SECURING MULTI-ANTENNA TWO-WAY RELAY CHANNELS WITH ANALOG NETWORK CODING AGAINST EAVESDROPPERS

Amitav Mukherjee and A. Lee Swindlehurst

Dept. of Electrical Engineering & Computer Science
University of California, Irvine
Irvine, CA 92697
email: {a.mukherjee;swindle}@uci.edu

ABSTRACT

This work investigates the vulnerability of analog network coding (ANC) to physical layer attacks from adversarial users, when all nodes are equipped with multiple antennas. Specifically, we examine the MIMO two way relay channel (TWRC) with two users trying to communicate with each other via a relay node in the presence of a passive eavesdropper. We propose a new performance metric, namely the secrecy sum rate of the MIMO TWRC, to quantify performance. We then consider secure transmission strategies for the scenarios of no eavesdropper channel state information at the transmitters (ECSIT), partial ECSIT, and complete ECSIT, respectively. Finally, numerical results are presented to illustrate the improvement in secrecy obtained with the proposed transmission schemes.

1. INTRODUCTION

Network coding is an emerging design paradigm for modern communication networks that allows intermediate nodes to mix signals received from multiple paths, as opposed to the traditional approach of separating them [1]. Network coding reduces the amount of transmissions in the network and thus improves the overall throughput. While originally designed for wireline networks, attention has recently gravitated toward physical layer network coding (PLNC) for wireless networks [2]-[3].

The pre-eminent application of PLNC is in the two-way relay channel (TWRC), which consists of two source nodes that wish to establish a bidirectional communication link via a helping relay node. With PLNC, the number of time slots required to exchange messages can be reduced to just two, compared to three or greater with conventional approaches. In the first phase, both sources simultaneously transmit their messages to the relay, which resembles a multiple access channel (MAC). In the subsequent time slot, the relay broadcasts a combination of its received signals. Each source node is then able to subtract out its own data from the signal received by it and therefore recover the message from the other node. Possible choices for the relaying protocol include estimate-and-forward [3], or amplify-and-forward, which is also known as analog network coding (ANC) [4]. Early work on the TWRC mostly focused on single-antenna nodes, with some recent results on multiple antennas (MIMO) at some or all nodes in [5]-[7].

The broadcast and superposition properties of the wireless medium that make ANC feasible also makes it vulnerable to eavesdropping or jamming. However, very little existing work can be found on physical layer security aspects of TWRCs with an external adversary. In [8], the single-antenna TWRC is studied with the relay itself as the eavesdropper and the secrecy rate as the performance metric, which differs significantly from our scenario. In the remainder of this work, we investigate a MIMO TWRC with a passive multi-antenna eavesdropper. We derive a new performance metric, namely the secrecy sum rate of the MIMO TWRC, to quantify performance. We then consider secure transmission strategies for different levels of eavesdropper channel state information at the transmitters (ECSIT). The impact of eavesdropping and corresponding counter-measures have been studied extensively for unidirectional MIMO point-to-point and relay channels in [9]-[12], for example.

2. MATHEMATICAL MODEL

We study the MIMO TWRC in which four multiple-antenna nodes are present: two legitimate users A and B that wish to exchange messages, a relay R, and a passive eavesdropper E equipped with N_A, N_B, N_R, and N_E antennas respectively, with $N_R = (N_A + N_B)$.

We make the following major assumptions:

1. All four nodes operate under a half-duplex constraint, i.e., they can either transmit or receive in a given time slot.

2. There is no direct communication link between A and

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318.

B, all signals must pass through the relay R.

3. A and B have complete channel state information (CSI) of their links to/from relay R; in turn R possesses perfect CSI of its channels to/from A and B. The eavesdropper on the other hand is assumed to have complete receive channel state information.

The various levels of knowledge of the eavesdropper's channels at transmitters A, B, R include: (a) no knowledge of the eavesdropper's channel state information (ECSIT); (b) partial ECSIT in the form of the statistics of channels to E, and (c) complete (statistical and instantaneous) ECSIT. While the primary focus of this paper is on the cases of no ECSIT and complete ECSIT, we also briefly describe the partial ECSIT scenario in the sequel.

The received signal at the relay after the MAC phase can be written as

$$\mathbf{y}_R = \mathbf{H}_A\mathbf{x}_A + \mathbf{H}_B\mathbf{x}_B + \mathbf{n}_R, \quad (1)$$

where $\mathbf{H}_A \in \mathbb{C}^{N_R\times N_A}$ and $\mathbf{H}_B \in \mathbb{C}^{N_R\times N_B}$ are the flat-fading channels from users A and B with transmit signals $\mathbf{x}_A \in \mathbb{C}^{N_A\times 1}, \mathbf{x}_B \in \mathbb{C}^{N_B\times 1}$, respectively, and $\mathbf{n}_R$ is the zero-mean complex Gaussian interference-plus-noise vector with covariance $\sigma_n^2\mathbf{I}$.

The design of the relay signal in the broadcast phase is an area of intensive research. The term physical-layer network coding was originally used to refer to a estimate-and-forward scheme at the relay [3], while an amplify-and-forward strategy was termed analog network coding (ANC) in [4]. The lower complexity of ANC due to its linear processing and avoidance of multiuser decoding makes it the relaying strategy of choice in the remainder of this work.

The received signals at the terminals in the BC phase (time slot 2) can be written as

$$\mathbf{y}_i = \mathbf{G}_i\mathbf{x}_R + \mathbf{n}_i, i = \mathsf{A}, \mathsf{B}, \mathsf{E},$$

where $\mathbf{x}_R \in \mathbb{C}^{N_R\times 1}$ is the relay signal, $\mathbf{G}_i$ is the MIMO fading channel from the relay to the i^{th} receiver, and $\mathbf{n}_i$ is the corresponding complex Gaussian noise-plus-interference vector analogous to the definition in (1). All channels and noise vectors are assumed to be uncorrelated temporally and across users in both time slots. Let the transmit signals in either phase have the following covariance matrices and transmit power constraints:

$$\begin{aligned} E\left\{\mathbf{x}_i\mathbf{x}_i^H\right\} &= \mathbf{Q}_i \quad (2)\\ \mathrm{trace}\left(\mathbf{Q}_i\right) &\leqslant P_i, i = \mathsf{A}, \mathsf{B}, \mathsf{R}. \quad (3)\end{aligned}$$

For the conventional ANC protocol based on the amplify-and-forward principle, the relay signal is

$$\mathbf{x}_R = \sqrt{g}\mathbf{W}\mathbf{y}_R, \quad (4)$$

where $\mathbf{W}$ is a $N_R \times N_R$ precoding matrix known to *all* receivers, and g is a scaling factor used to conform to the relay transmit power constraint:

$$g \leq \frac{P_R}{\mathrm{trace}\left\{\mathbf{W}\left(\mathbf{H}_A\mathbf{Q}_A\mathbf{H}_A^H + \mathbf{H}_B\mathbf{Q}_B\mathbf{H}_B^H + \mathbf{Z}_R\right)\mathbf{W}^H\right\}}.$$

The design of the relay precoding matrix $\mathbf{W}$ is one of the major components of the ANC scheme. Evidently, the simplest strategy is to apply $\mathbf{W} = \mathbf{I}$. A more efficient use of the multiple antennas at the relay would be to optimize $\mathbf{W}$ in order to maximize the TWRC sum rate [14], or another performance metric of choice.

Assuming perfect self-interference cancelation at A and B leads to the following effective received signals in time slot 2:

$$\begin{aligned} \hat{\mathbf{y}}_A &= \sqrt{g}\mathbf{G}_A\mathbf{W}\mathbf{H}_B\mathbf{x}_B + \sqrt{g}\mathbf{G}_A\mathbf{W}\mathbf{n}_R + \mathbf{n}_A \quad (5)\\ \hat{\mathbf{y}}_B &= \sqrt{g}\mathbf{G}_B\mathbf{W}\mathbf{H}_A\mathbf{x}_A + \sqrt{g}\mathbf{G}_B\mathbf{W}\mathbf{n}_R + \mathbf{n}_B \quad (6)\end{aligned}$$

Let the interference-plus-noise covariance matrix at each legitimate receiver be defined as $\mathbf{K}_i = \sigma_n^2 g\mathbf{G}_i\mathbf{W}\mathbf{W}^H\mathbf{G}_i^H + \mathbf{Z}_i, i = \mathsf{A}, \mathsf{B}$.

2.1. Performance Metric

The information rate achieved by each end user over two time slots is

$$\begin{aligned} R_A &= I\left(\hat{\mathbf{y}}_A; \mathbf{x}_B\right) \quad (7)\\ &= \log_2\frac{\left|\mathbf{K}_A + g\mathbf{G}_A\mathbf{W}\mathbf{H}_B\mathbf{Q}_B\mathbf{H}_B^H\mathbf{W}^H\mathbf{G}_A^H\right|}{\left|\mathbf{K}_A\right|}, \quad (8)\end{aligned}$$

$$\begin{aligned} R_B &= I\left(\hat{\mathbf{y}}_B; \mathbf{x}_A\right) \quad (9)\\ &= \log_2\frac{\left|\mathbf{K}_B + g\mathbf{G}_B\mathbf{W}\mathbf{H}_A\mathbf{Q}_A\mathbf{H}_A^H\mathbf{W}^H\mathbf{G}_B^H\right|}{\left|\mathbf{K}_B\right|} \quad (10)\end{aligned}$$

where $I(x;y)$ denotes the mutual information between x and y. The conventional sum rate (without security considerations) of the MIMO two-way relay channel can then be written as

$$R_s = \frac{1}{2}\left(R_A + R_B\right), \quad (11)$$

where the factor of $1/2$ represents the rate loss due to the half-duplex constraint.

Next, we model the adversary as an omniscient eavesdropper, with complete knowledge of all user channels and the relay precoding matrix. Each transmission phase in the current model grants an external eavesdropper an opportunity to overhear the transmitted information, whereas the legitimate receivers obtain a single observation of the data. The optimal strategy at the eavesdropper would be to combine the information received over the two phases to create a single effective MIMO-MAC, as shown next.

Let the signals received by the eavesdropper in phases 1 and 2 be

$$\begin{aligned} \mathbf{z}_1 &= \mathbf{C}_A\mathbf{x}_A + \mathbf{C}_B\mathbf{x}_B + \mathbf{m}_E \\ \mathbf{z}_2 &= \sqrt{g}\mathbf{G}_E\mathbf{W}\mathbf{y}_R + \mathbf{n}_E \end{aligned} \tag{12}$$

with MIMO channels $\mathbf{C}_A, \mathbf{C}_B$ from sources A and B, and $\mathbf{G}_E$ from relay R, respectively. Concatenating the above yields the effective MAC $\tilde{\mathbf{z}} = \left[\begin{array}{cc} \mathbf{z}_1^T & \mathbf{z}_2^T \end{array} \right]^T$. Define the effective channels from the sources to the eavesdropper as

$$\tilde{\mathbf{C}}_i = \left[\begin{array}{c} \mathbf{C}_i \\ \sqrt{g}\mathbf{G}_E\mathbf{W}\mathbf{H}_i \end{array} \right], i = \mathsf{A}, \mathsf{B}.$$

Similarly, define the effective interference-plus-noise vector at the eavesdropper as $\tilde{\mathbf{n}}_E = \left[\begin{array}{cc} \mathbf{m}_E^T & \mathbf{n}_E^T \end{array} \right]^T$, where $\tilde{\mathbf{n}}_E \in \mathbb{C}^{2N_R\times 1}$ is zero-mean complex Gaussian with block-diagonal covariance matrix $\mathbf{K}_E$.

The information rate leaked to the eavesdropper can then be computed from the sum capacity of the MIMO MAC [15] to be

$$R_e = \log_2 \frac{\left| \mathbf{K}_E + \sum_{i=A,B} \tilde{\mathbf{C}}_i\mathbf{Q}_i\tilde{\mathbf{C}}_i^H \right|}{|\mathbf{K}_E|}. \tag{13}$$

The capacity region of the MIMO TWRC with ANC is currently unknown. A viable alternative performance measure is the secrecy sum rate, which has been derived for multiuser networks in [13], for example. Therefore, we obtain the desired performance metric for the MIMO TWRC under eavesdropping, denoted as the instantaneous *network secrecy sum rate*, as

$$\begin{aligned} R_{sec} &= \sum_{i=A,B} \left[I\left(\hat{\mathbf{y}}_i;\mathbf{x}_i\right) - I\left(\tilde{\mathbf{z}};\mathbf{x}_i\right) \right] & (14) \\ &= \max\left[0, \left(R_s - R_e\right)\right]. & (15) \end{aligned}$$

3. NO EAVESDROPPER CSIT

We first investigate the TWRC without knowledge of the eavesdropper's instantaneous channels $\mathbf{C}_A, \mathbf{C}_B, \mathbf{G}_E$ at the transmitting nodes. When multiple antennas are available at the transmitting nodes, it is possible to transmit an artificial interference signal(s) on some of the spatial dimensions along with the information signals on the remainder. By transmitting the artificial interference in the orthogonal space of the channels of the legitimate destination(s) in either phase, only the eavesdropper is jammed while the receivers remain unaffected. Jamming potential eavesdroppers with artificial interference has been previously proposed for unidirectional point-to-point MIMO wiretap channels in [9]-[10].

Next, we describe the artificial interference scheme for transmitter A, with the same principle being true for transmitter B.In this case, the transmitters allocate sufficient resources to guarantee a minimum conventional sum rate criterion $R_{s,min}$ that is known to all of them.

MAC Phase: A's signal is split into two components, the secret message for B, denoted by the $D_A \times 1$ vector $\mathbf{z}_A$, and an uncorrelated $(N_A - D_A) \times 1$ interference signal vector $\mathbf{z}'_A$. Let $0 < \rho_A \leq 1$ denote the fraction of the total available power devoted to $\mathbf{z}_A$, and let $\mathbf{T}_A, \mathbf{T}'_A$ represent the $N_A \times D_A$ and $N_A \times (N_A - D_A)$ transmit beamformer matrices corresponding to $\mathbf{z}_A$ and $\mathbf{z}'_A$:

$$\mathbf{x}_A = \mathbf{T}_A\mathbf{z}_A + \mathbf{T}'_A\mathbf{z}'_A. \tag{16}$$

The elements of $\mathbf{z}_A$ are assumed to be uncorrelated, and the vectors $\mathbf{z}_A$ and $\mathbf{z}'_A$ are uncorrelated with each other as well. Thus, $\mathbf{Q}_A$ may be expressed as

$$\mathbf{Q}_A = \mathbf{T}_A\mathbf{Q}_{zA}\mathbf{T}_A^H + \mathbf{T}'_A\mathbf{Q}'_z\left(\mathbf{T}'_A\right)^H, \tag{17}$$

where $\mathbf{Q}_{zA}, \mathbf{Q}'_{zA}$ are covariance matrices associated with $\mathbf{z}_A$ and $\mathbf{z}'_A$, respectively, such that $\mathrm{Tr}(\mathbf{T}_A\mathbf{Q}_{zA}\mathbf{T}_A^H) \leq \rho_A P_A$, and $\mathrm{Tr}(\mathbf{T}'_A\mathbf{Q}'_{zA}\mathbf{T}'^H_A) \leq (1-\rho_A)P_A$.

With $\rho_A, \mathbf{Q}_{zA}, N$ and $\mathbf{T}_A$ specified as above, it remains to allocate the interference power so that it does not degrade R's signal. To guarantee this, we require

$$\mathbf{H}_A\mathbf{T}_A\mathbf{z}_A \perp \mathbf{H}_A\mathbf{T}'_A\mathbf{z}'_A \tag{18}$$

for all possible $\mathbf{z}$, which can be guaranteed by choosing $\mathbf{T}$ to be the dominant D_A right singular vectors of H_A, for example. A similar procedure applies for transmission of artificial interference by B in the first phase:

$$\mathbf{x}_B = \mathbf{T}_B\mathbf{z}_B + \mathbf{T}'_B\mathbf{z}'_B. \tag{19}$$

To increase the spatial dimensions available for artificial interference, we adopt the modified waterfilling approach of [10], where the product of power and spatial channels is minimized under a pre-selected rate constraint.

BC Phase: Given that the sum rate constraint $R_{s,min}$ is feasible in the second phase, it is desirable that R allocate any remaining resources to generate artificial interference as well. The relay signal is written as

$$\mathbf{x}_R = \sqrt{g}\mathbf{W}\mathbf{y}_R + \mathbf{z}'_R \tag{20}$$

where $\mathbf{z}'_R$ is the artificial interference transmitted in the second phase.

To avoid jamming the legitimate receivers, we require

$$\mathbf{z}'_R \perp \left[\begin{array}{cc} \mathbf{G}_A^H\mathbf{G}_A\mathbf{W}\mathbf{H}_B\mathbf{T}_B & \mathbf{G}_B^H\mathbf{G}_B\mathbf{W}\mathbf{H}_A\mathbf{T}_A \end{array} \right]. \tag{21}$$

Since we have $N_R = (N_A + N_B) \geqslant (D_A + D_B)$, the existence of an artificial interference signal which satisfies the orthogonality requirement in (21) is guaranteed.

At the eavesdropper, the effective noise covariance including the artificial interference can be represented as

$$\mathbf{K}_E = \left(\begin{array}{cc} E\left\{\mathbf{m}_E\mathbf{m}_E^H\right\} & \mathbf{0} \\ \mathbf{0} & E\left\{\mathbf{n}_E\mathbf{n}_E^H\right\} \end{array} \right)$$

where $E\left\{\mathbf{m}_E\mathbf{m}_E^H\right\} = \sum_{i=A,B} \left(\frac{1-\rho_i}{N'_i}\right) P_i\mathbf{C}_i\mathbf{T}_i\mathbf{T}_i^H\mathbf{C}_i^H + \mathbf{I}$, and $E\left\{\mathbf{n}_E\mathbf{n}_E^H\right\} = \left(\frac{1-\rho_R}{N'_R}\right) P_R\mathbf{G}_E\mathbf{T}_R\mathbf{T}_R^H\mathbf{G}_E^H + \mathbf{I}$.

4. COMPLETE EAVESDROPPER CSIT

We now examine the MIMO TWRC where A, B, and R possess complete (instantaneous and statistical) information regarding the eavesdropper's channels in the relevant time slots. In the second phase, the relay can attempt to design the precoding matrix $\mathbf{W}$ in order to maximize the conventional sum rate R_s:

$$\mathbf{W}^{opt} = \arg\max_{\mathbf{W}} R_{\text{sec}}. \quad (22)$$

From (14) we observe that the objective function is a difference of two concave functions, and therefore is neither convex nor concave. As a result, (22) is an unconstrained non-convex optimization problem, for which a numerical solution technique must be adopted. Some example approaches include the steepest or gradient descent method, which iteratively searches for a locally optimum solution in the direction of the gradient of R_{sec}. However, a globally optimal solution cannot be guaranteed for any such method.

Alternatively, a more intuitive approach based upon the generalized singular value decomposition (GSVD) can be adopted instead. For the point-to-point MIMO wiretap channel, the use of artificial interference is known to be suboptimal when complete ECSIT is available. Indeed, in the high SNR regime, it can be shown that the optimal strategy is to simultaneously diagonalize the main and eavesdropper channels with the aid of the GSVD [11]. In this section, we demonstrate how to extend this strategy to the MIMO TWRC by exploiting the self-interference cancelation feature intrinsic to the network.

MAC Phase: We describe the GSVD-based strategy for A, with the same principle being true for B. For the pair of channels $\mathbf{H}_A, \mathbf{C}_A$ from A to R, E, we define the GSVD as

$$\mathbf{U}^H \mathbf{H}_A \mathbf{Q} = \mathbf{\Sigma}_A, \quad \mathbf{V}^H \mathbf{C}_A \mathbf{Q} = \mathbf{\Sigma}_E$$

where

$$\mathbf{\Sigma}_A = \begin{pmatrix} \mathbf{0} & \\ & \mathbf{D}_A \end{pmatrix}, \quad \mathbf{\Sigma}_E = \begin{pmatrix} \mathbf{I} & \\ & \mathbf{D}_E \\ & \mathbf{0} \end{pmatrix}$$

and $\mathbf{D}_A = diag\{r_1, \ldots, r_s\}, \mathbf{D}_E = diag\{e_1, \ldots, e_s\}$ are diagonal matrices with positive elements. Let the (ordered) generalized singular values then be defined as $\alpha_i = \frac{r_i}{e_i}, i = 1, \ldots, s$.

Transmitter A constructs its transmit signal as

$$\mathbf{x}_A = \mathbf{Q} \begin{bmatrix} \mathbf{0} \\ \mathbf{u}_A \end{bmatrix}$$

where $\mathbf{u}_A \in \mathbb{C}^{s \times 1}$ is the Gaussian input with non-zero elements corresponding to generalized singular values greater than unity.

BC Phase: The re-application of the GSVD strategy to the BC phase is made possible by the self-interference cancelation at each receiver. In other words, even though the receivers do not cooperate, we can concatenate the channels into $\tilde{\mathbf{G}} = \begin{bmatrix} \mathbf{G}_A; & \mathbf{G}_B \end{bmatrix}$ and treat A and B as a single multi-antenna receiver due to the lack of any mutual interference. Therefore, R computes the relay signal based on the GSVD of the pair $\left\{\tilde{\mathbf{G}}, \mathbf{G}_E\right\}$.

4.1. Partial ECSIT

If the joint distribution of the eavesdropper's channels is known at the transmitters, then it is theoretically possible to maximize the ergodic network secrecy sum rate based on artificial interference as

$$\max_{\rho_A, \rho_B, \rho_R, D_A, D_B, D_R} \mathcal{E}\left\{R_{sec}\right\}. \quad (23)$$

where the expectation is taken over all the random inter-user channels. For simplicity, assume uniform power allocation at all transmitters, i.e., the information and artificial interference covariances are scaled identity matrices with the appropriate trace constraint. It is then straightforward to apply known results from random matrix theory and derive the expected value of R_{sec} in terms of the random eigenvalues of Wishart matrices. However, a joint optimization over all six parameters for the non-convex objective function in (23) would entail great complexity, and sub-optimal approaches with a predetermined power allocation may be more suitable.

5. NUMERICAL RESULTS

In this section, we present some numerical examples to illustrate the effectiveness of the proposed secure transmission strategies. For comparison, we refer to the sum rate maximizing ANC scheme without eavesdropping counter-measures in (4) as the *naive* scheme, which also includes uniform power allocation over the transmit antennas of A and B.

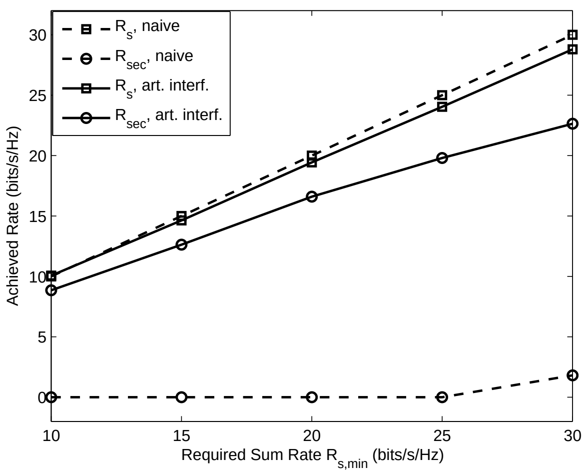

Fig. 1. TWRC network secrecy sum rate without ECSIT.

Fig. 1 compares the naive and no ECSIT ANC schemes as a function of the minimum desired conventional sum rate $R_{s,min}$, for $N_A = N_B = 6, N_R = 12, N_E = 2$. Here, SNR is defined as the total transmit power of A, set equal to the power at B and R, i.e., $P_A = P_B = P_R = 20dB$. The per-user minimum rate requirement in the BC phase is set to half the overall sum rate constraint $R_{s,min}$ for simplicity. It is apparent that an eavesdropper with even a fraction of the antennas of the the legitimate nodes can severely compromise the confidentiality of the MIMO TWRC. The artificial interference scheme offers a substantial improvement in secrecy, albeit with increased power usage, especially at low values of $R_{s,min}$.

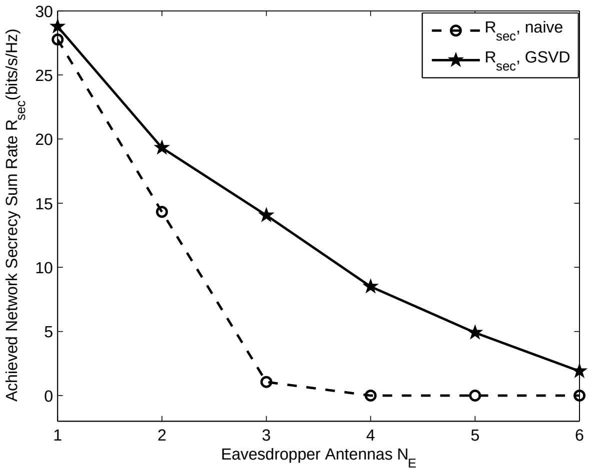

Fig. 2. TWRC network secrecy sum rate with complete ECSIT.

We compare the improvements in network secrecy sum rate when complete ECSIT is available as the number of eavesdropper antennas increases, for fixed $N_A = N_B = 8, N_R = 16$ and $P_A = P_B = P_R = 20dB$. Exploiting the ECSIT allows the MIMO TWRC to transmit with a non-zero secrecy sum rate for twice as many eavesdropper antennas compared to the naive scheme.

6. REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.

[2] Y. Wu, P. A. Chou, and S.-Y. Kung, "Information exchange in wireless networks with network coding and physical-layer broadcast," *Proc. 39th Annual Conf. Inf. Sciences and Systems (CISS)*, Mar. 2005.

[3] S. Zhang, S.-C. Liew, and P. P. Lam, "Physical-layer network coding," *Proc. IEEE MobiComm*, pp.358-365, 2006.

[4] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," *Proc. ACM SIGCOMM*, Aug. 2007.

[5] I. Hammerstrom, M. Kuhn, C. Esli, J. Zhao, A. Wittneben, and G. Bauch, "MIMO two-way relaying with transmit CSI at the relay," *Proc. IEEE SPAWC*, Jun. 2007.

[6] Y. C. Liang and R. Zhang, "Optimal analogue relaying with multi-antennas for physical layer network coding," *Proc. IEEE ICC*, pp. 3893-3897, May 2008.

[7] R. Zhang, C. Chai, Y. C. Liang, and S. Cui, "On capacity region of two-way multi-antenna relay channel with analogue network coding," *Proc. IEEE ICC*, June 2009.

[8] X. He and A. Yener, "The role of feedback in two-way secure communications," [Online]. Available at http://arxiv.org/abs/0911.4432

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[10] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," *Proc. IEEE SPAWC*, pp. 344-348, Perugia, June 2009.

[11] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," 2008. [Online]. Available at http://www.rle.mit.edu/sia/.

[12] K. T. Gowda, T. Q.S. Quek, and H. Shin, "Secure diversity-multiplexing tradeoffs in MIMO relay channels," *Proc. ISIT*, pp. 1433-1437, Seoul, July 2009.

[13] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, June 2008.

[14] K.-J. Lee, K. W. Lee, H. Sung, and I. Lee, "Sum-rate maximization for two-way MIMO amplify-and-forward relaying systems," *Proc. Veh. Tech. Conf.*, Barcelona, April 2009.

[15] A. Soysal and S. Ulukus, "Asymptotic optimality of beamforming in multi-user MIMO-MAC with no or partial CSI at the transmitters," *Proc. Veh. Tech. Conf.*, pp. 1619-1623, June 2005.