Secrecy Capacity of GSVD MIMOME Systems in the Presence of CSI Attacks

André S. Guerreiro, Gustavo Fraidenraich and Richard Demo Souza.

***Abstract*— We consider the transmission of confidential information over a multiple-input multiple-output multiple-eavesdropper (MIMOME) wireless channel, in which an active eavesdropper is able to attack the channel sounding process through intelligent jamming. We focus on transmission systems based on generalized singular value decomposition (GSVD). We propose and analyze, through computer simulations, the efficiency of several attack techniques that intend to disrupt the secret communication between legitimate users.**

***Keywords*— Channel sounding, GSVD, jamming, MIMOME channel, secrecy capacity**

I. Introduction

The broadcast nature of the wireless channel makes it very susceptible to eavesdropping, making the security of the transmitted information very critical. Recent information-theoretic researches have focused on improving communication security through the physical layer. Shannon [1] introduced the concept of perfect secrecy, which requires the mutual information between the source and the eavesdropper to be null and implies that the eavesdropper is not able to obtain any information. Wyner [2] introduced the wire-tap channel, a physical layer model to analyze the transmission of secret information through a wired Gaussian channel. Wyner's work showed that when the eavesdropper's channel is a degraded version of the main channel, there is a positive secrecy rate (which is defined as a transmission rate that respects perfect secrecy).

The work in [2] was later expanded by Csiszar and Korner [3] for the non-degraded broadcast channel, where the secrecy capacity was defined as the maximum secrecy rate. Determination of the secrecy capacity for the MIMO wiretap channel was addressed by Oggier in [4] assuming the transmitter has full channel state information (CSI) of all channels, and the characterization of the input covariance matrix that achieves secrecy capacity was studied in [5]. For the generalized singular value decompostion (GSVD) based transmission systems, a closed-form expression for the input covariance matrix that achieves secrecy capacity was determined in [6], assuming full CSI at the transmitter. Whether to improve or to disrupt secret communication, several studies were made on the potentials and threats of jamming. In [7], it was shown how secrecy can be achieved by adding artificially generated noise to the transmitted signal, and in [8] optimal jamming strategies for a full-duplex active eavesdropper was presented.

This work was partially supported by Capes and CNPq, Brazil

A. Guerreiro and G. Fraidenraich are with the Departament of Communications, State University of Campinas (Unicamp). R. D. Souza is with the Electronics Department (DAELN), Federal University of Technology - Parana (UTFPR)

In this paper, we analyze the transmission of a secret message in a MIMOME channel. In this model there are three terminals, a transmitter, an eavesdropper and an legitimate receiver (for simplicity we will refer to it just as receiver throughout this paper), each of them has an arbitrary number of antennas. We are inspired by [9], where Miller and Trappe considered a smart jammer, attacking the channel sounding process to disrupt communication between two legitimate users with multiple antennas. In a similar way, we consider an active eavesdropper (an eavesdropper that is able to observe the communication medium as well as modify its contents), which attacks the main channel sounding process (channel estimation between the transmitter and receiver, as the smart jammer in [9]) and is also able to manipulate the channel estimation between the eavesdropper and the transmitter (eavesdropper's channel sounding). The main difference between our work and [9] relies on the goal of the intelligent adversary. Our active eavesdropper acts on the sounding processes mainly to facilitate eavesdropping. By attacking only the channel sounding process, the eavesdropper easily satisfies a power constraint, as this process typically only occupies a fraction of the transmission time. Moreover, we introduce some specific attack strategies and evaluate their efficiency through computer simulations.

We begin in Section II by describing the system model, while Section III describes the channel sounding process. Section IV introduces the characteristics of some ideal and practical attacks, which are then investigated in Sections V and VI, respectively. Finally, Section VII concludes the paper.

II. System Model

This section is divided into three. In the first subsection, we provide a mathematical model for the channels, in the second subsection we present the GSVD and describe a GSVD based transmission system, and in the last subsection we discuss the secrecy capacity under the conditions stated before.

A. Channel model

Using n_t, n_e, and n_r to denote the number of antennas at the transmitter, eavesdropper and receiver, respectively, the received signals, $\mathbf{Y}$ and $\mathbf{Z}$, at the receiver and eavesdropper at a certain coherence period are, respectively

$$\mathbf{Y} = \mathbf{H}_m\mathbf{X} + \mathbf{V}_m, \tag{1}$$

$$\mathbf{Z} = \mathbf{H}_e\mathbf{X} + \mathbf{V}_e, \tag{2}$$

where matrix $\mathbf{X}$ $(n_t \times 1)$ represents the transmitted signal, $\mathbf{V}_m \in \mathbb{C}^{n_r \times 1}$ and $\mathbf{V}_e \in \mathbb{C}^{n_e \times 1}$ are additive zero mean complex Gaussian white noise vectors (AWGN) at the receiver and

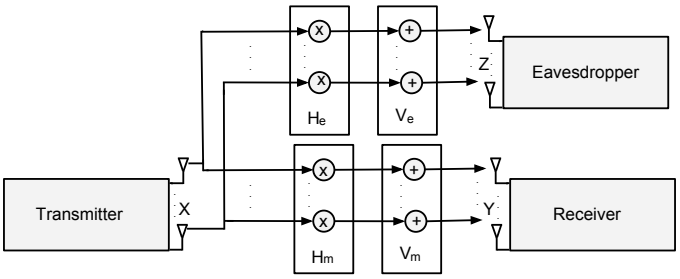

Fig. 1. Multiple input, multiple output, multiple eavesdropper (MIMOME) channel model

eavesdropper, respectively, with i.i.d entries with covariance matrix given by $\mathcal{CN}(0, \mathbf{I}N_0)$. The matrices $\mathbf{H}_m \in \mathbb{C}^{n_r \times n_t}$ and $\mathbf{H}_e \in \mathbb{C}^{n_e \times n_t}$ represent the channel gains associated with the main channel and the eavesdropper's channel, respectively. The channels are considered to be flat, quasi-static Rayleigh distributed. Figure 1 illustrates the above model.

B. GSVD Transmission

In GSVD based transmission systems, the transmitter has full CSI of the main channel and the eavesdropper's channel, and therefore uses GSVD beamforming [10], [11]. Although the assumption of full eavesdropper's CSI at the transmitter is unrealistic when the eavesdropper is a covert adversary, it is valid if the eavesdropper is a regular user within the network, such as in a time division multiple access environments.

Given the matrices $\mathbf{H}_m$ and $\mathbf{H}_e$ described before, the operation GSVD$(\mathbf{H}_m, \mathbf{H}_e)$ provides the matrices $\mathbf{\Psi}_m$, $\mathbf{\Psi}_e$, $\mathbf{C}$, $\mathbf{D}$ and $\mathbf{A}$ such that

$$\mathbf{H}_m = \mathbf{\Psi}_m \mathbf{C} \mathbf{A}^{-1}, \tag{3}$$

$$\mathbf{H}_e = \mathbf{\Psi}_e \mathbf{D} \mathbf{A}^{-1}, \tag{4}$$

where $\mathbf{\Psi}_m \in \mathbb{C}^{n_r \times n_r}$ and $\mathbf{\Psi}_e \in \mathbb{C}^{n_e \times n_e}$ are unitary matrices, $\mathbf{C} \in \mathbb{C}^{n_r \times q}$ and $\mathbf{D} \in \mathbb{C}^{n_e \times q}$ are non-negative diagonal matrices, and $\mathbf{A} \in \mathbb{C}^{n_t \times q}$, where $q = \min(n_t, n_e + n_r)$. Also

$$\mathbf{C}^T \mathbf{C} + \mathbf{D}^T \mathbf{D} = \mathbf{I}, \tag{5}$$

where operator $(.)^T$ is the transpose. The diagonal elements of $\mathbf{C}$ are called the generalized singular values. The transmitter precodes message $\mathbf{X}$ by multiplying it by matrix $\mathbf{A}$:

$$\mathbf{X}_t = \mathbf{A}\mathbf{X}. \tag{6}$$

Therefore, the signals received at the receiver and eavesdropper are given, respectively, by

$$\mathbf{Y} = \mathbf{\Psi}_m \mathbf{C} \mathbf{A^{-1}} \mathbf{X}_t + \mathbf{V}_m = \mathbf{\Psi}_m \mathbf{C} \mathbf{X} + \mathbf{V}_m, \tag{7}$$

$$\mathbf{Z} = \mathbf{\Psi}_e \mathbf{D} \mathbf{A^{-1}} \mathbf{X}_t + \mathbf{V}_e = \mathbf{\Psi}_e \mathbf{D} \mathbf{X} + \mathbf{V}_e. \tag{8}$$

The covariance matrix of $\mathbf{X}_t$ is $\mathbf{K_{xt}} = \mathbf{A P A^H}$, where operator $(.)^H$ is the Hermitian transpose. Since $\mathbf{C}$ and $\mathbf{D}$ are diagonal matrices, applying GSVD decomposition creates a set of parallel independent sub-channels between the transmitter and receiver and between the transmitter and eavesdropper.

C. Secrecy Capacity

The secrecy capacity for MIMO systems is given by [4]

$$\mathcal{C}_s = \max_{\mathbf{P} \succeq 0} (\log\det(\mathbf{I} + \mathbf{H_m} \mathbf{K}_{xt} \mathbf{H}_m^{\mathbf{H}}) - \log\det(\mathbf{I} + \mathbf{H}_e \mathbf{K}_{xt} \mathbf{H}_e^{\mathbf{H}})). \tag{9}$$

Specifically for GSVD based systems, we may decompose matrices $\mathbf{H}_m$ and $\mathbf{H_e}$ as in (3) and (4) in order to obtain

$$\begin{aligned} \mathcal{C}_s = \max_{\mathbf{P} \succeq 0} \{ & \log\det(\mathbf{I} + \mathbf{\Psi}_m \mathbf{C} \mathbf{P} \mathbf{C}^T \mathbf{\Psi}_m^H) \\ & - \log\det(\mathbf{I} + \mathbf{\Psi}_e \mathbf{D} \mathbf{P} \mathbf{D}^T \mathbf{\Psi}_e^H) \}, \end{aligned} \tag{10}$$

where $\mathbf{P}$ is the matrix whose entries define the power allocation amount antennas. However, (10) does not specify which matrix $\mathbf{P}$ should be used to achieve the secrecy capacity. The power allocation strategy described in [6] is assumed in this paper, since it was proved to achieve the secrecy capacity in MIMO GSVD systems. We denote by $\mathbf{P}^*$ the matrix that maximizes (10), and its diagonal elements can be calculated as

$$p_i^* = \begin{cases} \max\left(0, \frac{-1 + \sqrt{1 - 4c_i d_i + 4(c_i - d_i) c_i d_i / (\mu a_i)}}{2 c_i d_i}\right) & \text{if} \quad c_i > d_i \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

where p_i^*, c_i, d_i and a_i are the i-th diagonal entries of the matrices $\mathbf{P}^*$, $\mathbf{C}^T\mathbf{C}$, $\mathbf{D}^T\mathbf{D}$, and $\mathbf{A}^H\mathbf{A}$. The constant $\mu > 0$ is the Lagrangian parameter. The system is also subject to

$$\text{Tr}(\mathbf{A}^H \mathbf{A} \mathbf{P}) \leq p \tag{12}$$

where p is the total power constraint, and $Tr(.)$ is the trace.

Since $\mathbf{C}$ and $\mathbf{D}$ are diagonal matrices, applying (5), we may further simplify (10) to obtain

$$\mathcal{C}_s = \sum_{i=1}^{q} \log(1 + p_i^* c_i) - \log(1 + p_i^* - p_i^* c_i). \tag{13}$$

III. Channel sounding process

Sounding is the process of channel estimation. The transmitter sends a training sequence and based on this sequence the receiver or the eavesdropper estimates the channel. The sounding process of the main channel and the eavesdropper channel are performed at distinct moments, but in a similar fashion. We consider that the transmitter uses a time-division multiplexing scheme where a pilot tone is transmitted in each of the antennas, one at a time. The receiver (or eavesdropper, depending on which channel is being estimated) also receives the pilots with a single antenna, and estimates the gain between these two. By cycling through all the combinations of transmit/receive pairs of antennas, we are able to obtain an estimate for the whole MIMO channel, i.e., $\mathbf{H_m}$ and $\mathbf{H_e}$.

During the main channel sounding process, the eavesdropper may corrupt each gain estimate in an independent way (since each gain estimate is done in separate moments) by adding jamming signals to the pilots. After the receiver obtains the corrupted estimates of the main channel, it feeds them back to the transmitter. We consider the feedback channel to be error free. Moreover, we represent the corrupted main channel estimate at the transmitter as $\mathbf{H}'_m$. Figure 2 illustrates the process of jamming the received signal at the receiver. It is

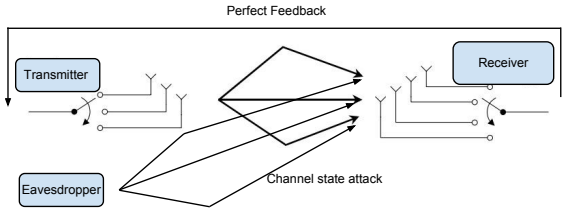

Fig. 2. Jamming the main channel estimation process

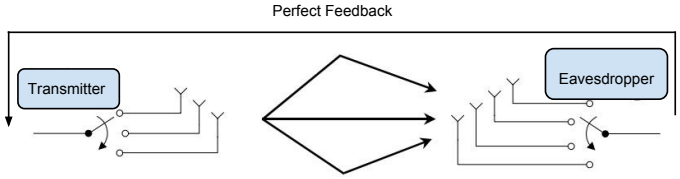

Fig. 3. Corrupted eavesdropper's channel estimation process

important to note that the attack occurs only at the process of channel estimation, but the data transmission is not attacked.

During the sounding process of the eavesdropper channel, after receiving the pilots from the transmitter the eavesdropper feeds back the channel state estimate. Note that the eavesdropper pretends to be an authentic user in order to exploit the possibility of disturbing its own channel estimation process. The eavesdropper exploits this characteristic of the channel sounding process to feed the transmitter with the desired corrupted values. There is no jamming in this process. We represent this corrupted eavesdropper's channel state estimate at the transmitter as $\mathbf{H}'_e$. We also consider this feedback to be error free. Figure 3 illustrates the process.

We also consider, in a few cases, that a least mean squares (LMS) algorithm [12] is used to minimize the effects of noise in the pilots. This algorithm consists of sending several pilots for each transmit/receive antenna pair, and it iteratively refines the estimate by minimizing the mean squared error.

IV. Attack strategies groups

We divide the attack strategies into two groups, the ideal attacks and the practical attacks. For the ideal attacks, we consider that the eavesdropper has full CSI of the main channel. Since it is able to attack the main channel sounding process, we consider it able to fully manipulate this estimate by adding the jamming signal to the pilots resulting in the desired corrupted channel estimate. Although full CSI of the main channel at the eavesdropper is not a practical assumption, the ideal attacks serve as an upper bound for the effect of a practical channel sounding attack.

For the practical attacks we consider that the eavesdropper only has full CSI of the eavesdropper's channel. It is still able to manipulate the estimation the transmitter makes of the eavesdropper's channel, but may only attack the main channel sounding process using conventional attacks such as jamming. What differentiates one attack strategy from the other is the way the eavesdropper corrupts the transmitter estimation of the channels. In order to evaluate the efficiency of each strategy we define following parameters:

Definition 1 (***Estimated secrecy rate***): Let c'_i be the i-th generalized singular value squared obtained by the operation GSVD$(\mathbf{H'}_m, \mathbf{H'}_e)$, and p'_i obtained by

$$p'_i = \max\left(0, \frac{-1+\sqrt{1-4(c'_i-c'^2_i)+(8c'_i-1)(c'_i-c'^2_i)/\mu a_i}}{2(c'_i-c'^2_i)}\right) \tag{14}$$

if $c'_i > 1 - c'_i$ and $p'_i = 0$ otherwise.

The **estimated secrecy rate** is

$$R_{se} = \sum_{i=1}^{q} \log(1+p'_i c'_i) - \log(1+p'_i - p'_i c'_i). \tag{15}$$

It represents the maximum secrecy rate estimated by the transmitter in the presence of the eavesdropper's attack. The power allocation strategy and the secrecy rate are calculated based on the corrupted channel estimation values.

Definition 2 (***Real Secrecy Rate***): Given $\mathbf{P'}$ the matrix in which the diagonal entries are calculated by (15), $\mathbf{A'}$ the precoding matrix obtained by GSVD$(\mathbf{H'}_m, \mathbf{H'}_e)$, we calculate the **real secrecy rate** as

$$\begin{aligned} R_{sr} = &\log\det(\mathbf{I} + \mathbf{\Psi}_m \mathbf{C}\mathbf{A}^{-1}\mathbf{A'}\mathbf{P'}(\mathbf{A'})^H \mathbf{A}^{-\mathbf{1}^H}\mathbf{C}^T {\mathbf{\Psi}_\mathbf{m}}^H) \\ &- \log\det(\mathbf{I} + \mathbf{\Psi}_m \mathbf{D}\mathbf{A}^{-1}\mathbf{A'}\mathbf{P'}(\mathbf{A'})^H \mathbf{A}^{-\mathbf{1}^H}\mathbf{D}^T {\mathbf{\Psi}_\mathbf{m}}^H), \end{aligned} \tag{16}$$

which represents the maximum secrecy rate the system actually obtains by using a power allocation strategy and a beamforming strategy based on corrupted values of the channel state. The power allocation strategy and the beamforming strategy are calculated based on the corrupted values, $(\mathbf{H'}_m, \mathbf{H'}_e)$, as these calculations are performed by the transmitter. The real secrecy rate is then calculated based on the real values of the channel $(\mathbf{H}_m, \mathbf{H}_e)$ as they do not change with the attacks. This mismatch, between estimated channel values and actual channel values, causes the beamforming strategy to be flawed and therefore there is no longer the formation of independent parallel sub-channels.

The parameter $\mathcal{C}_s$ is used to represent the secrecy capacity under no eavesdropper's attack.

V. Ideal attacks

In this section, we present the ideal attacks and provide the results of the simulations made for each one of them.

A. Inverse power allocation attack

The inverse power allocation attack corrupts the main and eavesdropper's channel in a way that the generalized singular values change their positions. The largest generalized singular value changes its position with the lowest, the second largest with the second lowest, and so on. As an example, consider that the generalized singular value matrix be given by

$$\mathbf{C} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}. \tag{17}$$

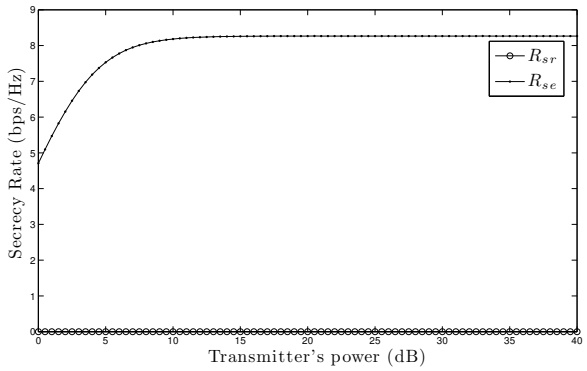

Fig. 4. Secrecy rate x Total power restriction - Inverse power allocation attack. $n_t = n_r = n_e = 5$, $N_0 = 1$

Supposing $a > b > c$, the attack would produce the following modified $\mathbf{C}$ matrix

$$\mathbf{C}' = \begin{pmatrix} c & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{pmatrix}, \tag{18}$$

where $\mathbf{C}'$ is the matrix in which the diagonal entries are the generalized singular values obtained by GSVD($\mathbf{H}'_m, \mathbf{H}'_e$).

The results from (11) and (14), matrices $\mathbf{P}^*$ and $\mathbf{P}'$ (diagonal matrix, containing the corrupted power allocation strategy), will have entries with approximate values but in different positions. The largest value of $\mathbf{P}^*$ will change the position with the lowest value at $\mathbf{P}'$. R_{sr} will be greatly affected by the position of the entries p_i^*. In this attack, more power will be allocated to the sub-channels with lower c_i and less (or no) power to the sub-channels with higher c_i.

As can be seen in Figure 4, R_{sr} is null. Since we are always allocating power to the worst subchannel, there is no rate of transmission that ensures secret communication in this scenario. The damaging characteristic of this attack is the fact that typically the transmitter sends information at rates close to what it believes to be the capacity. In this case, there is a great difference between R_{se} and R_{sr}. Therefore, the attack tricks the transmitter into sending information at rates above the real secrecy rate, compromising information security.

B. Main channel rank attack

By forcing all the columns of $\mathbf{H}'_m$ to be the same, the eavesdropper forces the main channel to have unitary rank. The transmitter is then forced to apply power only to a single sub-channel, losing all the benefits of having multiple antennas. Note that R_{sr} and R_{se} become lower than $\mathcal{C}_s$ for high transmit power. Figure 5 shows the effect of this strategy.

In our simulation, there was a $44,4\%$ transmission rate drop comparing to capacity (as we assume the transmitter sends at R_{se}) in the high transmit power region. We also observed that R_{sr} is 37.9% lower than R_{se}. This attack is able to lower the transmission rate (as $R_{se} < \mathcal{C}_s$), while at the same time compromising information security (as $R_{sr} < R_{se}$).

VI. Practical attacks

In this section, we present the practical attacks and provide the results of the simulations made for each one of them.

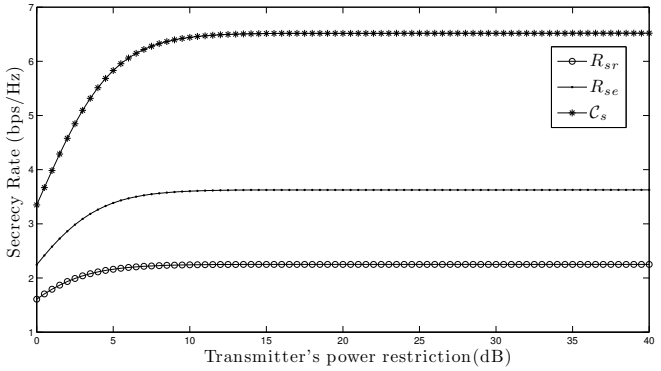

Fig. 5. Secrecy rate x Total power restriction- Main channel rank attack. $n_t = n_r = n_e = 5$, $N_0 = 1$

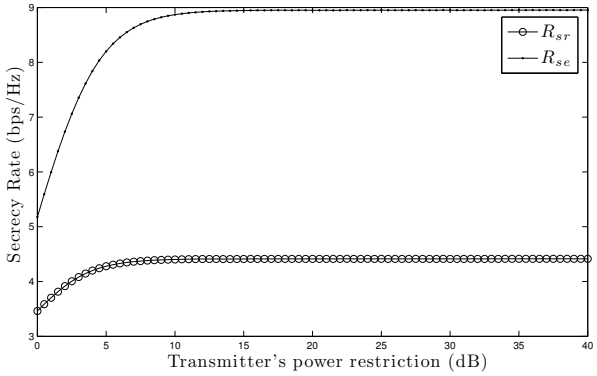

Fig. 6. Secrecy rate x Power restriction - Main channel noise attack. $n_t = n_r = n_e = 5$, $N_0 = 1$

A. Main channel noise attack

During the main channel sounding process, the eavesdropper attacks the receiver by sending white Gaussian noise. So the corrupted estimate is $\mathbf{H}'_m = \mathbf{H}_m + \mathbf{r}$, where $\mathbf{r}$ represents the jamming at the receiver. According to [13], small singular values tend to grow in the presence of random disturbances. When noise is added in the main channel sounding process, the eavesdropper is able to produce a main channel estimate with higher singular values than the original matrix $\mathbf{H_m}$. This results in R_{se} higher than R_{sr}.

It was considered in our simulation that the noise at the receiver has half the pilots power. As can be seen in Figure 6, the value of R_{se} was approximately 97.32% higher than R_{sr} at the high transmit power region. The problems of having higher estimated secrecy rate than real secrecy rate were discussed in the inverse power allocation attack.

In the sequel, the same scenario was simulated, but a LMS algorithm was used in order to minimize the effects of noise in the main channel sounding process. The secrecy rates (real, capacity and estimated) presented values very similar, showing that under these circumstances the attack becomes inefficient.

B. Degraded Eavesdropper's channel attack

By feeding back to the transmitter a eavesdropper's channel matrix multiplied by an arbitrarily low value:

$$\mathbf{H'}_e = m\mathbf{H}_e. \tag{19}$$

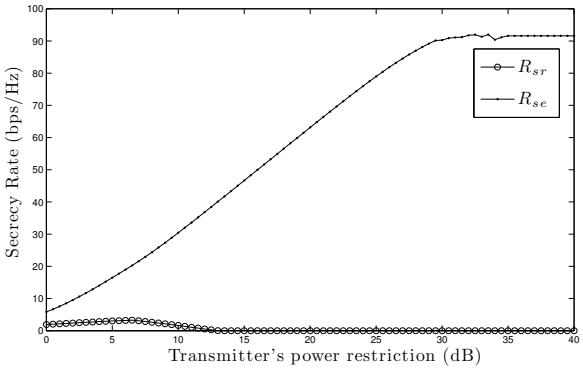

Fig. 7. Secrecy rate x Total power restriction - degraded eavesdropper's channel attack. $n_t = n_r = n_e = 5$, $N_0 = 1$

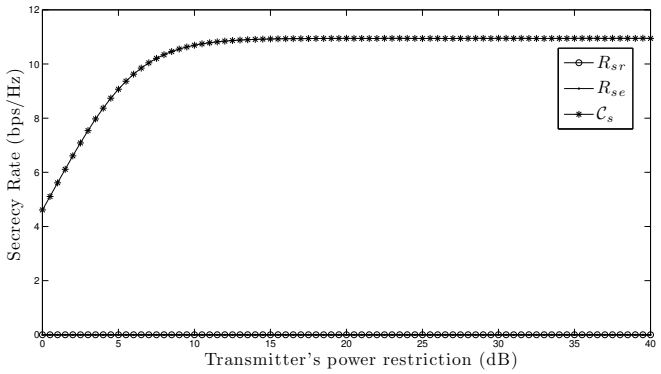

Fig. 8. Secrecy rate x Total power restriction - Super eavesdropper's channel attack. $n_t = n_r = n_e = 5$, $N_0 = 1$

By having $m << 1$, the eavesdropper is able to make its channel seem unable. R_{se} will be close to the main channel capacity (as the transmitter believe it is not being eavesdropped), and R_{sr} will be very low, due to a flawed power allocation strategy. Figure 7 shows the effects of this strategy. For this simulation, it was considered $m = 10^{-3}$. Note that, for the low transmit power region, there is still a non-zero R_{sr}, but for the high power region there is no rate in which the transmitter is able to transmit confidentially.

C. Super Eavesdropper attack

In this strategy, the eavesdropper feeds back to the transmitter an eavesdropper's channel matrix multiplied by an arbitrarily high value:

$$\mathbf{H'}_e = m\mathbf{H}_e, \tag{20}$$

where $m >> 1$. By doing so, the eavesdropper's channel seem to the transmitter to be much more able than it actually is, forcing the transmitter to send information at lower rates to ensure secrecy. Figure 8 shows the effects of this strategy. For this simulation, it was considered $m = 5$. In this simulation, while $\mathcal{C}_s = 10.94\ bps/Hz$, R_{se} and R_{sr} were null, as no power was allocated to the transmitter's antennas. The attack was able to convince the transmitter that there was no secure rate of transmission, completely disrupting communication between the legitimate users.

TABLE I
EFFECTS OF EACH ATTACK GROUP

Attack effect	Attack strategies
Lowering transmission rate ($R_{se} < \mathcal{C}_s$)	Main channel rank, Super eavesdropper attack
Compromising secrecy ($R_{se} > R_{sr}$)	Inverse power allocation, Degraded eavesdropper's channel, Main channel rank, Main channel noise

VII. CONCLUSION

We proposed and analyzed the efficiency of different channel sounding attack strategies for disrupting secret communication between the legitimate users. Even though we have not provided analytical proofs on the performance of these attacks, we believe that the simulations serve as a strong indication of the potential of attacking the channel sounding process.

Also, from the results it is possible to further divide the attack strategies into two distinct groups, based on the effects each attack has on the system. Table I illustrates these conclusions. Although lowering transmission rate between the legitimate users might not be a primary concern of a typical eavesdropper, it is interesting to see that the eavesdropper is able to do this with CSI attacks. Based on the information that is available and its main goal, the eavesdropper has the freedom to choose which strategy suits better. As a last remark, relying solely on the users feedback to estimate their channels may be a great liability to the overall secrecy in GSVD based systems, as any user may potentially become an eavesdropper.

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. Journ.*, vol. 29, pp. 656 – 715, 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355 – 1387, 1975.
[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339 – 348, 1978.
[4] F. Oggier and H.Babak, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. on Inform. Theory*, vol. 57, no. 8, pp. 4961 – 4972, 2011.
[5] A. Khisti and G.W.Wornell, "Secure Transmission with Multiple Antennas - Part ii: The MIMOME Wiretap Channel," *IEEE Trans. on Inform. Theory*, vol. 56, no. 11, pp. 5515 – 5532, 2010.
[6] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal Power Allocation for GSVD-Based Beamforming in the MIMO Wiretap Channel," *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, vol. 56, no. 11, pp. 2321 – 2325, 2010.
[7] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, pp. 2180 – 2189, 2008.
[8] A. Mukherjee and A. L. Swindlehurst, "A Full-Duplex Active Eavesdropper in MIMO Wiretap Channels: Construction and Countermeasures," *Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pp. 265 – 269, 2011.
[9] R. Miller and W. Trappe, "On the Vulnerabilities of CSI in MIMO Wireless Communication Systems," *IEE Trans. on mobile computing*, vol. 11, no. 8, pp. 1386 – 1398, 2011.
[10] C. F. V. Loan, "Generalizing the singular value decomposition," *SIAM J. Numer. Anal.*, vol. 13, no. 1, p. 76 83, 1976.
[11] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM J. Numer. Anal.*, vol. 18, no. 3, pp. 398 – 405, 1981.
[12] S. Haykin, *Adaptive Filter Theory*. Prentice-Hall, 1996, vol. 3rd Ed.
[13] G. W. Stewart, "Perturbation theory for the singular value decomposition," in *In SVD and Signal Processing, II: Algorithms, Analysis and Applications*. Elsevier, 1990, pp. 99–109.