Joint SVD-GSVD Precoding Technique and Secrecy Capacity Lower Bound for the MIMO Relay Wire-tap Channel

Marouen Jilani
Graduate School of Science and Technology
Keio University
3-14-1 Hiyoshi, Yokohama 223-8522, Japan
Email: marouan.jilani@gmail.com

Tomoaki Ohtsuki
Faculty of Science and Technology
Keio University
3-14-1 Hiyoshi, Yokohama 223-8522, Japan
Email: ohtsuki@ics.keio.ac.jp

***Abstract*—We consider a problem of secure communications for the communication system consisting of multiple outputs for a source and a relay and multiple inputs for the relay, a destination and an eavesdropper. For the above-mentioned communication system, we establish a lower bound on the secrecy capacity at which secure communications between the source and the destination are attainable. We make use of the singular value decomposition (SVD) and its generalization to decompose the whole system into parallel independent channels. At the source, the generalized singular value decomposition (GSVD) is performed to simultaneously diagonalize the channel matrices of the relay and the destination and independently code across the resulting parallel channels. At the relay, the SVD is performed to beamform the signal towards the destination. The scalar case of what we are considering in this paper has been investigated in previous literature, to prove that the introduction of a fourth party, the relay, in the wire-tap channel facilitates secure wireless communications. Our simulation results are in line with the scalar case's and prove to be successful in achieving secrecy capacity where the conventional model failed, i.e. when no relay is introduced and the eavesdropper's channel incurs as little noise as the legitimate receiver.**

I. Introduction

Wireless communications are prone to eavesdropping by nature : it is inevitable for electromagnetic waves propagated over the *public* medium to be subject to wire-tapping from an unwanted party, which makes the security one of the biggest challenges for the wireless community to ever encounter. However, owing to cryptography, wireless applications gained trust in the market. For instance, cryptosystems are deployed to prevent the computing power-limited enemy from causing any threat. Nevertheless, today the statement about this limitation is being regarded as a somehow strong assumption amid technological advances in computing technologies. Hence, the blink future of this kind of security and the need for the focus on security methods that drop this unrealistic assumption.

When introducing the brilliant notion of information-theoretic security [1], Shannon, the father of information theory, established the condition for a secure communication between legitimate parties to succeed: when an eavesdropper is no better informed about the transmit messages after intercepting them than he was before. By bringing the channel uncertainty into play, Wyner introduced the wire-tap channel [2] where he gave a new form of the condition for perfect secrecy, when the eavesdropper's equivocation about a message is equal to the entropy of the latter. For this to happen, the eavesdropper was assumed to incur a degraded version of the legitimate channel. From Wyner's model spanned many works that characterized the secrecy capacity of different channel models, namely the extension to the Gaussian channel [3], the broadcast channel [4] and the recent multiple-input multiple-output (MIMO) channel [5].

Among works to address the security issue in a relay-network scenario are [6], [7], [8] and [9]. In [6] and [7], the authors address the problem of securing a communication, between a sender and a receiver assisted by a relay, from the relay itself. In [8] and [9], the limits to the Gaussian wire-tap model in ensuring secure communications were pushed further by the introduction of a relay in the communication system. The fourth party proved to be a key component in establishing a secure link between the source and the destination even when the latter's channel is as noisy as the eavesdropper's. Our work here is also motivated by the fact that the MIMO wire-tap model is also insecure when the eavesdropper incurs as little noise as the destination. The behaviour of the above defined model following the introduction of a multi-antenna relay is to be analysed in this paper.

The generalized singular value decomposition (GSVD) will serve as a precoding technique in the model under investigation as did the singular value decomposition (SVD) for the Gaussian MIMO channel in [10]. While the SVD decomposes a system comprising a pair of sender/receiver into parallel independent sub-channels, the GSVD decomposes a system comprising one sender and two receivers. Although in [10] it has been proved that the SVD-based precoding technique achieves capacity, proving the same for the GSVD in our model is beyond the scope of this paper. GSVD precoding at the source in conjunction with SVD precoding at the relay allows for a simple derivation of the communication rates between the communicating parties as the whole system is decomposed into parallel independent channels. That being done, it becomes straightforward to transfer results from the scalar case ([8], [9]) and thus extend the proof, to the MIMO case, that a relay-assisted communication achieves secrecy when the conventional scheme fails.

The rest of the paper is organized as follows. In Section II,

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

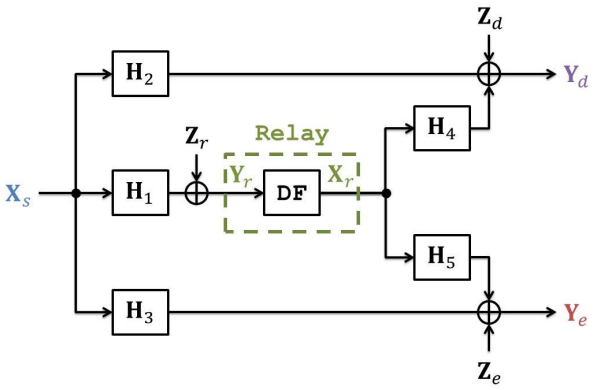

Fig. 1: System model

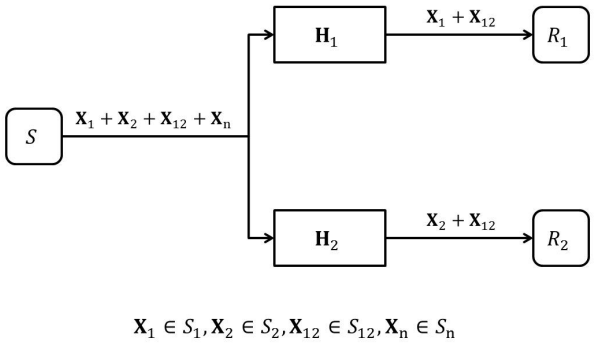

Fig. 2: GSVD-based precoding

we introduce the system model and give a brief statement about the GSVD and the secrecy capacity of the Gaussian relay wire-tap channel. Our results are derived in Section III and analysed in Section IV by computer simulations. Finally, we conclude our work in Section V.

Notations: For a given matrix $\mathbf{A}$, $\mathrm{trace}(\mathbf{A})$, $\mathrm{null}(\mathbf{A})$ and $\mathrm{rank}(\mathbf{A})$ denote the trace, the null space and the rank, respectively. The superscript $^\perp$ denotes the orthogonal complement of a subspace. Finally, $[x]^+$ is the maximum between x and 0.

II. System Model and Preliminaries

A. Channel Model

The MIMO relay wire-tap channel is depicted in Fig. 1. The source is assumed to have N_s transmit antennas. For simplicity, the relay has the same number of transmit and receive antennas, N_r. The destination as well as the passive eavesdropper are assumed to have N_d and N_e receive antennas, respectively. The relaying strategy is the decode and forward (DF) scheme. The above-defined channel can be modelled by the following system of equations:

$$\begin{aligned} \mathbf{Y}_r &= \mathbf{H}_1\mathbf{X}_s + \mathbf{Z}_r \\ \mathbf{Y}_d &= \mathbf{H}_2\mathbf{X}_s + \mathbf{H}_4\mathbf{X}_r + \mathbf{Z}_d \\ \mathbf{Y}_e &= \mathbf{H}_3\mathbf{X}_s + \mathbf{H}_5\mathbf{X}_r + \mathbf{Z}_e \end{aligned} \tag{1}$$

where

- $\mathbf{X}_i \in \mathbb{C}^{N_i \times 1}$, $\mathbf{X}_i \sim \mathcal{N}(0, \mathbf{Q}_i)$, $\mathrm{trace}(\mathbf{X}_i\mathbf{X}_i^\dagger) \leq P_i$, $i = s, r$ respectively, is the source transmit signal, relay transmit signal, respectively.
- $\mathbf{Y}_r \in \mathbb{C}^{N_r \times 1}$, $\mathbf{Y}_d \in \mathbb{C}^{N_d \times 1}$ and $\mathbf{Y}_e \in \mathbb{C}^{N_e \times 1}$ are the received signals at the relay, destination and eavesdropper nodes, respectively.
- $\mathbf{H}_1 \in \mathbb{C}^{N_r \times N_s}$, $\mathbf{H}_2 \in \mathbb{C}^{N_d \times N_s}$, $\mathbf{H}_3 \in \mathbb{C}^{N_e \times N_s}$, $\mathbf{H}_4 \in \mathbb{C}^{N_d \times N_r}$ and $\mathbf{H}_5 \in \mathbb{C}^{N_e \times N_r}$ are the complex-valued channel gain matrices as depicted in Fig. 1.
- $\mathbf{Z}_r \in \mathbb{C}^{N_r \times 1}$, $\mathbf{Z}_d \in \mathbb{C}^{N_d \times 1}$ and $\mathbf{Z}_e \in \mathbb{C}^{N_e \times 1}$ are independent complex Gaussian noise vectors with distribution $\mathcal{CN}(0, \mathbf{I}\sigma_r^2)$, $\mathcal{CN}(0, \mathbf{I}\sigma_d^2)$ and $\mathcal{CN}(0, \mathbf{I}\sigma_e^2)$, respectively.

B. Problem Statement

The source wishes to communicate with the destination. The relay takes part in the communication process by relaying data from the source to the destination. We assume the relay's channel to be less noisier than the destination's. Meanwhile, we do not exclude the case where a successful communication is feasible in the direct link (from source to destination). A question that arises here is: Why do we need a relay anyway?

To answer this question, we highlight the primary role of the relay in our model. The third legitimate party was not introduced for a primary goal to fill his traditional role [11] (to guarantee a *successful* communication when the direct link is too *noisy* to serve, alone), but to guarantee a *secure* communication when the direct link is *compromised* by eavesdropping. It has been proved that the relay assumes this new role in the scalar case [8]. Our goal here is to prove so for the MIMO case.

C. Generalized Singular Value Decomposition

Due to the use of the GSVD [12] in subsequent sections, it is convenient to introduce it, first, for a given $\mathbf{H}_1$ and $\mathbf{H}_2$ as in (1), we define the following classes of inputs

$$\begin{aligned} \mathcal{S}_1 &= \mathrm{null}(\mathbf{H}_1)^\perp \bigcap \mathrm{null}(\mathbf{H}_2) \\ \mathcal{S}_2 &= \mathrm{null}(\mathbf{H}_2)^\perp \bigcap \mathrm{null}(\mathbf{H}_1) \\ \mathcal{S}_{12} &= \mathrm{null}(\mathbf{H}_1)^\perp \bigcap \mathrm{null}(\mathbf{H}_2)^\perp \\ \mathcal{S}_n &= \mathrm{null}(\mathbf{H}_1) \bigcap \mathrm{null}(\mathbf{H}_2) \end{aligned} \tag{2}$$

Simply put, if we consider a sender S and two receivers R_1 and R_2 (with channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ of (1)) as in Fig. 2, then four independent input sets can be distinguished. $\mathcal{S}_1$ is the set of inputs that, if sent by S, lies simultaneously in the raw space of $\mathbf{H}_1$ and the null space of $\mathbf{H}_2$. $\mathcal{S}_2$ is analogous and thus straightforward to infer. $\mathcal{S}_{12}$ is the set of inputs that lies in the raw spaces of $\mathbf{H}_1$ and $\mathbf{H}_2$ simultaneously. Finally, transmitting a subset from $\mathcal{S}_n$ reaches neither R_1 nor R_2 since it lies simultaneously in the null spaces of $\mathbf{H}_1$ and $\mathbf{H}_2$. Thus, by carefully designing a codeword to be the summation of elements from the four defined sets in (2), the communication system is decomposed into parallel independent virtual channels : the private (unicast) channel to R_1, the private channel to R_2, the common (broadcast) channel to both R_1 and R_2 and the fourth channel to any receiver but R_1 and R_2. Letting $|A|$ denote the cardinality of a set A, we define $s_1 \triangleq |\mathcal{S}_1|$, $s_2 \triangleq |\mathcal{S}_2|$, $s_{12} \triangleq |\mathcal{S}_{12}|$, and $s_n \triangleq |\mathcal{S}_n|$. Intuitively,

TABLE I: s_1, s_2, s_{12}, s_n for different configurations of the full-rank pencil $(\mathbf{H}_1, \mathbf{H}_2)$

Scenario	Configuration	s_{12}	s_1	s_2	s_n
1	$N_r + N_d < N_s$	0	N_r	N_d	$N_s - (N_r + N_d)$
2	$N_r + N_d = N_s$	0	N_r	N_d	0
3	$\max(N_r, N_d) < N_s < N_r + N_d$	$(N_r + N_d) - N_s$	$N_s - N_d$	$N_s - N_r$	0
4	$N_d < N_s \leq N_r$	N_d	$N_r - N_d$	0	0
5	$N_r < N_s \leq N_d$	N_r	0	$N_d - N_r$	0
6	$N_s \leq \min(N_r, N_d)$	N_s	0	0	0

s_1, s_2 and s_{12} are the number of unicast channels to the relay, unicast channels to the destination and broadcast channels, respectively.

Definition 1. *For a given $\mathbf{H}_1$ and $\mathbf{H}_2$ as defined above, the GSVD of the pencil $(\mathbf{H}_1, \mathbf{H}_2)$ takes the form*

$$\mathbf{H}_1 = \mathbf{\Psi}_1 \mathbf{\Sigma}_1 \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{\Psi}^\dagger \quad (3)$$

$$\mathbf{H}_2 = \mathbf{\Psi}_2 \mathbf{\Sigma}_2 \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{\Psi}^\dagger \quad (4)$$

where $\mathbf{\Psi}_1 \in \mathbb{C}^{N_r \times N_r}$, $\mathbf{\Psi}_2 \in \mathbb{C}^{N_d \times N_d}$ and $\mathbf{\Psi} \in \mathbb{C}^{N_s \times N_s}$ are unitary, $\mathbf{\Omega} \in \mathbb{C}^{k\times k}$ is lower triangular and nonsingular, and

$$\mathbf{\Sigma}_1 = \begin{array}{c} \\ s_2 \\ s_{12} \\ s_1 \end{array} \begin{array}{c} \begin{array}{ccc} s_2 & s_{12} & s_1 \end{array} \\ \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{pmatrix} \end{array} \quad (5)$$

$$\mathbf{\Sigma}_2 = \begin{array}{c} \\ s_2 \\ s_{12} \\ s_1 \end{array} \begin{array}{c} \begin{array}{ccc} s_2 & s_{12} & s_1 \end{array} \\ \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D_2} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} \end{array} \quad (6)$$

are diagonal with real and strictly positive diagonal entries

$$\mathbf{D}_1 = \mathrm{diag}(r_1, \ldots, r_{s_{12}}) \quad (7)$$

$$\mathbf{D}_2 = \mathrm{diag}(e_1, \ldots, e_{s_{12}}) \quad (8)$$

To describe it in an intuitive manner, the GSVD decomposes a system comprising a sender and two receivers into parallel independent channels, which can then be encoded separately. Letting $k \triangleq \mathrm{rank}(\mathbf{H})$ with

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$$

it follows that $k = s_1 + s_2 + s_{12}$.

Table I indicates how s_1, s_2, s_{12} and s_n vary with different configurations for the full-rank pencil $(\mathbf{H}_1, \mathbf{H}_2)$, i.e the dimensions N_s, N_r and N_d. Surprisingly, the four sub-spaces does not coexist for any given configuration. Data in Table I may be represented in a more compact form as follows :

$$\begin{aligned} s_{12} &= \max\left(0, \min\left((N_r + N_d), N_s\right)\right) \\ s_1 &= N_r - s_{12} \\ s_2 &= N_d - s_{12} \\ s_n &= \max\left(0, N_s - (N_r + N_d)\right) \end{aligned}$$

For later use, we define $\mathbf{\Omega}_\mathrm{I}$ such that

$$\begin{bmatrix} \mathbf{\Omega}_{k\times k}^{-1} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \times \mathbf{\Omega}_\mathrm{I} = \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \quad (9)$$

A straightforward calculation gives

$$\mathbf{\Omega}_\mathrm{I} = \begin{bmatrix} \mathbf{\Omega}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \\ \mathbf{0}_{(N_s-k)\times k} & \mathbf{0}_{(N_s-k)\times(N_s-k)} \end{bmatrix} \quad (10)$$

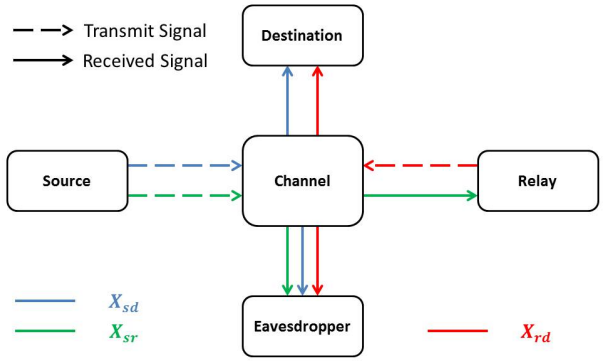

Fig. 3: Scenario 3 communication scheme

D. Lower Bound on the Secrecy Capacity for The Gaussian Relay Wire-tap Channel

A lower bound on the secrecy capacity for the Gaussian relay wire-tap channel is expressed as [9]

$$R_s \geq \left[\min\left\{I(X_s; Y_r|X_r), I(X_s, X_r; Y_d)\right\} - I(X_s, X_r; Y_e)\right]^+ \quad (11)$$

where X_s and X_r are the source and relay transmit signals. Y_r, Y_d and Y_e are the received signals at the relay, the destination and the eavesdropper, respectively.

III. Secrecy Rate for the Gaussian MIMO Relay Wire-tap Channel

In the following, we derive a lower bound on the secrecy capacity for the Gaussian MIMO relay wire-tap channel described by the system model in (1). The idea is to decompose the whole system into parallel independent channels, making it easy to transmit over interference-free virtual channels. The duration of communicating a codeword spans two time slots, with the beginning of a next communication interleaving with the end of a previous one. For that, the destination needs to split his antennas (not physically) into two groups, for the reception from the source and the relay. Following this communication scheme, only Scenario 3 and 4 arise as feasible ones. In Scenario 1 and 2, the receiver exploits all its antennas for the reception from the source. Thus, no further antennas are spared for the second time slot (reception from the relay). Hence, these two scenario are infeasible. In Scenario 5 and 6, since $s_{12} = 0$ (i.e. no private channel exists between the source and the relay), relaying cooperation can not be applied.

Due to the space limit, focus will be given only to Scenario 3. Scenario 4 is left to the extended version of this paper [13]

A. Scenario 3

The communication scheme is illustrated in Fig. 3. The source node performs a GSVD of the pencil $(\mathbf{H}_1, \mathbf{H}_2)$

$$\mathbf{H}_1 = \mathbf{\Psi}_r \mathbf{\Sigma}_r \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{\Psi}^\dagger \quad (12)$$

$$\mathbf{H}_2 = \mathbf{\Psi}_d \mathbf{\Sigma}_d \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{\Psi}^\dagger \quad (13)$$

where $k \triangleq \mathrm{rank}(\mathbf{H})$ with $\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$. The source, then chooses $\mathbf{X}_s$ as the sum of the information-bearing signals to the relay $\mathbf{X}_{sr}$ and the destination $\mathbf{X}_{sd}$

$$\begin{aligned} \mathbf{X}_{sr} &\in \mathcal{S}_1 \\ \mathbf{X}_{sd} &\in \mathcal{S}_2 \\ \mathbf{X}_s &= \mathbf{X}_{sr} + \mathbf{X}_{sd} \end{aligned} \quad (14)$$

The source pre-multiplies $\mathbf{X}_s$ by $\mathbf{\Psi\Omega}_{\mathrm{I}}$ before injecting it into the channel. The average power constraint at the sender is satisfied by

$$P_{sr} + P_{sd} \leq P_s \quad (15)$$

where

$$P_{sr} = \mathrm{trace}\left(\mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{Q}_{sr} \mathbf{\Omega}_{\mathrm{I}}^\dagger \mathbf{\Psi}^\dagger\right) \quad (16)$$

$$P_{sd} = \mathrm{trace}\left(\mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{Q}_{sd} \mathbf{\Omega}_{\mathrm{I}}^\dagger \mathbf{\Psi}^\dagger\right) \quad (17)$$

The relay node performs an SVD of $\mathbf{H}_4$,

$$\mathbf{H}_4 = \mathbf{U}_{rd} \mathbf{\Lambda}_{rd} \mathbf{V}_{rd}^\dagger \quad (18)$$

then chooses

$$\mathbf{X}_r \in \mathcal{S}_{12} \quad (19)$$

The relay pre-multiplies $\mathbf{X}_r$ by $\mathbf{V}_{rd}$ before injecting it into the channel. The average power constraint at the relay satisfies

$$\mathrm{trace}\left(\mathbf{V}_{rd} \mathbf{Q}_{rd} \mathbf{V}_{rd}^\dagger\right) \leq P_r \quad (20)$$

Combining (1), (12), (13), (14) and (18) yields

$$\begin{aligned} \mathbf{Y}_r &= \mathbf{H}_1 \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{X}_s + \mathbf{Z}_r \\ &\overset{(a)}{=} \mathbf{\Psi}_r \mathbf{\Sigma}_r \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sr} + \mathbf{Z}_d \end{aligned} \quad (21)$$

$$\begin{aligned} \mathbf{Y}_d &= \mathbf{H}_2 \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{X}_s + \mathbf{H}_4 \mathbf{V}_{rd} \mathbf{X}_r + \mathbf{Z}_r \\ &\overset{(b)}{=} \mathbf{\Psi}_d \mathbf{\Sigma}_d \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sd} + \mathbf{U}_{rd} \mathbf{\Lambda}_{rd} \mathbf{X}_r + \mathbf{Z}_d \end{aligned} \quad (22)$$

$$\begin{aligned} \mathbf{Y}_e &= \mathbf{H}_3 \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{X}_s + \mathbf{H}_5 \mathbf{V}_{rd} \mathbf{X}_r + \mathbf{Z}_e \\ &= \mathbf{H}_3 \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{X}_{sr} + \mathbf{H}_3 \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{X}_{sd} + \mathbf{H}_5 \mathbf{V}_{rd} \mathbf{X}_r + \mathbf{Z}_e \end{aligned} \quad (23)$$

In

(a) $\mathbf{X}_{sd}$ is nulled out by the relay's channel since it lies on $\mathrm{null}(\mathbf{H}_1)$.

(b) $\mathbf{X}_{sr}$ is nulled out by the destination's channel since it lies on $\mathrm{null}(\mathbf{H}_2)$.

The relay processes his received signal (21) by multiplying it by $\mathbf{\Psi}_r^\dagger$.

Since the destination receives the signals from the source and the relay over *independent* channels, (22) can be written as :

$$\mathbf{Y}_{sd} = \mathbf{\Psi}_d \mathbf{\Sigma}_d \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sd} + \mathbf{Z}_{sd} \quad (24)$$

$$\mathbf{Y}_{rd} = \mathbf{U}_{rd} \mathbf{\Lambda}_{rd} \mathbf{X}_{rd} + \mathbf{Z}_{rd} \quad (25)$$

where $\mathbf{Z}_{sd} + \mathbf{Z}_{rd} = \mathbf{Z}_d$. The destination processes his received signal in (24) ((25), respectively) by multiplying it by $\mathbf{\Psi}_d^\dagger$ ($\mathbf{U}_{rd}^\dagger$, respectively).

Then, the equations in (21), (24) and (25) become

$$\tilde{\mathbf{Y}}_r = \mathbf{\Sigma}_r \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sr} + \tilde{\mathbf{Z}}_r \quad (26)$$

$$\tilde{\mathbf{Y}}_{sd} = \mathbf{\Sigma}_d \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sd} + \tilde{\mathbf{Z}}_{sd} \quad (27)$$

$$\tilde{\mathbf{Y}}_{rd} = \mathbf{\Lambda}_{rd} \mathbf{X}_{rd} + \tilde{\mathbf{Z}}_{rd} \quad (28)$$

where $\tilde{\mathbf{Z}}_r = \mathbf{\Psi}_r^\dagger \mathbf{Z}_r$, $\tilde{\mathbf{Z}}_{sd} = \mathbf{\Psi}_d^\dagger \mathbf{Z}_{sd}$ and $\tilde{\mathbf{Z}}_{rd} = \mathbf{U}_{rd}^\dagger \mathbf{Z}_{rd}$ Summing (27) and (28) yields

$$\tilde{\mathbf{Y}}_d = \mathbf{\Sigma}_d \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \mathbf{X}_{sd} + \mathbf{\Lambda}_{rd} \mathbf{X}_{rd} + \tilde{\mathbf{Z}}_d \quad (29)$$

For the sake of clarity, we let

$$\mathbf{M}_{\mathcal{S}_n} \triangleq \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times(N_s-k)} \end{bmatrix} \quad (30)$$

Hence,

$$\tilde{\mathbf{Y}}_r = \mathbf{\Sigma}_r \mathbf{M}_{\mathcal{S}_n} \mathbf{X}_{sr} + \tilde{\mathbf{Z}}_r \quad (31)$$

$$\tilde{\mathbf{Y}}_d = \mathbf{\Sigma}_d \mathbf{M}_{\mathcal{S}_n} \mathbf{X}_{sd} + \mathbf{\Lambda}_{rd} \mathbf{X}_{rd} + \tilde{\mathbf{Z}}_d \quad (32)$$

Now secrecy capacity (11) is bounded below by

$$\begin{aligned} C_{sec}(P_s, P_r) &\geq [\min\{A, B\} - C]^+ \\ C_{sec}(P_s, P_r) &\geq [\min\{A - C, B - C\}]^+ \end{aligned} \quad (33)$$

where $A = I(\mathbf{X}_s; \mathbf{Y}_r | \mathbf{X}_r)$, $B = I(\mathbf{X}_s, \mathbf{X}_r; \mathbf{Y}_d)$ and $C = I(\mathbf{X}_s, \mathbf{X}_r; \mathbf{Y}_e)$.

Straightforward calculations result in

$$I(\mathbf{X}_s; \mathbf{Y}_r | \mathbf{X}_r) = \frac{1}{2} \log |\mathbf{I} + \mathbf{\Sigma}_r \mathbf{M}_{\mathcal{S}_n} \mathbf{Q}_{sr} \mathbf{M}_{\mathcal{S}_n}^\dagger \mathbf{\Sigma}_r^\dagger| \quad (34)$$

$$\begin{aligned} I(\mathbf{X}_s, \mathbf{X}_r; \mathbf{Y}_d) &= \frac{1}{2} \log |\mathbf{I} + \mathbf{\Sigma}_d \mathbf{M}_{\mathcal{S}_n} \mathbf{Q}_{sd} \mathbf{M}_{\mathcal{S}_n}^\dagger \mathbf{\Sigma}_d^\dagger \\ &+ \mathbf{\Lambda}_{rd} \mathbf{Q}_{rd} \mathbf{\Lambda}_{rd}^\dagger| \end{aligned} \quad (35)$$

$$I(\mathbf{X}_s, \mathbf{X}_r; \mathbf{Y}_e) = \frac{1}{2} \log |\mathbf{I} + \mathbf{S}_e| \quad (36)$$

where

$$\begin{aligned} \mathbf{S}_e &= \mathbf{H}_{se} \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{Q}_{sr} \mathbf{\Omega}_{\mathrm{I}}^\dagger \mathbf{\Psi}^\dagger \mathbf{H}_{se}^\dagger + \mathbf{H}_{se} \mathbf{\Psi\Omega}_{\mathrm{I}} \mathbf{Q}_{sd} \mathbf{\Omega}_{\mathrm{I}}^\dagger \mathbf{\Psi}^\dagger \mathbf{H}_{se}^\dagger \\ &+ \mathbf{H}_{re} \mathbf{V}_{rd} \mathbf{Q}_{rd} \mathbf{V}_{rd}^\dagger \mathbf{H}_{re}^\dagger \end{aligned} \quad (37)$$

IV. Simulation Results

In this section, we convey the secure communication performance of the proposed scheme by running two simulations. We compare our results to the MIMO wire-tap channel's, with no relay brought into play. We refer to it henceforth as the conventional model. The key to outperformance of one scheme over another is the secrecy rate achieved between the source and the destination.

In all simulations, the simulation settings in Table II are captured from situations where the conventional scheme yields secrecy rates equal to zero. To this end, the eavesdropper's channel needs to incur the same level of noise as the destination's ($\sigma_d^2 = \sigma_e^2$). Then we compute, for the same settings, the secrecy rate of our proposed scheme. We assume the relay to enjoy a better channel than the destination's ($\sigma_r^2 < \sigma_d^2$).

In Fig. 4, the achievable secrecy rates of the conventional and proposed schemes are plotted for two antenna configurations. The secrecy rates of the former remain null for all the source-destination SNR values while the latter yields positive ones. Since the destination's channel impairments are the same as

TABLE II: Simulation Settings

	Fig. 4	Fig. 5
Number of antennas		
N_s	$8, 4$	8
N_r	$6, 3$	6
N_d	$4, 2$	4
N_e	$4, 2$	4
Noise variances		
σ_r^2	1	1
σ_d^2	10	$10, 5$
σ_e^2	10	$10, 5$
Power allocation		
P_{sd}	$\frac{2}{3}P_s$	$\frac{2}{3}P_s$
P_{sr}	$\frac{1}{3}P_s$	$\frac{1}{3}P_s$
P_r	$\frac{1}{2}P_s$	
Figure axes		
x	$10\log\left(\frac{P_{sd}}{\sigma_d^2}\right)$ (dB)	$10\log\left(\frac{P_{sd}}{\sigma_d^2}\right)$ (dB)
y	(b/sec/Hz)	

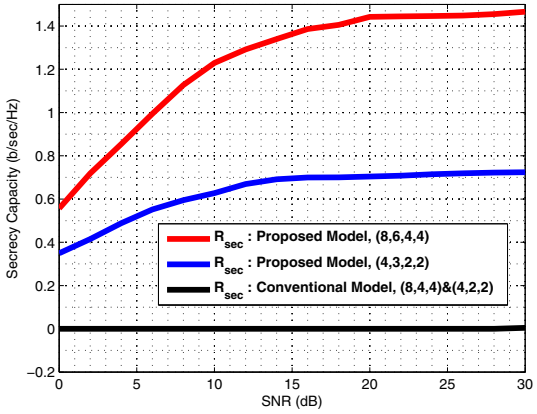

Fig. 4: Scenario 3's secrecy rate of the MIMO relay wire-tap channel and MIMO wire-tap channel, versus SNR: different antenna configurations (N_s, N_r, N_d, N_e) and (N_s, N_d, N_e)

those of the eavesdropper's ($\sigma_d^2 = \sigma_e^2$), the latter understands the channel output as much as the former does. Thus there is no rate such that a secure communication in the direct link can occur. Our scheme guarantees, thanks to the better channel that the relay enjoys, a certain secrecy rate. It is obvious that, by increasing the number of antennas for all parties, capacity increases, so does secrecy capacity. Hence the better secrecy level attained from the red curve than the blue one.

In Fig. 5, the achievable secrecy rates of the conventional and proposed schemes are plotted for two channel impairments at the destination (σ_d^2) and the eavesdropper (σ_e^2). The secrecy rates of the former remain null for all the source-destination SNR values while the latter yields positive ones. Here also, we get two secrecy levels for two noise levels at the eavesdropper. That is because the noisier the eavesdropper's channel, the

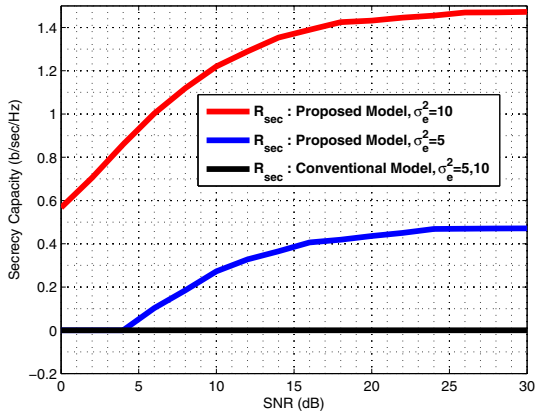

Fig. 5: Scenario 3's secrecy rate of the MIMO relay wire-tap channel and MIMO wire-tap channel, versus SNR: different noise values

better secrecy results are.

V. Conclusion

In this paper, the problem of securing a communication between a source and a destination with the help of a relay against a passive eavesdropper was considered. We referred to this model as the MIMO relay wire-tap channel for which a closed form of the secrecy rate was derived. The key step to this result was a combination of SVD and GSVD to decompose the whole system into parallel independent channels, which allowed for an easy derivation of the rates between the different parties. The proposed model outperforms the MIMO wire-tap channel with no relay assistance, when the eavesdropper's channel incurs as little noise as the destination's. This emphasizes the importance of cooperation in achieving secrecy.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 284, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wire-tap channel," *IEEE Int. Symp. on Inf. Theory*, June 2007.

[6] Y. Oohama, "Coding for relay channels with confidential messages," *IEEE Information Theory Workshop*, vol. 3, pp. 149–152, 2001.

[7] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *Information Theory, IEEE Transactions on*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[8] L. Lai and H. El Gamal, "Cooperation for secure communication: the relay wire-tap channel," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Apr. 2007.

[9] ——, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[10] E. Telatar, "Capacity of multi-antenna gaussian channels," *European Transactions on Telecommunications*, vol. 10, pp. 585–595, Dec. 1999.

[11] T. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[12] C. C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM Journal on Numerical Analysis*, vol. 18, no. 3, 1981.

[13] M. Jilani and T. Ohtsuki, "Joint svd-gsvd precoding technique and secrecy capacity lower bound for the mimo relay wire-tap channel," *submitted to IEEE Trans. Vehicular Tech.*