Securing the Alamouti MAC in the presence of a Multi-Antenna Eavesdropper

T. Allen, *Senior Member, IEEE,* A. Tajer, *Senior Member, IEEE*, N. Al-Dhahir, *Fellow, IEEE*

***Abstract*— We investigate the physical layer security of synchronous multiple access transmissions using the Alamouti space-time block code in fading channels. Specifically, multiple users communicate with a single intended receiver in the presence of an eavesdropper with multiple receive antennas. In our previous work, the users employed an artificial-noise-aided transmission technique developed for single-antenna eavesdroppers. In this letter, we extend this to the important case of a multi-antenna eavesdropper by optimizing the power allocation ratio and the number of users that participate in the artificial noise generation to provide a desired sum-rate secrecy capacity to multiple access transmissions.**

***Index Terms*—Artificial noise, multiple access channel, physical layer security, space-time block code**

I. Introduction

In the past few years, many research efforts have been made to study the physical layer security of various communications scenarios and under different channel state information (CSI) assumptions. In the pioneering studies in [1]–[4], it was revealed that a positive secrecy data rate is achieved if the transmitter-eavesdropper channel is a degraded version of the legitimate transmitter-receiver channel. However, in these studies, the eavesdropper's CSI was assumed to be available at the transmitter, which is usually impractical. More recently, research efforts have been directed towards designing practical transmission schemes to improve physical layer security by providing a signal-to-noise ratio (SNR) advantage for the legitimate receiver, e.g., through transmit beamforming (TBF) [5], secure on-off transmission [6], and secure opportunistic scheduling [7]. It is important to note that the above techniques are vulnerable in high SNR regimes for the eavesdropper. Therefore, to further degrade the eavesdropper's channel, the study in [9] proposes a channel prefixing scheme where artificial noise (AN) is added on top of the beam-formed information signal to confuse the eavesdropper. Using this strategy, the power allocation ratio between the information signal and the AN should be optimized to maximize the achievable secrecy rate. Notably, the schemes in [5]–[9] relax the strong assumption according to which the precise eavesdropper's CSI is available at the transmitters sites. However, these schemes do require instantaneous CSI feedback from the intended receiver, which is a major advancement toward practical secure communications.

In this letter, we make the following new contributions: First, we extend the contributions of [11] by analyzing the sum-rate capacity of the multiple-access channel (MAC) for an eavesdropper with multiple receive antennas (RX). To understand security ramifications, we analyze the sum-rate capacity of a multi-antenna eavesdropper when the AN technique described in [11] is employed to improve secrecy. In this case, however, we broaden the analysis by generalizing the number of users allowed to participate in the AN generation. Finally, we present a scheme for securing MAC transmissions, to a desired secrecy rate, by jointly optimizing the number of MAC users involved with generating the AN and the power allocation ratio to counter the losses in the sum-rate secrecy capacity when Eve has multiple RX.

The outline of this paper is as follows: We start in Section II by describing the system model. In Section III we analyze the proposed AN technique and propose a scheme to maintain a desired secrecy rate by jointly optimizing the number of users generating the AN and the power allocation ration when the eavesdropper has multiple receive antennas (RX). To verify our analysis, we present simulation results in Section IV and finally conclude in Section V

II. System Model

We leverage the model from [11], where N users simultaneously and synchronously communicate with a common receiver using the Alamouti space-time block code (STBC) in the presence of a passive eavesdropper. Both the legitimate and eavesdropper channels experience slow fading and their coherence times are assumed long enough to allow capacity-achieving codes within each block. We assume that the Alamouti users experience independent and identically distributed (IID) Rayleigh fading channels. The legitimate receiver (Bob) and the eavesdropper receiver (Eve) have perfect CSI and perform maximum likelihood (ML) joint detection of the combined signal from all transmitters simultaneously. From [11], the performance of joint detection is fundamentally limited by the SNR rather than the signal-to-interference ratio (SIR).

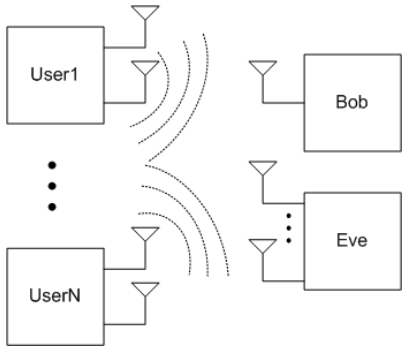

Fig 1: Synchronous MAC Model

As depicted in Fig 1, we assume that N users, denoted by User1,…,UserN, simultaneously transmit, each using $N_{tx} = 2$ transmit antennas, independent messages to a common receiver using the Alamouti STBC in the presence of a passive

eavesdropper (Eve). Bob has a single receive antenna while Eve has an arbitrary number of receive antennas. In addition, we assume that the message lengths are sufficiently long to allow proper coding and information theoretic results in the analysis.

The symbols transmitted by the n^{th} user in the kth Alamouti block are represented by $s_{n,k}$, and S_k is a $N_{tx} \cdot N \times 1$ vector that contains the transmitted symbols by all users. The transmitted symbols are assumed to be independent, zero-mean circularly symmetric complex Gaussian random variables and are power constrained such that $\mathbb{E}(|s_{n,k}|^2) = P_n$. Different users can transmit their signals at different power levels, which are controlled by the common receiver. Accordingly, we define the transmit power matrix $P \triangleq diag(P_1, \dots, P_N)$. The matrix $\boldsymbol{H_k}$ is the $2 \times N_{tx} \cdot N$ stacked equivalent of the Alamouti channel matrix whose elements, $\boldsymbol{h_{k,n}}$, represent the $2 \times N_{tx}$ Alamouti multiple access channel matrix associated with the n^{th} MAC user [11].

Let N_{rx} denote the number of receive antennas for Eve. Considering the received signal at the mth antenna, the matrix $\boldsymbol{G_{k,m}}$ has the same structure as $\boldsymbol{H_k}$ whose elements, $\boldsymbol{g_{k,n,m}}$, have the same structure as $\boldsymbol{h_{k,n}}$. Define $\boldsymbol{G_k} = [\boldsymbol{G_{k,1}}, \dots, \boldsymbol{G_{k,N_{rx}}}]^T$ as the combine channel matrix for Eve. Hence, Eve's instantaneous sum-rate capacity for the MAC with N users is given by

$$C_{E,k} = {}^1\!/_2 \log_2\left(\det\left(\boldsymbol{I_{2 \cdot N_{rx}}} + {}^1\!/_2 \cdot \boldsymbol{\Sigma_k^{-1}} \cdot (\boldsymbol{G_k} \cdot \boldsymbol{P} \cdot \boldsymbol{G_k^*})\right)\right), \quad (1)$$

where $\boldsymbol{\Sigma_k^{-1}}$ is a $2 \cdot N_{rx} \times 2 \cdot N_{rx}$ diagonal matrix that represents the inverse of the noise power at each receive antenna, $N_{E,m}$. Notice that $\boldsymbol{G_k} \cdot \boldsymbol{G_k^*}$ is a positive semi-definite matrix, and therefore we can use Hadamard's inequality to define an upper bound on the determinant (1), Specifically,

$$\det\left(\boldsymbol{I_{2 \cdot N_{rx}}} + {}^1\!/_2 \cdot \boldsymbol{\Sigma_k^{-1}} \cdot (\boldsymbol{G_k} \cdot \boldsymbol{P} \cdot \boldsymbol{G_k^*})\right) \leq \prod_m \left(1 + \sum_{n=1}^{N} \frac{\gamma_{E,n,m}}{2} \| \boldsymbol{g_{k,n,m}} \|_2^2\right)^2, \quad (2)$$

where $\gamma_{E,n,m} = P_n / 2 \cdot N_{E,m}$ is the average SNR associated with the transmission of the nth Alamouti MAC user to the m^{th} receive antenna and $\|\cdot\|_2$ represents the Forbenius norm. By using (2), we can now define an upper bound on the instantaneous sum-rate capacity when the receiver has multiple receive antennas

$$C_{E,k} \leq \sum_{m=1}^{N_{rx}} \log_2\left(1 + \sum_{n=1}^{N} \frac{\gamma_{E,n,m}}{2} \| \boldsymbol{g_{k,n,m}} \|_2^2\right). \quad (3)$$

It is important to note that (3) shows that Eve's instantaneous sum-rate capacity is bounded by the sum of the individual capacities associated with each of Eve's receive antennas. We used the Hadamard's inequality to bound the determinant because when we computed the elements of the positive semi-definite matrix $\boldsymbol{G_k} \cdot \boldsymbol{G_k^*}$, we found that the off-diagonal elements tend to the zero (due to the assumed independent channels) as the number of users increases; providing a tight upper bound.

III. Securing Alamouti MAC Transmissions

In this section, we extend the channel prefixing technique presented in [11] for countering the losses in the sum-rate secrecy capacity when Eve has multiple RX by allowing for more users to participate in the AN generation and adjusting their transmit powers.

A. Artificial Noise Generation

The combined signal transmitted by the nth user is $t_{k,n} = \sqrt{\phi_n} \cdot s_{k,n} + \sqrt{1-\phi_n} \cdot v_{k,n}$ where $s_{k,n}$ represents the symbols transmitted by the nth user and $v_{k,n}$ is the AN symbol generated and transmitted by the n^{th} user. We denote the power allocation ration for the nth MAC user by $\phi_n \in [0,1]$. Let the $V_k = [v_{k,1}, \dots, v_{k,N}]^T \in Null(H_k)$ denote the aggregate AN vector that is added to the aggregate signal vector S_k. Lastly, let the matrices Φ and Υ be as defined in [11]. Note that Eve's received signal on the m^{th} receive antenna is degraded by the AN even when Eve has ideally infinite SNR because Eve experiences independent fading ($h_{k,1} \neq g_{k,1,m}$ and $h_{k,2} \neq g_{k,2,m}$) and, in general, $V_k \notin \text{Null}(\boldsymbol{G_{k,m}})$. As was the case in [11], in order to place the focus on analyzing the impact of the AN on the secrecy performance, for the remainder of the letter we assume that all users have identical power constraints, i.e., $P_n = P$ and $\phi_n = \phi$ for $n \in \{1, \dots, N\}$. From this, Eve's instantaneous sum-rate capacity for the MAC with N users under the power allocation scheme controlled by P is given by

$$C_{k,E}^{AN} = \frac{1}{2}\log_2(\det(\boldsymbol{I_{2 \cdot N_{rx}}} + {}^1\!/_2 \cdot \boldsymbol{\Sigma_{AN,k}^{-1}} \cdot (\boldsymbol{G_k} \cdot (\boldsymbol{\Phi^2} \cdot \boldsymbol{P}) \cdot \boldsymbol{G_k^*}))), \quad (4)$$

where $\boldsymbol{\Sigma_{AN,k}^{-1}}$ is a $2 \cdot N_{rx} \times 2 \cdot N_{rx}$ diagonal matrix that represents the inverse of the combined noise power at each receive antenna and can be written as

$$\boldsymbol{\Sigma_{AN,k}^{-1}} \triangleq \text{diag}(\left(\left\|\boldsymbol{G_{k,1}} \cdot \boldsymbol{\Upsilon} \cdot V_k\right\|^2 + N_{E,1}\right)^{-1} \dots \left(\left\|\boldsymbol{G_{k,N_{rx}}} \cdot \boldsymbol{\Upsilon} \cdot V_k\right\|^2 + N_{E,N_{rx}}\right)^{-1}). \quad (5)$$

Assuming $N_{E,m} = N_E$ for $m \in \{1, \dots, N_{rx}\}$, we can write an upper bound for $C_{E,k}^{AN}$ by using Hadamard's inequality and simplifying, to get

$$C_{k,E}^{AN} \leq \check{C}_{k,E}^{AN} = \sum_{m=1}^{N_{rx}} \log_2((1 + \frac{\phi}{\left\|\boldsymbol{G_{k,m}} \cdot \boldsymbol{\Upsilon} \cdot V_k\right\|^2 + N_E} \cdot \frac{P}{2} \cdot \sum_{n=1}^{N}\sum_{j=1}^{2} \left|\boldsymbol{g_{k,j,n,m}}\right|^2)) \quad (6)$$

B. Structure of Null($\boldsymbol{H_k}$)

As shown in [11], the structure of $Null(\boldsymbol{H_k})$ allows for a vector $V_k \in Null(\boldsymbol{H_k})$ to be generated using the channel gains associated with any 2 users, in fact, for N users; only $2 \cdot \left\lfloor \frac{2N}{4} \right\rfloor = 2 \cdot \left\lfloor \frac{N}{2} \right\rfloor$ users can participate in AN generation at any one time. Furthermore, it was shown in [11] the actual users participating can be managed so that the long-term average power that different users spend on the AN vector is constant across all users (time-sharing). It is important to note that (35) and (37) in [11] show that all the basis vectors of $Null(\boldsymbol{H_k})$ have a similar structure and, when the user pairs are unique, they are mutually orthogonal. Therefore, with no loss of generality, we will analyze $V_k \in Null(\boldsymbol{H_k})$ assuming 2 users are participating in AN generation. To this end, we re-wright [11] to show an

alternate view of $V_k = (v_{k,1} \quad v_{k,2})^T \in Null(\boldsymbol{H_k})$, i.e.

$$v_{k,1} = \left(-\frac{\left(h_{k,2,1}\cdot h^*_{k,1,1} - \left(-h^*_{k,2,2}\right)\cdot h_{k,1,2}\right)}{\left|h_{k,1,1}\right|^2 + \left|h_{k,1,2}\right|^2}, -\frac{\left(h_{k,1,1}\cdot\left(-h^*_{k,2,2}\right) - \left(-h^*_{k,1,2}\right)\cdot h_{k,2,1}\right)}{\left|h_{k,1,1}\right|^2 + \left|h_{k,1,2}\right|^2}\right)^T \quad (7)$$

$$v_{k,2} = (1 \quad 0)^T$$

Notice that $v_{k,2}$ is constant, i.e., $(1 \quad 0)^T$ and the elements of $v_{k,1}$ are both t location-scaled random variables (RVs) with location μ = 0, scale σ =1/2, and ν = 4 degrees of freedom [12]. More importantly, it is clear that the mean of these elements remains at 0 and the variance is $\sigma^2 \cdot \frac{v}{v-2} = \frac{1}{2}$, showing that their behavior is very similar to a complex standard normal random variable, $\mathcal{N}_{\mathbb{C}}(0,1/2)$.

Define vectors $d_{1,n,m} \triangleq [g_{k,1,n,m} \quad g_{k,2,n,m}]$ and $d_{2,n,m} \triangleq \left[-g^*_{k,2,n,m} \quad g^*_{k,1,n,m}\right]$ that represent the channel gains associated with n^{th} user and the m$^{\text{th}}$ receive antenna over each timeslot of the k^{th} transmitted Alamouti codeword. Let the number of MAC users participating in AN generation be L and let the *2Lx1* AN vector $V_k = [v_{k,1}, \dots, v_{k,L}, 0, \dots, 0]^T$. Therefore, we can represent $\boldsymbol{G_{k,m}}$ as

$$\boldsymbol{G_{k,m}} = \begin{bmatrix} d_{1,1,m} & \dots & d_{1,N,m} \\ d_{2,1,m} & \dots & d_{2,N,m} \end{bmatrix} \quad (8)$$

and we write the received AN symbol on the m$^{\text{th}}$ receive antenna as

$$\boldsymbol{G_{k,m}}\cdot V_k = \left[\sum_{n=1}^{L} d_{1,n,m}\cdot v_{k,n} \quad \sum_{n=1}^{L} d_{2,n,m}\cdot v_{k,n}\right]^T.$$

We have shown in (7) that when n is even; $v_{k,n}$ is a constant vector, i.e. $(1 \quad 0)^T$ and when n is odd, $v_{k,n}$ consists of two t location-scaled RVs that can be approximated by $\mathcal{N}_{\mathbb{C}}(0,1/2)$ RVs. Note that when n is even, both $d_{1,n,m}\cdot v_{k,n}$ and $d_{2,n,m}\cdot v_{k,n}$ each result in elements that are $\mathcal{N}_{\mathbb{C}}(0,1)$ RVs. When n is odd, knowing that the elements of $v_{k,n}$ behave similar to $\mathcal{N}_{\mathbb{C}}(0,1/2)$ R.V.'s, it is not surprising that both $d_{1,n,m}\cdot v_{k,n}$ and $d_{2,n,m}\cdot v_{k,n}$ result in elements that empirically behave as $\mathcal{N}_{\mathbb{C}}(0,1)$. Therefore, the elements of $\boldsymbol{G_{k,m}}\cdot V_k$ associated with each timeslot can be approximated by $\mathcal{N}_{\mathbb{C}}(0, \mathrm{L})$ RVs. From this, we can conclude the AN combined with AWGN: 1) remains Gaussian and 2) changes at the same rate as the data; meaning that we can use information-theoretic results in our analysis.

C. Transmission Power Constraint

As in [11], consider the $2N \times 1$ vector of the form $V_k = \sqrt{\beta_k}\cdot\frac{U_k}{\|U_k\|}$ that satisfies $V_k \in Null(\boldsymbol{H_k})$, where $U_k \in Null(\boldsymbol{H_k})$ and the coefficient β_k is incorporated to control the power of V_k. Define $\bar{u}_{k,l}$ as the l^{th} 2×1 sub-vector of the vector $\bar{U}_k = U_k/\|U_k\|$ and denote its average power by $\delta_{k,l}$, i.e., $\delta_{k,l} = \mathbb{E}\left(\left\|\bar{u}_{k,l}\right\|^2\right)$. Hence, Bob will feed back the AN component $v_{k,l} = \sqrt{\beta_k}\cdot\bar{u}_{k,l}$, $l \in \{1, \dots, L\}$ to each of the L users participating in AN generation during the k$^{\text{th}}$ codeword. For the L users participating during the k^{th} time slot we have $\delta_{k,l} = \mathbb{E}\left(\left\|\bar{u}_{k,l}\right\|^2\right) = \frac{1}{2L}$ and for the remaining ones we set $\delta_{k,l} = 0$. This observation establishes that $\beta_k = 2LP$ and $\left\|\boldsymbol{G_{k,m}}\cdot\boldsymbol{Y}\cdot V_k\right\|^2 = (1-\phi_n)\cdot 2LP\left\|\boldsymbol{G_{k,m}}\cdot\bar{U}_k\right\|^2$ and shows that by increasing the number of users participating in AN generation, we are able to linearly increase the power of the AN signal received by each receive antenna. Moreover, we conclude that $\left\|\boldsymbol{G_{k,m}}\cdot V_k\right\|^2$ follows a $Gamma(2,2L)$ distribution and using properties of the Gamma distribution, we can see that $\left\|\boldsymbol{G_{k,m}}\cdot V_k\right\|^2 = 2L\left\|\boldsymbol{G_{k,m}}\cdot\bar{U}_k\right\|^2$ and therefore, $\left\|G_{k,m}\cdot\bar{U}_k\right\|^2$ follows a $Gamma(2,1)$ distribution.

D. Relationship between L and N_{rx}

In this section, we present a scheme to jointly optimize *L* and ϕ to maintain a desire secrecy rate when Eve has multiple receive antennas. Specifically we want to find an *L* and ϕ such that for a given N_{rx} and secrecy rate, the resulting AN will result in Eve's average capacity being equivalent to having 1 RX when the AN is being generated by only 2 users with equal power allocation (as demonstrated in [11]). It is important to note that although N_{rx} is not known to Bob; it is assumed that both N_{rx} and secrecy-rate, are specified by the system performance requirements. As such, we can first approximate $\check{C}^{AN}_{k,E}$ in (6) by assuming the high SNR regime ($N_E \approx 0$). Next, since the channel gains are IID and the AN is statistically equivalent for each antenna, we will assume that the time ensemble averages of the SINR for each antenna are approximately equivalent. From this, we can represent our result be in the form of [11], scale it by the desired secrecy rate, and equate the two to get

$$\log_2(1+X) - R = N_{rx}\cdot\log_2(1+X/K) \quad (9)$$

where $X = \mathbb{E}\left(\frac{1}{8\cdot\left\|\boldsymbol{G_{k,m}}\cdot\bar{U}_k\right\|^2}\cdot\sum_{n=1}^{N}\sum_{j=1}^{2}\left|g_{k,j,n,m}\right|^2\right) = \mathbb{E}(W\cdot Z)$ is Eve's time ensemble average SINR for a single antenna with equal power allocation and $K = L(1-\phi)/2\phi$.. Under these assumptions, we can us (9) to solve for K. For a given R and N_{rx} to optimize $\{L, \phi\}$, we find the $\tilde{L}$ and $\tilde{\phi}$ that satisfy (10) under the constraints of $2 \le \tilde{L} \le 2\cdot\left\lfloor\frac{N}{2}\right\rfloor$ and $0 < \tilde{\phi} < 1$, i.e.,

$$\frac{\tilde{L}}{2} = \mathrm{nint}\left(\frac{\tilde{\phi}}{(1-\tilde{\phi})}\cdot\frac{X}{\left(2^{-R}\cdot(X+1)\right)^{\frac{1}{N_{rx}}} - 1}\right), \quad (10)$$

where $\mathrm{nint}(\cdot)$ represents the nearest integer function. In order to maximize Bob's sum-rate capacity, the optimization process will initially set $\tilde{\phi} = 0.5$ and use (10) to find the optimal L. If a solution exists, we increase $\tilde{\phi}$ until just before $\tilde{L}$ increases. If a solution to (10) cannot be found, set $\tilde{L} = 2\cdot\left\lfloor\frac{N}{2}\right\rfloor$ and decrease $\tilde{\phi}$ until (10) is satisfied; otherwise an optimal $\{L, \phi\}$ does not exist for the given R and N_{rx}. It is important to note that increasing or decreasing ϕ will directly affect Bob's sum-rate capacity, but will inversely affect his secrecy capacity. More importantly, to evaluate (10), we need to evaluate X. The major difficulty with fully delineating the distribution of $W\cdot Z$ is that it involves common random variables. However, both numerator and denominator are non-linear functions of $\{g_{k,j,n,m}\}$ and therefore correlation is not preserved. Hence, for this discussion, we will assume that $W\cdot Z$ can be approximated

as being the product of two independent RVs and can approximate X by the product of the averages of $W \sim invGamma(\alpha_1, \beta_1)$ and $Z \sim Gamma(\alpha_2, \beta_2)$, to get

$$X \cong \left(\frac{1}{(\alpha_1 - 1)\beta_1} \cdot \alpha_2 \beta_2\right). \quad (11)$$

From the previous discussions, we have $\alpha_2 = 2N, \beta_2 = \frac{1}{8}, \alpha_1 = 2, \beta_1 = 1$, so $X = N/4$. Finally, when $N_{rx} = 1$, and R=0, and $\phi = 0.5$; (10) tells us that L = 2 which agrees with [11].

IV. Simulation Results

The instantaneous realizations of the channels are unknown to the Alamouti MAC users, and therefore, we adopt the secrecy outage probability as a relevant performance metric to quantify the security of the Alamouti MAC. For this purpose, we define the instantaneous sum-rate secrecy capacity of Alamouti MAC transmissions as the difference between the instantaneous sum-rate capacities of Bob as defined by Eq. 45 in [11] and Eve defined by (4), i.e.

$$C_s = \left[C_{k,B}^{AN} - C_{k,E}^{AN}\right]^+.$$

The simulation results are obtained via Monte Carlo simulations where the probabilities were obtained using at least 2000 realizations. Table 1 shows the parameters obtained from (10) that are used in AN generation for a given N_{rx} and desired secrecy rate, R (n/s indicates a solution does not exist). Figure 2 shows the secrecy outage probability vs. Bob's receive SNR for the scenarios highlighted in Table 1. Each simulation assumes a high SNR regime for Eve (i.e. SNR = 20 dB) with N = 30 MAC users.

Table 1: Simulation Parameters from (10)

N_{rx}	R = 0		R = 1		R = 2		R=3	
	L	ϕ	L	ϕ	L	ϕ	L	ϕ
1	2	0.60	6	0.55	14	0.51	30	0.11
2	8	0.52	16	0.51	30	0.49	n/s	n/s
4	22	0.51	30	0.47	30	0.30	n/s	n/s
8	30	0.39	30	0.28	30	0.16	n/s	n/s
16	30	0.22	30	0.16	n/s	n/s	n/s	n/s

The base-line scenario representing the case when $N_{rx} = 1$ and $\phi = 0.5$ is provided as a reference (black dashed line). Notice how the optimization process initially relies on L to provide the desired security level. Only when L is exhausted is ϕ used to achieve specified secrecy rate. The reason for this is that ϕ provides flexibility to either increase Bob's sum-rate capacity or Eve's SINR depending on the desired result. Accordingly, when comparing the results to the base-line scenario, it is easy to see that the optimization of L and ϕ proposed in (10) provides an effective mechanism to determine whether or not (and how) multiple access transmission can be secure in the presence of a multi-antenna eavesdropper.

V. Conclusion

In this letter, we have extended the contributions of [11] by analyzing the secrecy sum-rate capacity of the MAC when the users adopt the Alamouti STBC [10] in the presence of a passive eavesdropper with multiple receive antennas. We expanded the analysis of the AN technique described in [11] by generalizing the number of users allowed to participate in the AN generation up to a maximum of $2 \cdot \left\lfloor \frac{N}{2} \right\rfloor$ users. Finally, we presented a method for securing multiple access transmissions by optimizing the number of users and power allocation needed in AN generation to maintain a specific level of security; countering the losses in the sum-rate secrecy capacity when Eve has multiple receive antennas.

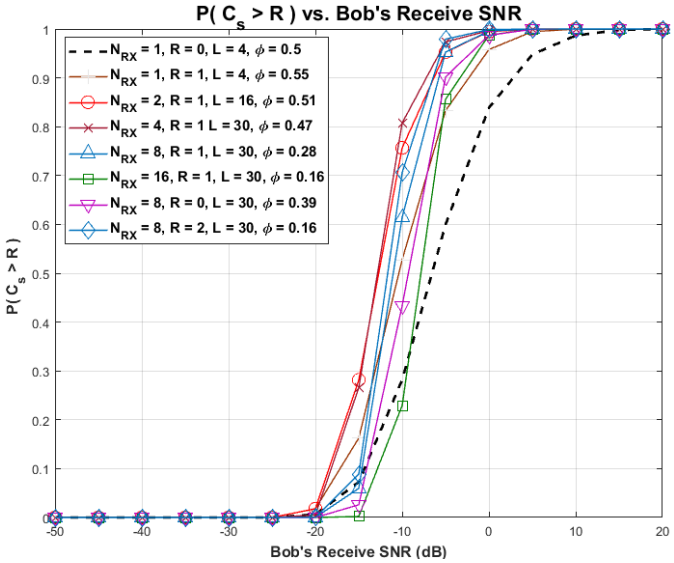

Fig 2: Secrecy Outage Probability for the Alamouti MAC in the presence of a multi-antenna eavesdropper.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal,* vol. 28, no. 4, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451-456, Jul 1978.

[5] S. Bashar, Z. Ding and G. Y. Li, "On Secrecy of Codebook-based Transmission Beamforming under Receiver Limited Feedback," *IEEE Transactions on Wireless Communications,* vol. 10, no. 4, pp. 1212-1223, April 2011.

[6] B. He and X. Zhou, "Secure On-Off Transmission Design with Channel Estimation Errors," *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 12, pp. 1923-1936, Dec. 2013.

[7] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Processing Letters,* vol. 20, no. 2, pp. 141-144, Feb. 2013

[8] S. Yan, N. Yang, R. Malaney and J. Yuan, "Transmit Antenna Selection with Alamouti Coding and Power Allocation in MIMO Wiretap Channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1656-1667, March 2014.

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

[10] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451-1458, Oct 1998.

[11] T. Allen, A. Tajer and N. Al-Dhahir, "Secure Alamouti MAC Transmissions," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3674-3687, June 2017

[12] Etemad and M. Amirmazlaghani, "A new statistical detector for CT-based multiplicative image watermarking using the t location-scale distribution," *2017 9th International Conference on Information and Knowledge Technology (IKT)*, pp. 175-180, Tehran,2017.