JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University |

http://www.saujs.sakarya.edu.tr/

Title: Secrecy Outage Probability of Modified TAS/Alamouti-STBC Schemes under Pilot Contamination Attacks

Authors: Ahmet Faruk Coşkun

Recieved: 2018-08-13 22:38:50

Revised: 2018-09-13 11:26:22

Accepted: 2018-10-24 17:35:44

Article Type: Research Article

Volume: 23

Issue: 1

Month: February

Year: 2019

Pages: 94-105

How to cite
Ahmet Faruk Coşkun; (2019), Secrecy Outage Probability of Modified TAS/Alamouti-STBC Schemes under Pilot Contamination Attacks. Sakarya University Journal of Science, 23(1), 94-105, DOI: 10.16984/saufenbilder.453314
Access link
http://www.saujs.sakarya.edu.tr/issue/38708/453314

Sakarya University Journal of Science 23(1), 94-105, 2019

Secrecy Outage Probability of Modified TAS/Alamouti-STBC Schemes under Pilot Contamination Attacks

Ahmet Faruk COŞKUN*[1]

ABSTRACT

Modified transmit antenna selection (M-TAS)/Alamouti orthogonal space-time block coding (STBC) schemes have been shown to achieve superior error performance together with a reduced-rate feedback channel in the presence of feedback imperfections when compared to the conventional TAS/Alamouti-STBC schemes. By shifting the focus of the investigation, this paper answers the query on whether the modified schemes provide enhancements in also the secrecy outage probability (SOP) performance of multi-antenna schemes in wiretap channels. The exact expressions of the SOP for the M-TAS/Alamouti-STBC schemes in Rayleigh fading channels have been derived and validated via Monte Carlo simulations. Additionally, the deteriorating effect of active eavesdropping has been demonstrated by simulating the pilot contamination attacks (PCAs) on the feedback channel. The extensive investigation and comparisons to the conventional schemes have shown that M-TAS/Alamouti-STBC schemes employed at the transmission end of the legitimate link provide considerable enhancements in the secrecy rates of wireless communications systems in the presence of PCAs.

Keywords: Pyhsical layer security, TAS, Alamouti-STBC, pilot contamination attack

1. INTRODUCTION

Due to the broadcasting nature of wireless communications systems, the information content of the legitimate transmitter - receiver link might be intercepted by eavesdroppers in the same network. Accordingly, communications security is becoming a more challenging design issue to be resolved especially as the state-of-the-art and forthcoming wireless communications standards encourage to successfully operate in heterogenous networks each serving massive number of user terminals. Traditional measures that promise secure communications mainly employ cryptographic protocols to be implemented in the network layer [1]. Nevertheless, the involved secret-key distribution and management processes might be unaffordable and extremely fragile to attacks [2]. Hence, by exploiting the characteristics of wireless channels, physical layer security concept is becoming more prominent for the purpose of providing secure data transmission between the transmitter and legitimate user(s) in wiretap channels.

The pioneering researches that have focused on communications security by physical-layer means have examined the single-input single-

* Corresponding Author

[1] The Scientific and Technological Research Council of Turkey, Kocaeli, Turkey. E-mail: ahmet.coskun@tubitak.gov.tr

output (SISO) wiretap scenario constituted by transmitter, receiver and eavesdropper terminals with single transceiver [1]-[5]. Afterwards, as the multi-antenna transmitter and/or receiver designs have attracted utmost attention for the sake of their spectrally-efficient and fading-resistant characteristics in rich multi-path scattering environments, enhanced-security physical layer designs consolidated by multi-input multi-output schemes have come up [5]-[20]. The investigations prosecuted within these studies have examined the communications security concept of several well-known transmit and/or receive diversity schemes from the perspective of secrecy outage probability (SOP) in the presence of single- or multi-antenna eavesdroppers. SOP which might be briefly defined as the probability that the secrecy capacity is less than a specific transmission rate, constitutes a useful metric for the researchers to assess the communications secrecy. The average SOP achieved by a single-antenna transmitter and a maximal-ratio-combining (MRC) receiver at the legitimate user in the presence of an eavesdropper with also MRC-receiver has been examined in [8] for Rayleigh-distributed channel amplitudes. The study in [9] has focused on the wiretap scenario constituted by single-antenna transmitter and receiver ends in the legitimate link and a multi-antenna eavesdropper that is considered to employ MRC or selection combining (SC) in Rician fading environments. In addition to receive-diversity-based schemes employed at the legitimate user and eavesdropper users, the usage of transmit-diversity based schemes consisting of or including transmit beamforming (TBF), space-time block coding (STBC) and transmit antenna selection (TAS) have also attracted the researchers' attention. The communications security has been shown in [10]-[13] to be enhanced efficiently with the help of TBF. Despite being probably the most efficient means of transmit diversity scheme that enables secure communications, TBF suffers from its dependency on the precise channel state information (CSI) of the legitimate and the wiretap link at the transmitter. The high feedback burden and computational complexity faced by TBF schemes especially in case of increased number of transmit radio-frequency (RF) chains might be seen as unaffordable from the implementation perspective.

As an efficient way to achieve enhanced transmit diversity orders and reliable communications with reduced feedback requirements and hardware complexity, TAS-based transmission strategies have been of interest [14]-[20]. The simplest TAS scheme that switches the single transmit antenna maximizing the received SNR at the legitimate user has been investigated for MRC receivers [15]-[18] and generalized SC receivers [19] at the legitimate user and eavesdropper users in Rayleigh [14], [16]-[19] and non-identically distributed Nakagami-*m* [15] fading environments. The examination in [16] has introduced the average SOP performance of TAS/MRC scheme in the presence of an MRC-enhanced eavesdropper by also taking the practical conditions of time-delayed feedback (TDF) and binary symmetric channel-based feedback errors (FEs) into account. The authors of [17] have also concentrated on the same scheme in TDF conditions, and have proposed a modified TAS/MRC scheme that promises to achieve enhanced communications security in the presence of feedback delays. Relying on the practical assumption that the CSI of eavesdropper channels is difficult to be available at the transmitter especially if the eavesdropper is not a registered user of the same network or is a dedicated wiretapper, the antenna selection criterion employed within the studies [15]-[17], [19] and [20] is based on maximizing the instantaneous combined SNR at the legitimate receiver.

The conventional form of the combined TAS/STBC scheme has only been examined in [20] for Rayleigh fading environments from the communications security perspective. Here, under the assumptions of delayless and error-free feedback between the legitimate user and transmitter terminals, the authors have provided an extensive analysis on the average secrecy

performances achieved in the passive wiretapping scenario where the transmitter employs combined TAS with dual-branch Alamouti-STBC, and the legitimate user and eavesdropper users employ MRC. By providing comparisons between the SOP performances of single TAS and the conventional[2] TAS/Alamouti-STBC (C-TAS/Alamouti-STBC) schemes, [20] has demonstrated the superiority of the combined scheme when compared to the single-branch TAS.

Being motivated by the lack of an investigation on the effects of active eavesdropping (e.g., PCAs) on the secrecy performance of C-TAS/Alamouti-STBC schemes and the potential enhancements offered by the modified TAS/Alamouti-STBC (M-TAS/Alamouti-STBC) schemes under practical imperfections (as shown in [21] for imperfect feedback case), this paper focuses on the SOP performances of both schemes in the presence of PCAs. By focusing on the practical scenario where the transmitter does not have any CSI of the eavesdropper's channel, this paper analyzes the usage of the conventional and M-TAS/Alamouti-STBC schemes at the transmitter end of a legitimate wireless link in the presence of PCAs in flat Rayleigh fading channels, and makes the following specific contributions:

- The exact SOP expression for M-TAS/Alamouti-STBC schemes,
- the exhibition of the advantages such as the average SNR required to achieve a specific level of communications secrecy that are obtained by employing M-TAS/Alamouti-STBC schemes instead of the conventional ones,
- effects of active eavesdroppers that perform pilot contamination attack (PCA) [5] to the feedback channel in the legitimate (i.e., main) link,
- a useful perspective for the design of multi-antenna diversity schemes that are more robust to active eavesdropping techniques, and that provide enhancements in the average communications secrecy.

2. SYSTEM MODEL AND SNR STATISTICS

This paper focuses on the average secrecy performances of the multi-antenna diversity schemes that are constructed by performing Alamouti-STBC signaling combined with TAS at the transmission sessions and MRC scheme at the reception sessions. As sketched in Figure 1-(a), the investigated diversity schemes employ conventional and modified versions of the combined TAS/Alamouti-STBC with two active RF chains among n_A total antennas of the transmitter (namely Alice). And at the receive ends of both the legitimate and the eavesdropping users (namely Bob and Eve, respectively), optimal receive-combining (i.e., MRC) is employed through n_B and n_E antennas, respectively.

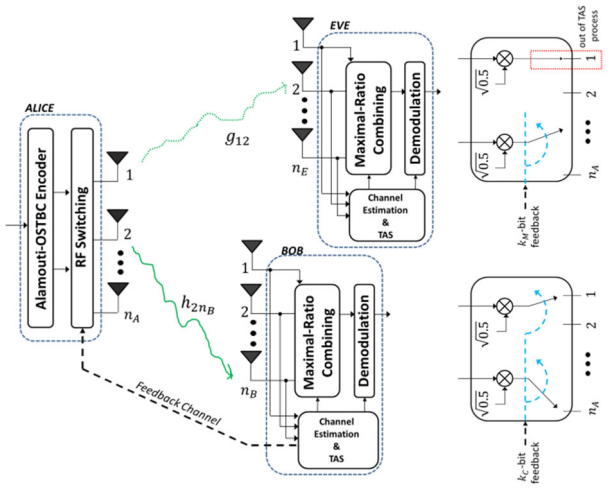

Figure 1 (a) Schematic representation of the TAS/Alamouti-STBC techniques in the presence of an

[2] Here, the term conventional is used to distinguish the straightforward but optimal antenna-subset-selecting scheme from the modified versions that have been previously introduced in [21].

eavesdropper (b) Detailed view of RF switching block for the conventional (at bottom) and modified (at top) schemes

For clarity, we first recall the system descriptions of both the C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC schemes. As shown in Figure 1-(a), both schemes occupy a feedback channel that is dedicated to convey the antenna subset index to Alice and to assist the transmission process through the best transmit-receive branches between Bob and Alice.

2.1 Conventional TAS/Alamouti-STBC

Since modified versions of combined TAS/STBC scheme have been proposed and analyzed in [21] in the presence of feedback imperfections, the scheme with the most straightforward approach to perform transmission over an optimal subset has been labeled as conventional. Note that, the antenna subset selection strategy has been shown to provide the optimal solution with the highest total channel gain in ideal feedback and antenna switching conditions, whereas it is not the case in practical conditions as shown in [21].

Without regarding the feedback burden of high-complexity brute-force subset selection and its complications on a practical feedback link, the C-TAS/Alamouti-STBC scheme performs dual-branch STBC transmission after selecting the antenna subset that consists of the transmit antennas with the ordinal numbers $o_{C,1}$ and $o_{C,2}$ among n_A total transmit antennas as seen in Figure 1-(a). Hence, the ordered antenna indices $(o_{C,1}, o_{C,2})$, where $o_{C,j} \in \{1,2,\dots,n_A\}$, $j = 1,2$, comprise only a subset among $K_C = \binom{n_A}{2}$ total combinations, and denote the orders of the transmit antennas selected (perfectly or erroneously). It would be clear that in the case of ideal subset selection (i.e., no PCAs or other imperfections), the ordinal numbers would be $o_{C,1} = 1$ and $o_{C,2} = 2$. Besides, this type of subset selection is shown to result in a feedback-bit load of $k_C = \lceil \log_2 K_C \rceil$ in [22] since the feedback information should only convey the subset index corresponding to two transmit antenna indices. Here, $\lceil \cdot \rceil$ denotes the smallest integer that is greater than or equal to its argument.

2.2 Modified TAS/Alamouti-STBC

Modified TAS/STBC (M-TAS/STBC) schemes are constructed by modifying the antenna selection/switching strategy at the transmitter ends of communication links, and are proposed to reduce the average feedback-bit requirement and to enhance the average error probability in the presence of practical feedback impairments. They are shown to efficiently reduce the feedback requirement of the C-TAS/STBC and to provide average SNR savings when compared to C-TAS/STBC schemes in the presence of FEs [22].

As seen in Figure 1-(b), the modified scheme with the single antenna selection allocates the first transmit antenna for transmission regardless from the antenna selection process, and switches the second transmit antenna by determining the best antenna with the highest total channel gain among the remaining $n_A - 1$ ones. Since the size of antenna set that is subject to the single-selection is shrinked to $K_M = n_A - 1$ (when compared to the conventional case), the feedback-bit load required to switch the selected antenna is reduced to $k_M = \lceil \log_2 K_M \rceil$ per each Alamouti-STBC transmission period.

The Alamouti-STBC mapper at Alice inserts the digitally-modulated message symbols x_1 and x_2 into the first row of the Alamouti transmission matrix that had been denoted by $\mathcal{G}_2$ and defined as

$$\mathcal{G}_2 = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_{21}^* \end{pmatrix} \quad (1)$$

as also provided in Eqs. (3) and (4) of [21]. Each row of the matrix consists of the symbols that are transmitted from each antenna while columns correspond to transmission time slots. Hence, the symbols x_1 and $-x_2^*$ will be conveyed through the first transmit antenna (i.e., dedicated regardless from the TAS process). After the selection of the single transmit antenna that had been determined to maximize the output SNR at the legitimate

receiver, the signal transmission of the second row of the Alamouti STBC codeword matrix is directed to the selected (single) transmit antenna.

2.3 SNR Statistics of M-TAS/STBC Schemes

The envelopes of the complex Gaussian-distributed fading coefficients $h_{j,i}$, $i = 1,2,\dots,n_B$, $j = 1,2,\dots,n_A$ defined through the transmitter and receiver antennas of the legitimate user, and $g_{j,i}$, $i = 1,2,\dots,n_E$ defined through the transmitter and receiver antennas of the eavesdropper are assumed to be i.i.d. Rayleigh fading variables with the squared mean of unit magnitude $\Omega = E\left[|h_{j,i}|^2\right] = E\left[|g_{j,i}|^2\right] = 1, \quad \forall i,j.$ Here, $E[\cdot]$ denotes the expectation operator. Under the assumption that the channel estimation processes are perfectly done at Bob and Eve, the combined instantaneous SNR at each receiver output of Bob and Eve through the j^{th} transmit antenna would be obtained as: $\gamma_{B,j} = \bar{\gamma}_B \sum_{i=1}^{n_B}|h_{j,i}|^2$ and $\gamma_{E,j} = \bar{\gamma}_E \sum_{i=1}^{n_E}|g_{j,i}|^2$ where the subscripts B and E stand for the main link (i.e., the link between Alice and Bob) and the wiretap link (i.e., the link between Alice and Eve), respectively. Besides, $\bar{\gamma}_{B/E} = \frac{E_s}{N_{o,B/E}}$ are the average branch SNRs defined in terms of the average energy per symbol (E_s) and the one-sided power spectral densities of the additive white Gaussian noise (AWGN) ($N_{o,B}$ and $N_{o,E}$) at each receiver antenna of Bob and Eve, respectively. The instantaneous SNR $\gamma_{B,j}$ and $\gamma_{E,j}$ will follow Gamma distribution with the PDF and CDF given as $f_{L,j}(x) = \frac{x^{n_L-1}e^{-x/\bar{\gamma}_L}}{\bar{\gamma}_L^{n_L}\Gamma(n_L)}$ and $F_{L,j}(x) = \frac{\psi(n_L, x/\bar{\gamma}_L)}{\Gamma(n_L)} = 1 - e^{-x/\bar{\gamma}_L}\sum_{n=0}^{n_L-1}\frac{[x/\bar{\gamma}_L]^n}{\Gamma(n+1)}, \quad x \geq 0,$ respectively where $\Gamma(\cdot)$ and $\psi(\cdot)$ denote the Gamma and the incomplete Gamma function, respectively, and the label L becomes B and E for the main and wiretap links.

2.3.1 SNR Statistics of the Legitimate Link

For multi-antenna diversity systems employing M-TAS/Alamouti-STBC scheme, the first transmit antenna is employed regardlessly as seen at the top of Figure 1-(b), and the single transmit antenna which maximizes the received instantaneous SNR at Bob is selected among the remaining $K_M = n_A - 1$ antennas by comparing the instantaneous SNRs $\gamma_{B,j}$, $j = 1,2,\dots,n_A$: $\gamma_{B,max} = \max_{j=1,2,\dots,n_A}\{\gamma_{B,j}\}$. After switching the m^{th}, $m \in \{1,2,\dots,K_M\}$ best transmit antenna as a result of possible erroneous decoding, the resulted instantaneous post-processing SNR at the receiver output of the legitimate user will be

$$\gamma_{B,M}^{(m)} = \frac{1}{2}\left(\gamma_{B,(m)} + \gamma_{B,1}\right). \tag{2}$$

Here $\gamma_{B,(m)}$ denotes the m^{th} maximum instantaneous SNR among K_M transmit branch SNRs and $\gamma_{B,1}$ denotes the instantaneous combined SNR of the first transmit branch used regardlessly from the antenna selection process. As seen from Eq. (2), the total transmit power is equally distributed among two active transmit antennas. The statistics of the instantaneous combined SNR in Eq. (2) could be examined by evaluating the moment-generating function (MGF)

$$\mathcal{M}_{\gamma_{B,M}^{(m)}}(s;m) = E\left[e^{-\frac{s}{2}\gamma_{B,(m)}}\right]E\left[e^{-\frac{s}{2}\gamma_{B,1}}\right]. \tag{3}$$

Since the PDF expression related to the order statistics $\gamma_{B,(m)}$ has been defined in [21] as

$$f_{\gamma_{B,(m)}}(x;m) = \frac{\binom{n_A-2}{m-1} f_B(x)[F_B(x)]^{n_A-m-1}}{(n_A-1)^{-1}[1-F_B(x)]^{1-m}} \tag{4}$$

using the Laplace transform pair in [25, Eq. (2.2.1-2)], $\mathcal{M}_{\gamma_{B,(m)}}(s;m) = E\left[e^{-\frac{s}{2}\gamma_{B,(m)}}\right]$ is expressed as

$$\mathcal{M}_{\gamma_{B,(m)}}(s;m) = b_0 \sum_{n=0}^{n_A-m-1} b_1 \sum_{r=0}^{(n+m-1)(n_B-1)} \times \frac{\mu_{r,n+m-1,n_B}}{2^{r+n_B}} \frac{\Gamma(r+n_B)}{[s+2(n+m)/\bar{\gamma}_B]^{r+n_B}} \tag{5}$$

Where $\mu_{r,n+m-1,n_B}$ is the multinomial coefficient that has been defined in [23, Eq. (0.314)], $b_0 = \frac{n_A-1}{\bar{\gamma}_B^{n_B}\Gamma(n_B)}\binom{n_A-2}{m-1}$, $b_1 = (-1)^n\binom{n_A-m-1}{n}$. By substituting Eq. (5) and the MGF corresponding

to the single-diversity-branch SNR $E\left[e^{-\frac{s}{2}\gamma_{B,1}}\right] = \left[1+\frac{s\bar{\gamma}_B}{2}\right]^{-n_B}$ into Eq. (3), and applying inverse Laplace transform, the overall PDF of the combined instantaneous SNR for the M-TAS/STBC scheme could be obtained as:

$$f_{\gamma_{B,M}}(x;m) = b_0 \sum_{n} b_1 \sum_{r} b_2\, w(x). \tag{6}$$

Here, the parameter is $b_2 = \frac{\Gamma(r+n_B)\mu_{r,n+m-1,n_B}}{\bar{\gamma}_B^{n_B} 2^{r+2n_B}}$ and the x-dependent function $w(x)$ is obtained by after partial fraction decomposition (PFD) prescribed in [23, Eq. (2.102)] and the inverse Laplace transform:

$$w(x) = \begin{cases} \dfrac{x^{v_1+v_2-1}e^{-x\kappa_1}}{\Gamma(v_1+v_2)}, & n=0, m=1 \\ \displaystyle\sum_{j=1}^{2}\sum_{i=1}^{v_j} \frac{e_{ij}x^{i-1}e^{-x\kappa_j}}{\Gamma(i)}, & \text{otherwise.} \end{cases} \tag{7}$$

Here $v_j = n_B + r(j-1)$, $\kappa_1 = 2/\bar{\gamma}_B$, $\kappa_2 = \kappa_1(n+m)$ and e_{ij} denotes the PFD coefficients.

2.3.2 SNR Statistics of the Wiretap Link

The eavesdropper user, assumed to have perfect knowledge of the channel coefficients $g_{j,i}$, $j = 1,2,\dots,n_A$, $i = 1,2,\dots,n_E$, intercepts the information conveyed in the legitimate link (between Alice and Bob) by employing n_E-branch MRC. Since the wiretap channels can only make use of dual transmit branches that is accordingly switched due to the channel quality of the legitimate link, Eve could achieve no additional diversity gain provided by TAS but the STBC combining gain with the asymptotic diversity order of $2n_E$. The combined instantaneous SNR at the receiver output of Eve could be defined as

$$\gamma_E = \frac{1}{2}\left(\gamma_{E,t} + \gamma_{E,j\neq t}\right), t, j \in \{1,2,\dots,n_A\} \tag{8}$$

as given in [18] and [20]. With the help of independence between branch SNRs, the MGF of Eq. (8) might be easily obtained as $\mathcal{M}_{\gamma_E}(s) = \left[1+\frac{s\bar{\gamma}_E}{2}\right]^{-2n_E}$. By using the Laplace transform pair given in [25, Eq. (2.1.2-71)], the PDF of the combined SNR at the receiver output of Eve could be expressed as

$$f_{\gamma_E}(x) = \frac{x^{2n_E-1}e^{-2x/\bar{\gamma}_E}}{[\bar{\gamma}_E/2]^{2n_E}\Gamma(2n_E)}, x \geq 0. \tag{9}$$

As infered from the instantaneous combined SNR expression in Eq. (8) and its PDF in Eq. (9), the SNR statistics would have no dependency on TAS process, which later will be mentioned in Section V to provide advantages by means of communications secrecy.

3. FEEDBACK CHANNEL

For C-TAS/Alamouti-STBC technique, the feedback information between Bob and Alice conveys the single index corresponding to the antenna index vector that consists of the selected antenna indices. Since each combination of the antenna indices would correspond to a combination of ordered antenna indices (i.e., $\boldsymbol{o}_{C,m} = (o_{C,1}, o_{C,2})$), the index $m \in \{1,2,\dots,K_C\}$, will also represent the index of the vector that consists of ordinals. For a transmitter configuration of $n_A = 3$, there would only be $K_C = \binom{3}{2} = 3$ total combinations of the ordered antenna index vector (i.e., $(o_{C,1}, o_{C,2}) = (1,2)$, (1,3) and (2,3)), and the corresponding index of an ideally or erroneously activated antenna subset would be $m = 1,2,3$, respectively. The ordered index vector corresponding to the ideal antenna selection/switching case would be $\boldsymbol{o}_{C,1} = (1,2)$ that is meant to use the first and second best transmit antennas for two-branch STBC. However, due to the FEs, the feedback message might be decoded to other antenna index vectors $\boldsymbol{o}_{C,m}$, $m \neq 1$: $\boldsymbol{o}_{C,2} = (1,3)$ or $\boldsymbol{o}_{C,3} = (2,3)$. For different values of n_A, the antenna index combinations and the corresponding index values (i.e., m) might be easily associated and employed via a look-up table-like mechanism. Whereas for M-TAS/Alamouti-STBC technique, the feedback information conveys simply the single index corresponding to the selected antenna: $m \in \{1,2,\dots,K_M\}$.

The indices related to the selected transmit antenna subsets are fed back from Bob to Alice over an open (non-secure) and low-rate feedback link that is considered to have fading characteristics from a more realistic viewpoint [22]. Here, note that Eve might access the antenna indices determined by Bob, she will not be able attain any diversity gains since she has no information about the main link's CSI and even though she had, the indices are tailored due to the main link. However, in the case of active eavesdropping, Eve might contaminate the feedback channel from Bob to Alice in order to manipulate the antenna switching procedure through her favor.

The k_C- and k_M-bit feedback informations are sent to Alice followed by $\mathcal{L}_C$- and $\mathcal{L}_M$-phase shift keying (PSK) modulation where $\mathcal{L}_C = 2^{kc}$ and $\mathcal{L}_M = 2^{k_M}$. Due to degrading effects of the feedback channel with fading characteristics and the PCAs on the feedback channel, the index information might be decoded erroneously. For C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC cases, the antenna subset with an ideally or erroneously determined index vector $\boldsymbol{o}_{C,m}$ and the index m will be activated with the probabilities $p_m \triangleq \mathbf{P}\{\boldsymbol{o}_{C,m}\}$ and $p_m \triangleq \mathbf{P}\{\mathrm{m}\}$ while the other antennas are kept silent. The a priori probabilities are defined as $p_m = \sum_{j=1}^{K_{C/M}} p(s_j)\,\mathbf{P}(s_j \to s_m)$, where s_j denotes the baseband symbol belonging to $\mathcal{L}_{C/M}$-PSK modulation, $p(s_j)$ represents the occurrence probability of the symbol s_j and $\mathbf{P}(s_j \to s_m)$ is the pairwise error probability (PEP) related to the j^{th} and m^{th} symbols corresponding to the j^{th} and m^{th} best transmit antennas (or subsets). The feedback message, delivering $k_{C/M}$ bits in order to represent $K_{C/M}$ transmit antenna combinations, can be erroneously decoded to one of the $\mathcal{L}_{C/M} \geq K_{C/M}$ index values because of feedback imperfections and PCAs. This might cause the proper transmit antenna (subset) indices $1,2,\dots,K_{C/M}$ to be de-mapped to any of the improper transmit antenna (subset) indices $K_{C/M}+1, K_{C/M}+2, \dots, \mathcal{L}_{C/M}$ (which can be called feedback failure (FF)). Thus, assuming that each transmit antenna subset is selected equally-likely in the presence of FF as in [22], the a priori probabilities would be increased by the factor $\frac{1}{K_{C/M}}\sum_{j=K_{C/M}+1}^{\mathcal{L}_{C/M}} p_j$ yielding

$$p'_m = p_m + \frac{1}{K_{C/M}} \sum_{j=K_{C/M}+1}^{\mathcal{L}_{C/M}} p_j. \tag{10}$$

Hence, it would be possible to cover also the case of $\mathcal{L}_{C/M} > K_{C/M}$ rather than the limited case of $K_{C/M} = 2^b$, $b \in \mathbb{Z}^+$.

4. THE EFFECTS OF ACTIVE EAVESDROPPING

This section describes the effects of active eavesdropping on the average SOP values of TAS-aided diversity schemes (e.g., conventional and modified TAS/STBC, single TAS/MRC). In order to investigate the degradations on the communications secrecy, the eavesdropper is assumed to act not only to scrounge the information of the legitimate link but also to contaminate the TAS and antenna switching processes at Alice in order to manipulate the information flow from Alice in her favor. For this purpose, the active eavesdropping scheme based on pilot contamination attack (PCA) introduced in [5] has been involved. As could be found in Section 3 of [5], PCA might be applied by eavesdroppers in both in full-duplex and half-duplex communications modes. Hence, eavesdroppers would be able to contaminate the training and reverse training phases performed between Alice and Bob. Here, by assuming that the communications between Alice and Bob are half-duplex and Eve has syncronized to the timelines of the legitimate link, the training phase (i.e., run via the feedback transmission) between Alice and Bob could be misleaded by the intruding signal replica of Eve. Firstly, both Bob and Eve determines their optimal transmit antenna subsets individually. Then, during the feedback transmission phase (i.e., accomplished for the purpose of enhancing the communications

security between Bob and Alice via TAS), both Bob and Eve transmit their modulated symbols to the feedback decoder at Alice. Hence, because of the high-rate coherence between the feedback signals conveyed to Alice, the baseband symbols received at Alice could be expressed as in [5, Eq. (4)]:

$$y_{A,p} = \sqrt{P_{B,p}} h_{B,A} s_{m_B} + \sqrt{P_{E,p}} h_{E,A} s_{m_E} + \eta_A \qquad (11)$$

Here, $\sqrt{P_{B,p}}$ and $\sqrt{P_{E,p}}$ are the average power values related to the signal transmissions over the feedback links Bob→Alice and Eve→Alice, respectively. Similarly, $h_{B,A}$ and $h_{E,A}$ are the complex Gaussian-distributed channel gains of both links, s_{m_B} and s_{m_E} denote the unit-magnitude (i.e., $|s_{m_B}| = |s_{m_E}| = 1$) modulated PSK symbols those correspond to the transmit antenna subset indices m_B and m_E determined by Bob and Eve, respectively, and η_A is the complex AWGN with zero mean and variance of $N_{o,A}$. Since the average SNR of the legitimate feedback link is defined as $\bar{\gamma}_{FC}^{(L)} \triangleq P_{B,p}/N_{o,A}$, the average SNR of the eavesdropping link would be similarly obtained as $\bar{\gamma}_{FC}^{(E)} \triangleq P_{E,p}/N_{o,A}$. Assuming that the channel estimation at Alice is perfect, Alice would attempt to decode the received PSK symbol in order to determine the selected transmit antenna subset index and to enhance the communications security. After defining the power ratio $\Gamma_{FC} \triangleq P_{E,p}/P_{B,p}$, it is intuitively obvious to state that the increasing values of Γ_{FC} would cause Eve to contaminate and dominate the feedback information. In the case of Eve's relatively increased feedback transmit power, Alice would decide on the transmit antenna indices in the favor of Eve.

5. SECRECY PROBABILITY PERFORMANCES

After having the SNR statistics of both the main link and the wiretap link derived, we have focused on the examination of M-TAS/STBC schemes from the communications security perspective. In order to examine the SOP performances of multi-antenna diversity schemes that employ M-TAS/Alamouti-STBC techniques at the transmitter, we have focused on deriving the exact expressions for the PDF, CDF and average SOP. With the help of the derived performance metrics, it would be possible to examine the variation of the average SOP of the modified schemes due to the several system configurations and practical imperfections such as PCAs.

SOP is the probability that the secrecy capacity C_s is less than a specific transmission rate $\mathcal{R}_0$ (bits/channel-use) where C_s is expressed in [17, Eq. (6)] as

$$C_s = \begin{cases} \log_2\left(\dfrac{1+\gamma_B}{1+\gamma_E}\right), & \gamma_B > \gamma_E, \\ 0, & \gamma_B \le \gamma_E. \end{cases} \qquad (12)$$

The SOP that is formulated as $P_{SOP}(\mathcal{R}_0) = \Pr(C_s < \mathcal{R}_0)$ has been shown in [17, Eq. (14)] to be evaluated as

$$P_{SOP}(\mathcal{R}_0; m) = 1 - \int_{y=0}^{\infty} \int_{x=\beta(y)}^{\infty} f_{\gamma_{B,M}}(x; m)\, f_{\gamma_E}(y) dx dy \qquad (13)$$

where $\beta(y) = 2^{\mathcal{R}_0} y + 2^{\mathcal{R}_0} - 1$. Substituting the PDF expressions $f_{\gamma_{B,M}}(x; m)$ and $f_{\gamma_E}(y)$ given in Eq. (6) and Eq. (9) into Eq. (13) would result in

$$P_{SOP}(\mathcal{R}_0; m) = 1 - b_0 w_0 \sum_{n} b_1 \sum_{r} b_2\, W(\mathcal{R}_0). \qquad (14)$$

Here, $w_0 \triangleq [\bar{\gamma}_E/2]^{-2n_E}/\Gamma(2n_E)$ and $W(\mathcal{R}_0)$ is derived for the case of $n = 0, m = 1$ as

$$W^{(n=0,m=1)}(\mathcal{R}_0) = e^{-\kappa_1(2^{\mathcal{R}_0}-1)} \sum_{k=0}^{v_1+v_2-1} \frac{\kappa_1^{k-v_1-v_2}}{\Gamma(k+1)} \times \sum_{q=0}^{k} \binom{k}{q} \frac{2^{q\mathcal{R}_0}[2^{\mathcal{R}_0}-1]^{k-q}\Gamma(q+2n_E)}{[2^{\mathcal{R}_0}\kappa_1 + (1/\bar{\gamma}_E)]^{q+v_1+v_2}} \qquad (15)$$

and for the case of $n \neq 0, m \neq 1$ as

$$W^{(n\neq 0,m\neq 1)}(\mathcal{R}_0) = \sum_{j=1}^{2} \sum_{i=1}^{v_j} \sum_{k=0}^{v_j-1} \frac{e_{ij} e^{-\kappa_j(2^{\mathcal{R}_0}-1)} \kappa_j^{k-v_j}}{\Gamma(k+1)}$$

$$\times \sum_{q=0}^{k} \binom{k}{q} \frac{2^{q\mathcal{R}_0}[2^{\mathcal{R}_0}-1]^{k-q}\Gamma(q+2n_E)}{\left[2^{\mathcal{R}_0}\kappa_j + (1/\bar{\gamma}_E)\right]^{q+v_j}}. \quad (16)$$

Consequently, Eqs. (14)-(16) constitute the exact average SOP performance of the M-TAS/Alamouti-STBC scheme. Note that, the average SOP performance $P_{SOP}(\mathcal{R}_0; m)$ is only valid in the case of (ideally or erroneously) activating the m^{th} combination of transmit antenna subset $m \in \{1,2,\ldots,K_M\}$. Hence, the overall average SOP performances of the modified schemes would be obtained by simply weighting by the a priori probabilities p'_m defined by Eq. (10) and superposing the above-mentioned ordinal-dependent performance metrics over the entire possible transmit antenna indices and the subset combinations:

$$P_{SOP}(\mathcal{R}_0) = \sum_{m=1}^{K_M} p'_m \, P_{SOP}(\mathcal{R}_0; m). \quad (17)$$

6. NUMERICAL RESULTS

This section presents numerical results consisting of exact SOP performance results together with Monte Carlo simulations of diversity schemes that employ C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC under active eavesdropping effects. In order to examine the practical performances of these schemes and to highlight the robustness of the modified schemes, several performance results are provided in Figures 2 and 3 consisting of comparisons for different system and channel configurations. In both figures, the numerical results related to C-TAS/Alamouti-STBC, M-TAS/Alamouti-STBC and TAS/MRC schemes are depicted by black, blue and green curves respectively. Besides, by comparing the secrecy performances of M-TAS/STBC schemes to those of the conventional ones under same system and channel conditions, the enhancements gathered by the modified schemes have been exhibited. For this purpose, the SOP values of the C-TAS/STBC schemes under passive eavesdropping conditions (perfect feedback w/o PCAs) are evaluated by using the theoretical expressions provided by the pioneering work in [20]. For benchmarking purposes, the average SOP performance results of single TAS/MRC scheme have been included in Figures 2 and 3. The SOP performances of both the conventional schemes in the presence of PCAs and all cases of single TAS/MRC scheme are evaluated via Monte Carlo simulations. Besides, the simple decoding procedure for the received feedback signal defined in Eq. (11) has been performed via Monte Carlo simulations that would result in the a priori probabilities given in Eq. (10).

With the aim of examining the variation in the average SOP performance of TAS/STBC and single TAS/MRC schemes in the presence of PCAs, we have focused on the scenario with the parameters $n_A = 3$, $n_B = 2$, $n_E = 1$, $\mathcal{R}_0 = 1$ bit/s/Hertz, $\bar{\gamma}_E = 5$ dB, $\bar{\gamma}_{FC}^{(L)} = 0$ dB. In Figure 2, the effects of active eavesdropping based on PCA are demonstrated in the presence of a noisy feedback channel (i.e., $N_{o,A} \neq 0$).

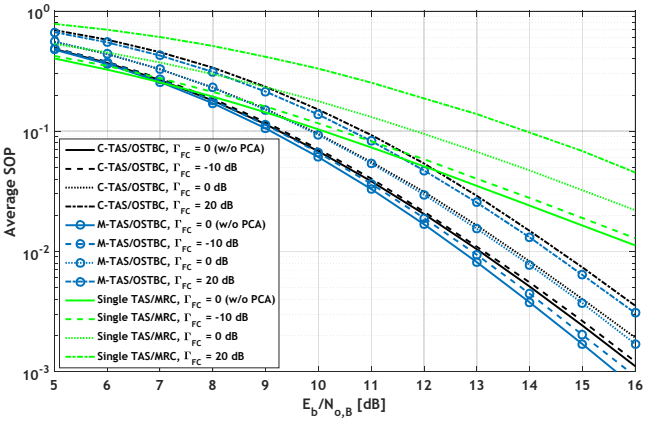

Figure 2 Average SOP of TAS/STBC and single TAS/MRC schemes for $n_A = 3$, $n_B = 2$, $n_E = 1$, $\mathcal{R}_0 = 1$ bit/s/Hertz, $\bar{\gamma}_E = 5$ dB, $\bar{\gamma}_{FC}^{(L)} = 0$ dB and under the effects of PCA ($\Gamma_{FC,dB} \in \{-\infty, -10, 0, 20\}$)

In Figure 2, the C-TAS/Alamouti-STBC, M-TAS/Alamouti-STBC and single TAS/MRC schemes are seen to face degradations with the increasing values of Γ_{FC}. When compared to the single TAS/MRC scheme which severely suffers from vanishing transmit diversity order (i.e., unity as the non-transmit-diversity SISO/SIMO

schemes) in the presence of practical imperfections such as PCAs, C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC schemes keep maintaining at least the transmit diversity order achievement of twice the SISO/SIMO schemes. Besides, the modified schemes are seen to achieve average SNR gains of 0.35 dB, 0.25 dB, 0.1 dB and 0.2 dB for $\Gamma_{FC,dB} \in \{-\infty, -10, 0, 20\}$, respectively at an average SOP of 10^{-2} when compared to the conventional schemes. This clearly shows that the modified schemes are more robust against PCAs when compared to the conventional (and also to single TAS/MRC) schemes.

Another examination on SOP performances of single TAS/MRC, C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC schemes has been made by considering a noise-free feedback channel (i.e., $N_{o,A} = 0$) and demonstrated in Figure 3 for $n_A = 4$, $n_B = 2$, $n_E = 2$, $\mathcal{R}_0 = 1$ bit/s/Hertz, $\bar{\gamma}_E = 5$ dB and $\Gamma_{FC,dB} \in \{-\infty, -10, 0, 20\}$.

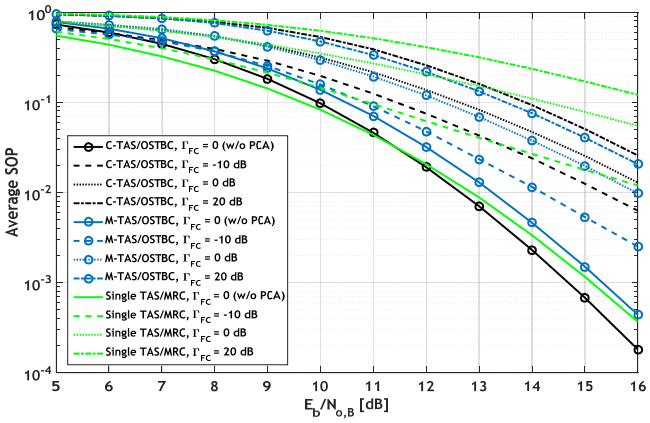

Figure 3 Average SOP of the TAS/STBC and single TAS/MRC schemes for $n_A = 4$, $n_B = 2$, $n_E = 2$, $\mathcal{R}_0 = 1$ bit/s/Hertz, $\bar{\gamma}_E = 5$ dB, $\bar{\gamma}_{FC}^{(L)} \to \infty$ and under the effects of PCA ($\Gamma_{FC,dB} \in \{-\infty, -10, 0, 20\}$)

As seen from the SOP curves given in Figure 3, for the ideal case of $\bar{\gamma}_{FC}^{(L)} \to \infty$ and $\Gamma_{FC,dB} \to -\infty$ (i.e., perfect feedback w/o PCAs), single TAS/MRC scheme outperforms both the C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC schemes in lower SNR (i.e., < 10 dB) region. For higher SNR values, the C-TAS/Alamouti-STBC scheme achieves the best SOP performance among three schemes. However, as the dominance of the Eve's contamination signal becomes evident (by the increasing values of Γ_{FC}), the M-TAS/Alamouti-STBC schemes are seen to provide additional SNR savings when compared to both single TAS/MRC and C-TAS/Alamouti-STBC schemes. Similar to the cases in Figure 2, employing modified schemes instead of the conventional ones provides average SNR savings of 0.6 dB, 0.3 dB and 0.37 dB, respectively for $\Gamma_{FC,dB} = -10, 0, 20$ at an average SOP of 10^{-1}.

7. CONCLUSIONS

We have examined the advantages obtained by the usage of the M-TAS/Alamouti-STBC schemes at the transmitter of a closed-loop diversity scheme from the perspective of physical layer security. The analytical derivations and the numerical results presented within this paper have exhibited the robustness of the modified scheme also to the active eavesdropping techniques such as PCAs when compared to the conventional scheme. Considering fading channel characteristics at both the legitimate/wiretap links and the feedback links, statistics related to the output SNR and the performance metrics have been presented in the presence of PCAs. SOP curves have shown that, in the presence of PCAs both schemes maintain the asymptotic diversity order that is provided by the pure Alamouti-STBC transmission and the optimal-diversity reception provided by the MRC. Analytical and numerical performance results clearly point out the potential of secrecy performance degradations that might be faced by both the C-TAS/Alamouti-STBC and M-TAS/Alamouti-STBC schemes due to the feedback imperfections caused by PCAs, and the superiority of M-TAS/Alamouti-STBC scheme to C-TAS/Alamouti-STBC scheme in the presence of PCAs.

Consequently, the considerable average SNR gain achieved against the conventional scheme in the presence of PCAs, provide the modified scheme to maintain significant importance in

real-world wireless communications system design from also the perspective of communications secrecy.

The authors think that further researches would be worth to be carried out on proposing novel antenna selection strategies and optimizing them by paying regard to probable imperfections in channel estimation and feedback processes (e.g., channel estimation errors, feedback delay and errors, and active eavesdropping).

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, pp. 656-715, Oct. 1949.

[2] B. Schneier, "Cryptographic design vulnerabilities," *Comput.*, vol. 31, no. 9, pp. 29-33, Sep. 1998.

[3] A. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355-1-387, Oct. 1975.

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

[5] X. Zhou, B. Maham and A. Hjørungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Trans. Wire. Commun.*, vol. 11, no. 3, pp. 903-907, March 2012.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part I: the MISOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part II: the MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[9] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509-511, May 2011.

[10] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853-860, Sep. 2011.

[11] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[12] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640-649, Sep. 2011.

[13] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858-3871, September 2016.

[14] Y. Zhang, Y. Ko, R. Woods, and A. Marshall, "Defining spatial secrecy outage probability for exposure region-based beamforming," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 2, pp. 900-912, February 2017.

[15] H. Alves, M. De C. Tomé, P. H. J. Nardelli, C. H. M. De Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter," *IEEE Access*, vol. 4, pp. 4861-4873, 2016.

[16] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[17] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis

for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Foren. Sec*., vol. 10, no. 8, pp. 1617-1619, August 2015.

[18] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Foren. Sec.*, vol. 10, no. 11, pp. 2435-2446, November 2015.

[19] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 1, pp. 214-225, Jan. 2016.

[20] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett*., vol. 17, no. 9, pp. 1754-1757, Sept. 2013.

[21] S. Yan, N. Yang, R. Malaney, J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wirel. Commun.*, vol. 13, no. 3, pp. 1656-1667, March 2014.

[22] A. F. Coşkun, O. Kucur, "Feedback-rate efficient transmit antenna selection/Alamouti scheme with robust error performance in the presence of feedback errors," *IEEE Comm. Lett*., vol. 17, no. 5, pp. 908-911, May 2013.

[23] I. Gradshteyn, I. Ryzhik, *Tables of Integrals, Series and Products*, Academic Press: San Diego CA, 1994.

[24] H. A. David and H. N. Nagaraja, *Order Statistics, 3rd ed.* Hoboken, NJ: Wiley, 2003.

[25] P. Prudnikov, Y. A. Brychkov, O. I. Marichev, *Integrals and Series, Vol. 5*, Gordon and Breach Science Publishers: New York, 1986.