have the jamming support from Bob (in phase 1) and Alice (in phase 2), thus the beamformers $T_b$ and $T_{a2}$ in step 2 will not be used. In step 3, when the necessary amount of power for information signals is assigned, all remaining jamming power will be used by Bob and Alice in phase 1 and phase 2, respectively; i.e., $P - p_{a,k}$ and $P - p_{r,k}$ will be assigned to $\text{diag}\{Q_{z,a}, Q_{z,b}\}$ and $\text{diag}\{Q_{z,r}, Q_{z,t}\}$.

4. NUMERICAL RESULTS

In the following simulations, the elements of all the channel matrices are assumed to be zero-mean, i.i.d. complex Gaussian, and the nodes are assumed to be located at the four corners of a parallelogram with identical side length 800m. We assume a path-loss coefficient of 3.5, and the same background noise power $\sigma^2 = -60$dBm at all nodes. In order to compare the performance of the different cooperative jamming schemes, we also investigate using conventional relay transmissions without jamming. For this case, all the transmit power is assigned to the information signals. For scenarios involving individual transmit power constraints, the total transmit power is assumed to be evenly distributed to all transmit nodes. The fixed target rate for relay transmission is set to be $R_t = 2$bps/Hz.

The secrecy rate as a function of transmit power is shown in Fig. 1, where all nodes have four antennas. In this case, we see that if no jamming signals are used, a positive secrecy rate is barely possible. It can also be seen that having a global power constraint yields better performance than when individual power constraints are used. Obviously, FCJ achieves a big gain in terms of secrecy rate compared with PCJ, since FCJ leads to a higher dimensional
jamming subspace than PCJ, although both are subject to the same power constraint. Fig. 2 provides a detailed look at how the number of eavesdropper antennas affects the performance of the different cooperative jamming schemes. In this case, Alice, Bob and the Relay are equipped with four antennas, and the number of Eve’s antennas increases from two to ten. It can be seen that as the capability of the eavesdropper increases, the relative secrecy rate of FCJ is several times that of PCJ when $N_e \geq 4$, although the secrecy rates of all methods approach zero.

### 5. CONCLUSIONS

In this paper, we have proposed partially cooperative jamming (PCJ) and fully cooperative jamming (FCJ) strategies for a two-hop DF relay-eavesdropper network with unknown ECSI. Instead of maximizing the secrecy rate, our algorithms meet a target rate for the relay network while minimizing the product of the power allocated to signal transmission and the number of transmitted information streams. All remaining power and signal dimensions are allocated to jamming signals in order to degrade the eavesdropper’s channel. FCJ is seen to provide the best performance in terms of secrecy rate, since it is able to degrade additional signal dimensions at the eavesdropper.

### 6. REFERENCES


