Published in IET Communications
Received on 3rd July 2013
Revised on 31st August 2013
Accepted on 9th October 2013
doi: 10.1049/iet-com.2013.0564

Special Issue: Secure Physical Layer Communications

ISSN 1751-8628

Secure multiple-input single-output communication – Part II: δ-secrecy symbol error probability and secrecy diversity

Thang Van Nguyen[1], Youngmin Jeong[1], Jin Sam Kwak[2], Hyundong Shin[1]

[1]Department of Electronics and Radio Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 446-701, Korea
[2]WILUS Institute of Standards and Technology, 263-2 Yangjae-dong, Seocho-gu, Seoul 137-894, Korea
E-mail: hshin@khu.ac.kr

Abstract: The authors consider secure beamforming with artificial noise in a multiple-input single-output multiple-eavesdropper (MISOME) wiretap channel, where a transmitter has access to full channel state information (CSI) of a legitimate channel but only partial CSI of eavesdropper channels. In the second part of this study, the authors first put forth a new notion of symbol error probability (SEP) for confidential information – called the 'δ-secrecy SEP' – to connect the reliability and confidentiality of the legitimate communication in MISOME wiretap channels. For single-antenna colluding and non-colluding eavesdroppers, the authors then quantify the diversity impact of secure beamforming with artificial noise on the δ-secrecy SEP and show that the artificial -noise strategy with n_t transmit antennas preserves the secrecy diversity of order $n_t - n_e$ for n_e colluding eavesdroppers and $n_t - 1$ for n_e non-colluding eavesdroppers, respectively. In addition, the authors determine the optimal power allocation between the information-bearing signal and artificial noise to minimise the δ-secrecy SEP in the presence of weak or strong eavesdroppers, and further develop the switched power allocation for general eavesdropping attacks.

1 Introduction

Multiple-antenna systems have been known as an efficient solution to increase the achievable communication rate and reliability as well as physical-layer security in wireless channels [1–18]. The notion of secrecy outage probability along with the ε-outage secrecy capacity was introduced for a single-antenna wiretap channel in [19], extended for multiple-antenna eavesdroppers in [20] and refined in [21] to discriminate between the reliability and secrecy in an outage event. Using this secrecy outage reformulation, the optimal power allocation between the information-bearing signal and artificial noise was investigated for a multiple-input single-output (MISO) wiretap channel [22].

Communication over a wireless channel is unreliable mainly because of a significant probability that the channel is in deep fade. One of the effective ways to mitigate this problem is to realise the 'diversity' – that is, providing more resolvable signals that fade independently. Since these resolvable signals are rarely in deep fade at the same time, the diversity serves to enhance the communication reliability, leading to increase a slope of error probability or outage probability at high signal-to-noise ratio (SNR). More generally, the diversity-multiplexing tradeoff (DMT) for multiple-input multiple-output (MIMO) communication was introduced in [3] as a 'high SNR' characterisation of the 'reliability–rate' tradeoff [6]. The maximum diversity gain can be attained without requiring channel state information (CSI) at the transmitter [7–10]. For wiretap channels, however, the secure diversity relies strongly on the amount of CSI at the transmitter [23–26] In particular, the secure DMT of MIMO wiretap channels was analysed in [23] for both cases of no CSI and full CSI of legitimate and eavesdropper channels, where it has been shown that the eavesdropper impacts to secrecy diversity at both the transmitter and receiver for the no CSI case but only transmit antennas for the full CSI case. Furthermore, the zero-forcing (ZF) and artificial-noise strategies were suggested to achieve the maximum secure diversity when the CSI of only the eavesdropper or legitimate channel is available at the transmitter, respectively. The secure DMT was also analysed for MIMO single-relay channels [24], MIMO multiple-relay channels [25] and MIMO wiretap channels with a ZF transmit scheme at finite SNR [26].

As in the first part of the paper [18], we consider secure beamforming with artificial noise in a MISO multiple-eavesdropper (MISOME) wiretap channel, where a transmitter has access to full CSI of a legitimate channel but only partial CSI of eavesdropper channels. To characterise the diversity impact, we deal with two types of eavesdroppers in this second part of the paper: 'colluding' and 'non-colluding' eavesdroppers. The colluding eavesdroppers can exchange and combine information for the best adversarial attack. The main contributions of the second part can be summarised as follows:

- We put forth a new notion of symbol error probability (SEP) of confidential information – called the 'δ-secrecy

SEP' – to connect the reliability and confidentiality of the legitimate communication (see Definition 2). We then exemplify the δ-secrecy SEP of M-ary phase-shift keying (M-PSK) for secure beamforming with artificial noise in the MISOME wiretap channel for both colluding and non-colluding eavesdropping attacks (see Theorem 1).

- We assess the 'secrecy diversity' – that is, the high-SNR slope of the δ-secrecy SEP curve – as a counterpart to the ordinary diversity order without accounting for physical-layer security. We show that the artificial-noise strategy with n_t transmit antennas preserves the secrecy diversity of order $n_t - n_e$ and $n_t - 1$ for n_e single-antenna colluding and non-colluding eavesdroppers, respectively, whereas this high-SNR slope vanishes with no artificial noise, unveiling the fact that 'reliable and confidential' communication is infeasible in this case (see Theorem 2).
- We treat the power allocation problem between the information-bearing signal and artificial noise to minimise the δ-secrecy SEP. We first determine the power allocation solutions for 'weak' (low SNR) and 'strong' (high SNR) eavesdroppers (see Theorems 3 and 4); and then leverage these solutions to develop a switched power allocation strategy for general eavesdropping attacks.

The rest of the paper is organised as follows. In Section 2, we present the system model. Section 3 introduces the notions of the δ-secrecy SEP and secrecy diversity. In Section 4, we treat the power allocation problem to minimise the δ-secrecy SEP. Numerical examples are provided in Section 5 and conclusions are finally given in Section 6. We shall use the same notation and symbols as in the first part of the paper [18].

2 System model

We consider a MISOME wiretap channel, as illustrated in Fig. 1, where an n_t antenna transmitter (Alice) sends confidential messages to a single-antenna legitimate receiver (Bob) in the presence of n_e single-antenna passive eavesdroppers (Eves) that only receive the signal from the transmitter without transmitting any jamming signals to the receiver. The received signals at the receiver and eavesdroppers are given, respectively, by

$$y_r = \sqrt{\frac{\mathrm{snr}_r}{n_t}}\boldsymbol{h}_r\boldsymbol{x} + z_r \tag{1}$$

$$y_{ek} = \sqrt{\frac{\mathrm{snr}_e}{n_t}}\boldsymbol{h}_{ek}\boldsymbol{x} + z_{ek}, \quad k = 1, 2, \ldots, n_e \tag{2}$$

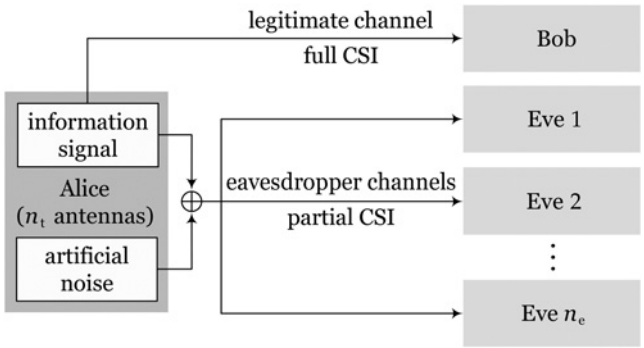

Fig. 1 *MISOME wiretap channel with artificial noise*

where $\boldsymbol{x} \in \mathbb{C}^{n_t}$ is the transmitted signal satisfying the power constraint $\mathbb{E}\{\| \boldsymbol{x} \|^2\} = 1$; $\boldsymbol{h}_r \sim \mathcal{N}_{1,n_t}$ and $\boldsymbol{h}_{ek} \sim \mathcal{N}_{1,n_t}$ are Rayleigh-fading channel gains from the transmitter to the receiver and the kth eavesdropper, respectively; $z_r \sim \mathcal{N}_{1,1}$ and $z_{ek} \sim \mathcal{N}_{1,1}$ are additive white Gaussian noises; and snr_r and snr_e are the average received SNRs at the receiver and eavesdroppers without employing artificial noise, respectively. For brevity, we set the same average SNR for all eavesdropper links. However, we can treat a general case of transmitter-to-eavesdropper SNRs using the superanalysis methodology in [12]. All the random quantities $\boldsymbol{x}$, $\boldsymbol{h}_r$, $\boldsymbol{h}_{ek}$, z_r and z_{ek} are statistically independent.

As in [18], the transmitter utilises artificial noise to cause interference to the eavesdroppers, leading to the transmitted signal

$$\boldsymbol{x} = \sqrt{\lambda}\boldsymbol{u}_I s_I + \sqrt{\frac{1-\lambda}{n_t - 1}}\boldsymbol{U}_A \boldsymbol{s}_A \tag{3}$$

and the received signals at the legitimate receiver and the kth eavesdropper as follows

$$y_r = \sqrt{\lambda \frac{\mathrm{snr}_r}{n_t}} \| \boldsymbol{h}_r \| s_I + z_r \tag{4}$$

$$y_{ek} = \sqrt{\lambda \frac{\mathrm{snr}_e}{n_t}} g_{Ik} s_I + \sqrt{\frac{1-\lambda}{n_t - 1}\frac{\mathrm{snr}_e}{n_t}} \boldsymbol{g}_{Ak} \boldsymbol{s}_A + z_{ek} \tag{5}$$

where s_I, $\boldsymbol{s}_A$, $\boldsymbol{u}_I$, $\boldsymbol{U}_A$ and λ are defined in [18, eq. (3)], $g_{Ik} \triangleq \boldsymbol{h}_{ek}\boldsymbol{u}_I$ and $\boldsymbol{g}_{Ak} \triangleq \boldsymbol{h}_{ek}\boldsymbol{U}_A$. Since $[\boldsymbol{u}_I \ \boldsymbol{U}_A]$ is a unitary matrix, $g_{Ik} \sim \mathcal{N}_{1,1}$ and $\boldsymbol{g}_{Ak} \sim \mathcal{N}_{1,n_t-1}$ are statistically independent.

3 δ-secrecy SEP and secrecy diversity

From the information-theoretic perspective, secure communication can be characterised by the secrecy outage probability (in addition to the ergodic secrecy rate), defined as the probability that the instantaneous achievable secrecy rate is less than a target secrecy rate [19, 27]. However, these measures fail to provide insight into the tradeoff between the communication reliability of the legitimate link and the confidentiality against the eavesdropper link. In practical coding systems, the coding complexity is finite and the codeword length cannot span to infinity for arbitrarily reliable communication. Hence, a stronger form of the channel coding theorem can be pursued to determine the exponentially decaying behaviour of the error probability as a function of the codeword length and communication rate: for example, the random coding error exponent [6] and the channel dispersion [28]. Instead of this difficult analysis, we now deal with a diversity aspect as in a no confidential counterpart. In this section, we introduce a new notion of error probability of the confidential information to connect the reliability and confidentiality (in terms of secrecy outage) of the legitimate communication, and analyse the diversity effect of secure beamforming with artificial noise on this secrecy error probability.

doi: 10.1049/iet-com.2013.0564

3.1 δ-secrecy SEP

Definition 1 (secrecy score): Let Γ_r and Γ_e be the instantaneous SNR and signal-to-interference-plus-noise ratio (SINR) at the legitimate receiver and the eavesdropper, respectively. Then, the 'secrecy score' Δ_s is defined as

$$\Delta_s = \frac{1+\Gamma_r}{1+\Gamma_e} \tag{6}$$

Remark 1: With Gaussian signalling, the secrecy score Δ_s reflects the perfect secrecy since the instantaneous secrecy rate can be written as $[\ln \Delta_s]^+$. For discrete signalling such as M-PSK or M-ary quadrature amplitude modulation, Δ_s can serve as a secrecy constraint to protect the legitimate communication in the presence of eavesdroppers. The SNR and SINR have been used as secrecy constraints to design secure beamforming [29, 30].

Definition 2 (δ-secrecy SEP): Let $\hat{s}_I$ be the decoded information at the legitimate receiver. Then, the 'δ-secrecy SEP', denoted by $P_e^{(s)}(\delta)$, for $\delta \geq 1$ and $0 < \lambda \leq 1$ is defined as the probability that either the secrecy score Δ_s is smaller than δ or the legitimate receiver decodes incorrectly the confidential information when Δ_s is larger than δ given that s_I is transmitted. That is,

$$P_e^{(s)}(\delta) = \mathbb{P}\{\mathcal{O} \cup \mathcal{E} | s_I \text{ transmitted}\} \tag{7}$$

where $\mathcal{O} = \{\Delta_s < \delta\}$ is the secrecy outage event, $\mathcal{E} = \{\hat{s}_I \neq s_I, \Delta_s \geq \delta\}$ is the error event and δ is a predesigned parameter that reveals the level of confidentiality.

Remark 2: For any signalling, the secrecy constraint will not be guaranteed if $\Delta_s < 1$. Therefore it is reasonable to only consider the case of $\delta \geq 1$. Note that we can determine (adaptively to $\boldsymbol{h}_r$) the optimal value of λ that minimises the δ-secrecy SEP. However, the power allocation $\lambda \in (0, 1)$ between the information and artificial noise does not affect the high-SNR slope of the δ-secrecy SEP curve (see Theorem 2). Hence, we can set λ to a deterministic value in (0, 1) for a simple design – for example, the 'decisive power allocation' [18, Theorem 2]. For the colluding case (which includes a single n_e-antenna eavesdropper [18]), the eavesdroppers can exchange and combine information to obtain the best attack, whereas each eavesdropper extracts information by own herself for the non-colluding case.

(1) *Colluding eavesdroppers:* In this case, we can view n_e single-antenna eavesdroppers as an n_e-antenna eavesdropper. Let Γ_e° be the instantaneous SINR of the n_e-antenna eavesdropper after combining information. Then, Γ_r and Γ_e° are given, respectively, by

$$\Gamma_r = \lambda \frac{\text{snr}_r}{n_t} \| \boldsymbol{h}_r \|^2 \tag{8}$$

$$\Gamma_e^\circ = \lambda \frac{\text{snr}_e}{n_t} \boldsymbol{g}_I^\dagger \left(\mathbf{I} + \frac{1-\lambda}{n_t - 1} \frac{\text{snr}_e}{n_t} \boldsymbol{G}_A \boldsymbol{G}_A^\dagger \right)^{-1} \boldsymbol{g}_I \tag{9}$$

where $\boldsymbol{g}_I \triangleq [g_{I1} \quad g_{I2} \quad \cdots \quad g_{In_e}]^T$, $\boldsymbol{G}_A \triangleq [\boldsymbol{g}_{A1}^T \quad \boldsymbol{g}_{A2}^T \quad \cdots \quad \boldsymbol{g}_{An_e}^T]^T$ and the superscript $(\cdot)^T$ denotes the transpose. The cumulative distribution functions of Γ_r and Γ_e° are given by [18]

$$F_{\Gamma_r}(x) = 1 - \sum_{k=0}^{n_t-1} \frac{1}{k!} \left(\frac{n_t}{\lambda \text{snr}_r} x \right)^k e^{-(n_t/\lambda \text{snr}_r)x}, \quad x \geq 0 \tag{10}$$

and (11)

where $a_\lambda = ((1-\lambda)/(n_t - 1))(\text{snr}_e/n_t)$. Therefore, it follows from (10), (11), and [18, eq. (6)] that

$$\mathbb{P}\{s_I \text{ transmitted}\} = 1 - F_{\Gamma_e^\circ}(\gamma_\lambda^\circ) \tag{12}$$

where

$$\gamma_\lambda^\circ \triangleq \exp\left\{ \sum_{i=0}^{n_e-1} \sum_{j=0}^{n_e-1-i} \binom{n_t-1}{j} \frac{a_\lambda^j}{i!} \mathcal{I}_{n_t-1}^{i+j} \left(0, \lambda \frac{\text{snr}_e}{n_t}, a_\lambda\right) \right\} - 1 \tag{13}$$

and $\mathcal{I}_n^m(a, b, c)$ is given in [18, eq. (29)].

(2) *Non-colluding eavesdroppers:* In this case, the strongest eavesdropper directly decides the secrecy rate of the legitimate channel. Let $\Gamma_e^\star$ be the instantaneous SINR of the strongest eavesdropper. Then, $\Gamma_e^\star$ is given by

$$\Gamma_e^\star = \max_k \lambda \frac{\text{snr}_e}{n_t} \frac{|g_{Ik}|^2}{1 + a_\lambda \| \boldsymbol{g}_{Ak} \|^2} \tag{14}$$

It follows readily from (11) that

$$F_{\Gamma_e^\star}(z) = \left[1 - \left(1 + \frac{1-\lambda}{n_t - 1} \frac{z}{\lambda} \right)^{1-n_t} e^{-(n_t/(\lambda \text{snr}_e))z} \right]^{n_e}, \quad z \geq 0 \tag{15}$$

Using again (15), we have

$$\mathbb{P}\{s_I \text{ transmitted}\} = 1 - F_{\Gamma_e^\star}(\gamma_\lambda^\star) \tag{16}$$

where

$$\gamma_\lambda^\star \triangleq \exp\left\{ \sum_{i=1}^{n_e} \binom{n_e}{i} (-1)^{i-1} \mathcal{I}_{(n_t-1)i}^0 \left(0, \frac{\lambda}{i} \frac{\text{snr}_e}{n_t}, \frac{a_\lambda}{i}\right) \right\} - 1 \tag{17}$$

In the following, we exemplify the δ-secrecy SEP for M-PSK signalling. For any arbitrary two-dimensional signalling constellation with polygonal decision boundaries, we can also obtain the δ-secrecy SEP using Craig's SEP expression (see, e.g. [12, eq. (20)]).

$$F_{\Gamma_e^\circ}(z) = 1 - \sum_{i=0}^{n_e-1} \sum_{j=0}^{n_e-1-i} \binom{n_t-1}{j} \frac{a_\lambda^j}{i!} \left(\frac{n_t}{\lambda \text{snr}_e} \right)^{i+j} \frac{z^{i+j}}{\left(1 + (1 - \lambda/n_t - 1)(1/\lambda)z\right)^{n_t-1}} e^{-(n_t/\lambda \text{snr}_e)z}, \quad z \geq 0 \tag{11}$$

Theorem 1: Let

$$\left(\Gamma_{\mathrm{e}},\, \gamma_{\lambda},\, [[i,j]]\right) = \begin{cases} \left(\Gamma_{\mathrm{e}}^{\circ},\, \gamma_{\lambda}^{\circ},\, i\right), & \text{if colluding} \\ \left(\Gamma_{\mathrm{e}}^{\star},\, \gamma_{\lambda}^{\star},\, j\right), & \text{if non-colluding} \end{cases} \tag{18}$$

Then, for any $\delta \geq 1$ and $\lambda \in (0, 1]$, the δ-secrecy SEP of M-PSK for secure beamforming with artificial noise is given by

$$P_{\mathrm{e}}^{(\mathrm{s})}(\delta) = P_1 + P_2 \tag{19}$$

with (20) and (21)

where $c_{\mathrm{PSK}} = \sin^2(\pi/M)$, $\Theta = \pi - (\pi/M)$, $\varrho_{\lambda} = [(\gamma\lambda + 1)/\delta - 1]^{+}$, $\xi_{\lambda} = \max\{\delta - 1,\, \varrho_{\lambda}\}$ and

$$\chi_{\theta k} \triangleq \left(\frac{n_{\mathrm{t}}}{\lambda \mathrm{snr}_{\mathrm{r}}} + [[1,\, k]]\frac{n_{\mathrm{t}}}{\lambda\delta\mathrm{snr}_{\mathrm{e}}} + \frac{c_{\mathrm{PSK}}}{\sin^2\theta}\right)^{-1} \tag{22}$$

Proof: See Appendix 1. □

Remark 3: The notion of δ-secrecy SEP can be viewed as a joint-refinement version of the SEP and secrecy outage probability that is usually used to evaluate the secrecy level of channels. Herein, we incorporate the secrecy outage event $\mathcal{O}$ with the error event $\mathcal{E}$ of the legitimate receiver in a joint formula such that the impact of confidentiality to the error probability can be considered. Note that the connection (reliability) outage and secrecy outage were defined in [31] as two separate events. The secrecy outage probability was also refined in [21] to treat the confidentiality conditioned on message transmission. In contrast, the δ-secrecy SEP $P_{\mathrm{e}}^{(\mathrm{s})}(\delta)$ captures both the reliability and secrecy events in a unifying formula in order to adapt for practical designs, still exhibiting the properties of the secrecy outage probability and the error probability as well as accounting for the conditional probability of message transmission.

3.2 Secrecy diversity

We now quantify the diversity impact of secure beamforming with artificial noise on a high-SNR slope of the δ-secrecy SEP curve as a counterpart to the ordinary diversity order without accounting for the intrinsic secrecy.

Theorem 2 (achievable secrecy diversity order): Let

$$d_{\mathrm{s}} \triangleq \lim_{\substack{\mathrm{snr}_{\mathrm{r}},\mathrm{snr}_{\mathrm{e}} \to \infty \\ \frac{\mathrm{snr}_{\mathrm{e}}}{\mathrm{snr}_{\mathrm{r}}} \to \alpha}} \frac{-\log P_{\mathrm{e}}^{(\mathrm{s})}(\delta)}{\log \mathrm{snr}_{\mathrm{r}}} \tag{23}$$

be the achievable secrecy diversity order of δ-secrecy SEP. Then, we have

$$d_{\mathrm{s}} = \begin{cases} n_{\mathrm{t}} - [[n_{\mathrm{e}},\, 1]], & \text{if } 0 < \lambda < 1 \\ 0, & \text{if } \lambda = 1 \end{cases} \tag{24}$$

Proof: Note that

$$\begin{aligned} &\mathbb{P}\{\mathcal{O}|s_{\mathrm{I}} \text{ transmitted}\} \leq P_{\mathrm{e}}^{(\mathrm{s})}(\delta) \\ &\leq \mathbb{P}\{\mathcal{O}|s_{\mathrm{I}} \text{ transmitted}\} + \mathbb{P}\{\hat{s}_{\mathrm{I}} \neq s_{\mathrm{I}}|s_{\mathrm{I}} \text{ transmitted}\} \end{aligned} \tag{25}$$

Since s_{I} is transmitted with probability one at high SNR, we can ignore the condition event 's_{I} transmitted' in (25). For $0 < \lambda < 1$, it follows from (46) that (26)

$$\begin{aligned} P_1 \triangleq\, &\mathbb{P}\{\mathcal{O}|s_{\mathrm{I}} \text{ transmitted}\} \\ =\, &\frac{1 - F_{\Gamma_{\mathrm{e}}}(\varrho_{\lambda})}{1 - F_{\Gamma_{\mathrm{r}}}(\gamma_{\lambda})}\left[F_{\Gamma_{\mathrm{r}}}(\delta\varrho_{\lambda} + \delta - 1) - F_{\Gamma_{\mathrm{r}}}(\gamma_{\lambda})\right] + \frac{1}{1 - F_{\Gamma_{\mathrm{r}}}(\gamma_{\lambda})}\frac{e^{((1-\delta)n_{\mathrm{t}}/\lambda\mathrm{snr}_{\mathrm{r}})}}{(n_{\mathrm{t}} - 1)!}\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}}\sum_{i=1}^{n_{\mathrm{e}}}\sum_{j=0}^{[[n_{\mathrm{e}}-i,0]]} \\ &\times \sum_{k=0}^{n_{\mathrm{t}}-1}\left\{(-1)^{[[0,i-1]]}\binom{n_{\mathrm{e}}}{[[0,\, i]]}\binom{n_{\mathrm{t}} - 1}{j}\binom{n_{\mathrm{t}} - 1}{k}\frac{a_{\lambda}^{j-1}}{[[i - 1,\, 0]]!}(\delta - 1)^{n_{\mathrm{t}}-1-k}\left(\frac{n_{\mathrm{t}}}{\lambda\delta\mathrm{snr}_{\mathrm{e}}}\right)^{-k-1}\right. \\ &\times \left(\left[[1,\, i]\right] + \delta\frac{\mathrm{snr}_{\mathrm{e}}}{\mathrm{snr}_{\mathrm{r}}}\right)^{[[1-i,0]]-j-k}\mathcal{I}_{(n_{\mathrm{t}}-1)[[1,i]]-1}^{[[i-1,0]]+j+k}\left(\left(\frac{\delta}{\mathrm{snr}_{\mathrm{r}}} + \frac{[[1,\, i]]}{\mathrm{snr}_{\mathrm{e}}}\right)\frac{n_{\mathrm{t}}}{\lambda}\varrho_{\lambda},\, \frac{a_{\lambda}}{[[1,\, i]] + \delta(\mathrm{snr}_{\mathrm{e}}/\mathrm{snr}_{\mathrm{r}})},\right. \\ &\left.\left.\frac{a_{\lambda}}{[[1,\, i]] + \delta(\mathrm{snr}_{\mathrm{e}}/\mathrm{snr}_{\mathrm{r}})}\right)\right\} \end{aligned} \tag{20}$$

$$\begin{aligned} P_2 \triangleq\, &\mathbb{P}\{\mathcal{E}|s_{\mathrm{I}} \text{ transmitted}\} \\ =\, &\frac{1}{\pi}\int_0^{\Theta}\left(1 + \frac{\lambda\mathrm{snr}_{\mathrm{r}}}{n_{\mathrm{t}}}\frac{c_{\mathrm{PSK}}}{\sin^2\theta}\right)^{-n_{\mathrm{t}}}\frac{1 - F_{\Gamma_{\mathrm{r}}}\left(\left(1 + (\lambda\mathrm{snr}_{\mathrm{r}}/n_{\mathrm{t}})(c_{\mathrm{PSK}}/\sin^2\theta)\right)\xi_{\lambda}\right)}{1 - F_{\Gamma_{\mathrm{r}}}(\gamma_{\lambda})}\,\mathrm{d}\theta \\ &- \frac{(n_{\mathrm{t}}/\lambda\mathrm{snr}_{\mathrm{r}})^{n_{\mathrm{t}}}}{1 - F_{\Gamma_{\mathrm{r}}}(\gamma_{\lambda})}\sum_{i=1}^{n_{\mathrm{e}}}\sum_{j=0}^{[[n_{\mathrm{e}}-i,0]]}\sum_{k=0}^{[[i+j-1,0]]}\left\{(-1)^{[[0,i-1]]}\binom{n_{\mathrm{e}}}{[[0,\, i]]}\binom{n_{\mathrm{t}} - 1}{j}\binom{[[i - 1,\, 0]] + j}{k}\right. \\ &\times \frac{e^{[[1,i]](\delta-1)n_{\mathrm{t}}/(\lambda\delta\mathrm{snr}_{\mathrm{e}})}}{\pi(n_t - 1)!}\left(1 + \frac{1 - \delta}{\lambda\delta}\frac{1 - \lambda}{n_{\mathrm{t}} - 1}\right)^{(1-n_{\mathrm{t}})[[1,i]]+1}\frac{a_{\lambda}^{j-1}}{[[i - 1,\, 0]]!}\frac{(n_{\mathrm{t}}/(\lambda\delta\mathrm{snr}_{\mathrm{e}}))^{[[i,1]]+j-2}}{(1 - \delta)^{k+[[1-i,0]]-j}} \\ &\left.\times \int_0^{\Theta}\chi_{\theta i}^{n_{\mathrm{t}}+k-1}\mathcal{I}_{(n_{\mathrm{t}}-1)[[1,i]]-1}^{n_{\mathrm{t}}+k-1}\left(\frac{\xi_{\lambda}}{\chi_{\theta i}},\, \frac{\chi_{\theta i}}{1 - \delta + \lambda\delta(n_{\mathrm{t}} - 1)/(1 - \lambda)},\, \frac{\chi_{\theta i}}{1 - \delta + \lambda\delta(n_{\mathrm{t}} - 1)/(1 - \lambda)}\right)\mathrm{d}\theta\right\} \end{aligned} \tag{21}$$

doi: 10.1049/iet-com.2013.0564

where the symbol $\doteq$ denotes asymptotically exponential equality

$$f(\lambda) \doteq g(\lambda) \Leftrightarrow \lim_{\lambda\to\infty} \frac{\log f(\lambda)}{\log \lambda} = \lim_{\lambda\to\infty} \frac{\log g(\lambda)}{\log \lambda} \tag{27}$$

Using (25), (26), and the fact that $\mathbb{P}\{\hat{s}_I \neq s_I\} \doteq \mathrm{snr}_r^{-n_t}$, we obtain $d_s = n_t - [[n_e, 1]]$ for $0 < \lambda < 1$. For $\lambda = 1$, we can obtain $d_s = 0$ after some manipulations. □

Remark 4: By employing artificial noise, we can maintain the secrecy diversity of order $n_t - n_e$ for colluding eavesdroppers, which is also the maximum achievable diversity with full CSI [23]. For non-colluding eavesdroppers, the artificial-noise beamforming attains the secrecy diversity of order $n_t - 1$ regardless of the number of single-antenna eavesdroppers. In contrast, the high-SNR slope of δ-secrecy SEP vanishes with no artificial noise ($\lambda = 1$), reflecting the fact that reliable and confidential communication cannot be guaranteed for the legitimate link in this case. Theorem 2 further unveils that an 'eavesdropper selection' (i.e. the strongest non-colluding attack) exhibits different behaviour to the heaves dropper combining (i.e. the colluding attack) in terms of the secrecy diversity, in contrast to the same diversity behaviour of 'antenna selection' and 'antenna combining'.

4 Power allocation strategies

In this section, we attempt to find the optimal power allocation figure λ to minimise the δ-secrecy SEP. As in [18], we first find the power allocation solutions for weak (low SNR) and strong (high SNR) eavesdroppers, and then leverage these solutions to develop a switched power allocation strategy for general eavesdropping attacks.

4.1 Weak eavesdroppers ($\mathrm{snr}_e \ll 1$)

Theorem 3: The optimal value of $\lambda \in [0, 1]$ that minimises the δ-secrecy SEP for weak (low snr_e) eavesdroppers in the low-snr_r regime is equal to $\lambda = 1$.

Proof: As $\mathrm{snr}_r \to 0$ with $\delta > 1$, the δ-secrecy SEP is dominated by P_1 in (20). Since (28) we first see that the probability of the event 's_I transmitted' is independent of λ in the low-snr_e regime. Next, it is obvious that the joint outage probability (for $\delta > 1$)

$$\begin{aligned}\mathbb{P}\{\mathcal{O}, s_I \text{ transmitted}\} &= \mathbb{P}\left\{\frac{\mathrm{snr}_r}{n_t} \| \boldsymbol{h}_r \|^2 < \frac{\delta - 1}{\lambda} + \delta \frac{\mathrm{snr}_e}{n_t} \| \boldsymbol{g}_I \|^2, \right. \\ &\qquad \left. \| \boldsymbol{h}_r \|^2 \geq n_e \frac{\mathrm{snr}_e}{\mathrm{snr}_r} + o(\mathrm{snr}_e)\right\}\end{aligned} \tag{29}$$

is minimised at $\lambda = 1$. Therefore P_1 is minimised at $\lambda = 1$ and the optimal solution for λ that minimises the δ-secrecy SEP is equal to $\lambda = 1$ when $\delta > 1$. For $\delta = 1$, it is clear from (20), (28) and (29) that P_1 is independent of λ at low snr_e. Since the event $\{\mathcal{O}^c, s_I \text{ transmitted}\}$ is again free of λ for $\delta = 1$, P_2 in (21) and hence, the δ-secrecy SEP is minimised at $\lambda = 1$ by allocating the maximum power to the information signal. □

Remark 5: For weak eavesdroppers, the transmitter should use all the power for information-bearing signal transmission since the thermal noise is enough to disturb the signal reception at the eavesdroppers.

4.2 Strong eavesdropper ($\mathrm{snr}_e \gg 1$)

Lemma 1: For given $\boldsymbol{h}_r$ and $\delta > 1$, let

$$\psi^\star(\boldsymbol{h}_r) = \operatorname*{argmin}_{0\leq\lambda\leq 1} \mathbb{P}\{\mathcal{O}|\boldsymbol{h}_r\} \tag{30}$$

Then, we have

$$\psi^\star(\boldsymbol{h}_r) = \min\left\{1, \sqrt{\frac{(\delta-1)n_t}{\mathrm{snr}_r}} \frac{1}{\| \boldsymbol{h}_r \|}\right\} \tag{31}$$

at high snr_r as $\mathrm{snr}_e \to \infty$.

$$\begin{aligned}\mathbb{P}\{\mathcal{O}\} &\doteq F_{\Gamma_r}(\delta - 1) + \sum_{i=1}^{n_e} \sum_{j=0}^{[[n_e-i,0]]} \sum_{k=0}^{n_t-1} \mathrm{snr}_r^{-n_t-[[i-1,0]]} \int_0^\infty \frac{v^{[[i-1,0]]+j+k}}{\left(1 + (1-\lambda)/(n_t-1)(v/\lambda)\right)^{(n_t-1)[[1,i]]}} e^{-\left(\delta/\mathrm{snr}_r + [[1,i]]/\mathrm{snr}_e\right)(n_t/\lambda)v} \, \mathrm{d}v \\ &\doteq \sum_{k=n_t}^{\infty} \frac{(\delta-1)^k}{k!\mathrm{snr}_r^k} e^{-(\delta-1)/(\mathrm{snr}_r)} + \sum_{i=1}^{n_e} \sum_{j=0}^{[[n_e-i,0]]} \sum_{k=0}^{n_t-1} \mathrm{snr}_r^{-n_t+j+k+1} \underbrace{\int_0^\infty \left(v^{[[i-1,0]]+j+k}\right)/\left(1 + \mathrm{snr}_r v\right)^{(n_t-1)[[1,i]]} e^{-v} \, \mathrm{d}v}_{\doteq \mathrm{snr}_r^{-\min\{(n_t-1)[[1,i]],[[i,1]]+j+k\}}} \\ &\doteq \begin{cases} \mathrm{snr}_r^{-n_t} + \mathrm{snr}_r^{-n_t+[[n_e,1]]}, & \text{if } \delta > 1 \\ \mathrm{snr}_r^{-n_t+[[n_e,1]]}, & \text{if } \delta = 1 \end{cases} \\ &\doteq \mathrm{snr}_r^{-n_t+[[n_e,1]]}\end{aligned} \tag{26}$$

$$\begin{aligned}\mathbb{P}\{s_I \text{ transmitted}\} &= \mathbb{P}\left\{\lambda \frac{\mathrm{snr}_r}{n_t} \| \boldsymbol{h}_r \|^2 \geq \exp\left[\mathbb{E}_{\boldsymbol{g}_I}\left\{\ln\left(1 + \lambda \frac{\mathrm{snr}_e}{n_t} \| \boldsymbol{g}_I \|^2 + o(\mathrm{snr}_e)\right)\right\} - 1\right]\right\} \\ &= \mathbb{P}\left\{\| \boldsymbol{h}_r \|^2 \geq n_e \frac{\mathrm{snr}_e}{\mathrm{snr}_r} + o(\mathrm{snr}_e)\right\}\end{aligned} \tag{28}$$

Proof: Letting

$$Z \triangleq \left[\left[\boldsymbol{g}_{\mathrm{I}}^{\dagger}(\boldsymbol{G}_{\mathrm{A}}\boldsymbol{G}_{\mathrm{A}}^{\dagger})^{-1}\boldsymbol{g}_{\mathrm{I}},\ \max_{k}\frac{|g_{\mathrm{I}k}|^2}{\|\boldsymbol{g}_{\mathrm{A}k}\|^2}\right]\right]$$

as $\mathrm{snr}_{\mathrm{e}} \to \infty$ at high $\mathrm{snr}_{\mathrm{r}}$, we have

$$\mathbb{P}\{\mathcal{O}|\boldsymbol{h}_{\mathrm{r}}\} = \mathbb{P}\left\{Z > \frac{\|\boldsymbol{h}_{\mathrm{r}}\|^2\,\mathrm{snr}_{\mathrm{r}}}{(n_{\mathrm{t}}-1)n_{\mathrm{t}}\delta}(1-\lambda) + \frac{\delta-1}{(n_{\mathrm{t}}-1)\delta}\left(1-\frac{1}{\lambda}\right)\right\} \tag{32}$$

from which we complete the proof. □

Theorem 4: Let $\lambda^{\star}$ be the optimal value of $\lambda \in [0, 1]$ that minimises the δ-secrecy SEP for strong (high $\mathrm{snr}_{\mathrm{e}}$) eavesdroppers in the high-$\mathrm{snr}_{\mathrm{r}}$ regime. Then, the first-order optimal $\lambda^{\star}$ is unique and is the solution of

(i) Colluding eavesdroppers ($n_{\mathrm{e}} > 1$):

$$g_1(\lambda) \triangleq (\delta-1)\frac{1-\lambda}{\lambda^2} + \frac{n_{\mathrm{t}}!\Omega\left[(n_{\mathrm{t}}-1)\delta\right]^{n_{\mathrm{e}}-n_{\mathrm{t}}}}{n_{\mathrm{e}}(n_{\mathrm{e}}-2)!\binom{n_{\mathrm{t}}-1}{n_{\mathrm{e}}}\left(\mathrm{snr}_{\mathrm{r}}/n_{\mathrm{t}}\right)^{n_{\mathrm{e}}-1}}$$

$$\frac{(1-\lambda)^{n_{\mathrm{t}}-n_{\mathrm{e}}+1}}{\lambda^{n_{\mathrm{t}}+1}} - (n_{\mathrm{e}}-1)\frac{\mathrm{snr}_{\mathrm{r}}}{n_{\mathrm{t}}} = 0 \tag{33}$$

(ii) Non-colluding eavesdroppers:

$$g_2(\lambda) \triangleq \frac{n_{\mathrm{t}}!\Omega\left[(n_{\mathrm{t}}-1)\delta\right]^{1-n_{\mathrm{t}}}}{n_{\mathrm{t}}-1}\frac{(1-\lambda)^{n_{\mathrm{t}}}}{\lambda^{n_{\mathrm{t}}+1}} - \frac{\mathrm{snr}_{\mathrm{r}}}{n_{\mathrm{t}}} = 0 \tag{34}$$

where

$$\Omega \triangleq \frac{1}{\pi}\sum_{k=0}^{n_{\mathrm{t}}-1}\int_0^{\Theta}\frac{(\delta-1)^k}{k!}\left(\frac{\sin^2\theta}{c_{\mathrm{PSK}}}\right)^{n_{\mathrm{t}}-k}\mathrm{e}^{-(\delta-1)(c_{\mathrm{PSK}}/\sin^2\theta)}\,\mathrm{d}\theta \tag{35}$$

Proof: Since s_{I} is transmitted with probability one at high SNR, we have

$$\lambda^{\star} = \arg\min_{0\le\lambda\le1}(\mathbb{P}\{\mathcal{O}\} + \mathbb{P}\{\mathcal{E}\}) \tag{36}$$

Using Lemma 1, we infer that $\lambda^{\star} \to 0$ for $\delta > 1$, as $\mathrm{snr}_{\mathrm{r}}$ and $\mathrm{snr}_{\mathrm{e}}$ tend to infinity. Indeed, assuming that $\lambda^{\star} > 0$ as $\mathrm{snr}_{\mathrm{r}}$, $\mathrm{snr}_{\mathrm{e}} \to \infty$, we have $\mathbb{P}\{\mathcal{E}\} \doteq \mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}$. Hence, $\lambda^{\star} \doteq \mathbb{P}\{\mathcal{O}\}$. However, it follows from Lemma 1 that $\arg\min_{0\le\lambda\le1}\mathbb{P}\{\Delta_{\mathrm{s}} < \delta\} \to 0$ as $\mathrm{snr}_{\mathrm{r}}$, $\mathrm{snr}_{\mathrm{e}} \to \infty$. This is contradictory to the assumption. Therefore, we arrive at the fact that $\lambda^{\star} > 0$ for $\delta \ge 1$ as $\mathrm{snr}_{\mathrm{r}}$, $\mathrm{snr}_{\mathrm{e}} \to \infty$, by the continuity of $P_{\mathrm{e}}^{(\mathrm{s})}(\delta)$ at $\delta = 1$.

Since

$$\mathbb{P}\{\mathcal{E}\} = \Omega\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}} + o\left(\mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}\right) \tag{37}$$

we can rewrite (36) as

$$\lambda^{\star} = \arg\min_{0\le\lambda\le1} h(\lambda) \tag{38}$$

where

$$\begin{aligned} h(\lambda) &\triangleq \int_0^{\infty}\int_0^{(n_{\mathrm{t}}/\mathrm{snr}_{\mathrm{r}})\left((\delta-1/\lambda)+(n_{\mathrm{t}}-1)\delta/(1-\lambda)z\right)} f_Z(z)f_{\|\boldsymbol{h}_{\mathrm{r}}\|^2}(u)\mathrm{d}u\mathrm{d}z \\ &\quad + \Omega\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}} + o\left(\mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}\right) \\ &= \int_0^{\infty} F_{\|\boldsymbol{h}_{\mathrm{r}}\|^2}\left(\frac{n_{\mathrm{t}}}{\mathrm{snr}_{\mathrm{r}}}\left(\frac{\delta-1}{\lambda} + \frac{(n_{\mathrm{t}}-1)\delta}{1-\lambda}z\right)\right)f_Z(z)\mathrm{d}z \\ &\quad + \Omega\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}} + o\left(\mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}\right) \end{aligned} \tag{39}$$

By differentiating $h(\lambda)$ with respect to λ, we have (40)

where the PDF of Z can be obtained from (11) and (15). Using Taylor expansion and the fact that $\lambda^{\star} \to 0$ as $\mathrm{snr}_{\mathrm{r}}$, $\mathrm{snr}_{\mathrm{e}} \to \infty$, after some algebra, we can simplify $\mathrm{d}h(\lambda)/\mathrm{d}\lambda = 0$ as follows

$$\frac{\mathrm{d}h(\lambda)}{\mathrm{d}\lambda} = 0 \Leftrightarrow \begin{cases} g_1(\lambda) = 0, & \text{if colluding}(n_{\mathrm{e}} > 1) \\ g_2(\lambda) = 0, & \text{if non-colluding} \end{cases} \tag{41}$$

Since $g_1(\lambda)$ and $g_2(\lambda)$ are decreasing functions in λ with $g_1(0)$

$$\begin{aligned} \frac{\mathrm{d}h(\lambda)}{\mathrm{d}\lambda} &= -\Omega\mathrm{snr}_{\mathrm{r}}\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}+1} + o\left(\mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}\right) \\ &\quad + \frac{n_{\mathrm{t}}}{\mathrm{snr}_{\mathrm{r}}}\int_0^{\infty}\left[\frac{(n_{\mathrm{t}}-1)\delta}{(1-\lambda)^2}z - \frac{\delta-1}{\lambda^2}\right]f_{\|\boldsymbol{h}_{\mathrm{r}}\|^2}\left(\frac{n_{\mathrm{t}}}{\mathrm{snr}_{\mathrm{r}}}\left(\frac{\delta-1}{\lambda} + \frac{(n_{\mathrm{t}}-1)\delta}{1-\lambda}z\right)\right)f_Z(z)\,\mathrm{d}z \\ &= -\Omega\mathrm{snr}_{\mathrm{r}}\left(\frac{n_{\mathrm{t}}}{\lambda\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}+1} + \left[\left[n_{\mathrm{e}}, 1\right]\right]\left(n_{\mathrm{t}} - 1\left[\left[n_{\mathrm{e}}, 1\right]\right]\right)\frac{e^{-(n_{\mathrm{t}}/\mathrm{snr}_{\mathrm{r}})(\delta-1)/\lambda}}{(n_{\mathrm{t}}-1)!}\left(\frac{n_{\mathrm{t}}}{\mathrm{snr}_{\mathrm{r}}}\right)^{n_{\mathrm{t}}} \\ &\quad \times \int_0^{\infty}\left\{\left[\frac{\delta-1}{\lambda} + \frac{(n_{\mathrm{t}}-1)\delta}{1-\lambda}z\right]^{n_{\mathrm{t}}-1}\left[\frac{(n_{\mathrm{t}}-1)\delta}{(1-\lambda)^2}z - \frac{\delta-1}{\lambda^2}\right]\right. \\ &\quad \left.\times\frac{z^{\left[\left[n_{\mathrm{e}}-1,0\right]\right]}}{(1+z)^{n_{\mathrm{t}}}}\left[1-(1+z)^{1-n_{\mathrm{t}}}\right]^{\left[\left[0,n_{\mathrm{e}}-1\right]\right]}e^{-(n_{\mathrm{t}}/\mathrm{snr}_{\mathrm{r}})((n_{\mathrm{t}}-1)\delta/(1-\lambda))}\,\mathrm{d}z\right\} + o\left(\mathrm{snr}_{\mathrm{r}}^{-n_{\mathrm{t}}}\right) \end{aligned} \tag{40}$$

doi: 10.1049/iet-com.2013.0564

> 0, $g_1(1) < 0$, $g_2(0) > 0$ and $g_2(1) < 0$, we complete the proof. □

Remark 6: If the eavesdroppers do not collude, the first-order optimal $\lambda^\star$ is independent of the number of eavesdroppers whereas $\lambda^\star$ is a function of both n_t and n_e if the eavesdroppers collude. The first-order optimal $\lambda^\star$ behaves as follows

(i) Colluding eavesdroppers ($n_e > 1$):

See (42), where κ is the unique solution of

$$\frac{n_t!\Omega\big((n_t-1)\delta\big)^{n_e-n_t}}{n_e(n_e-2)!\binom{n_t-1}{n_e}}\kappa^{n_e}+(\delta-1)\kappa+1-n_e=0 \quad (43)$$

(ii) Non-colluding eavesdroppers:

$$\lambda^\star=\left[\frac{n_t!\Omega\big((n_t-1)\delta\big)^{1-n_t}}{n_t-1}\right]^{(1/n_t+1)}\left(\frac{\mathrm{snr}_r}{n_t}\right)^{-(1/n_t+1)}+o\big(\mathrm{snr}_r^{-(1/n_t+1)}\big) \quad (44)$$

Note that $\lambda^\star$ has the form of $\lambda^\star \doteq \mathrm{snr}_r^{-\alpha}$ with $0 < \alpha < 1$. This again confirms that $\lambda^\star \to 0$ in the high-SNR regime. Furthermore, $\lambda^\star$ decreases with n_e (for colluding attacks) and snr_r, while growing with n_t.

4.3 Switched strategy

In general, it is infeasible to optimise λ because of the non-tractable form of δ-secrecy SEP in (19). Instead, we

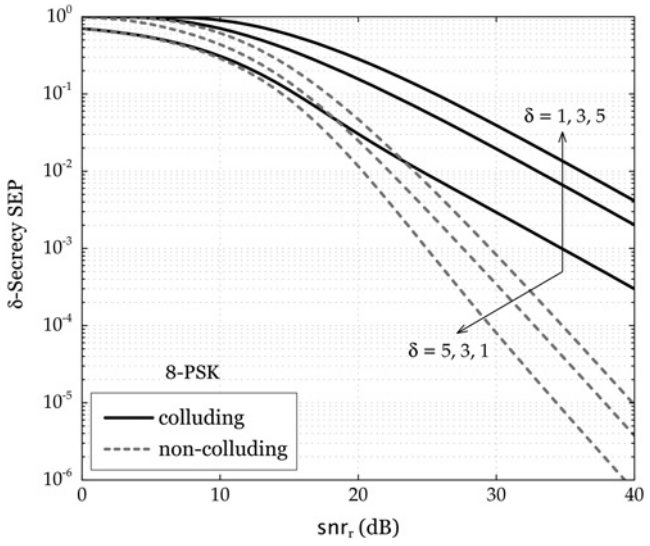

Fig. 2 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for colluding (solid line) and non-colluding (dashed line) eavesdroppers at $\delta = 1$, 3 and 5 when $n_t = 3$, $n_e = 2$, $\lambda = 0.5$ and $snr_e = snr_r$*

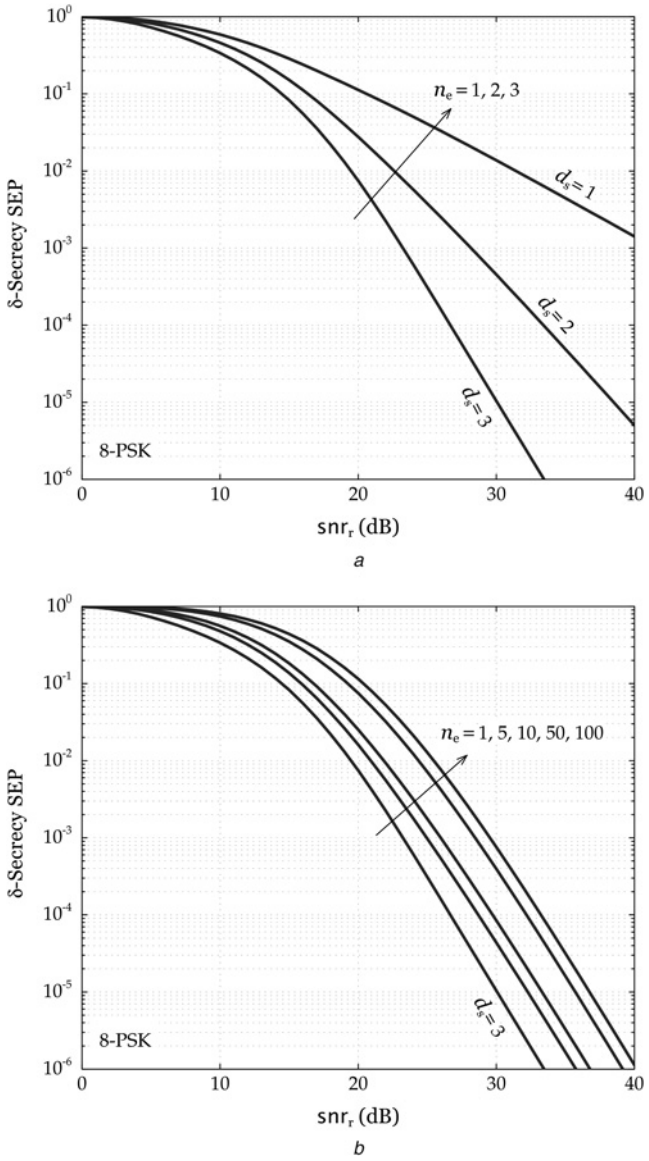

Fig. 3 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for*
a Colluding eavesdroppers with $n_e = 1$, 2 and 3
b Non-colluding eavesdroppers with $n_e = 1$, 5, 10, 50 and 100 when $n_t = 4$, $\lambda = 0.5$, $\delta = 2$ and $\mathrm{snr}_e = \mathrm{snr}_r$

$$\lambda^\star=\begin{cases}\left(\dfrac{n_e-1}{\delta-1}\dfrac{\mathrm{snr}_r}{n_t}\right)^{-1/2}+o\big(\mathrm{snr}_r^{-1/2}\big), & \text{if } n_t<2n_e-1,\quad \delta>1\\ \left(\kappa\dfrac{\mathrm{snr}_r}{n_t}\right)^{-1/2}+o\big(\mathrm{snr}_r^{-1/2}\big), & \text{if } n_t=2n_e-1)\\ \left[\dfrac{n_t!\Omega\big((n_t-1)\delta\big)^{n_e-n_t}}{n_e!\binom{n_t-1}{n_e}}\right]^{1/(n_t+1)}\left(\dfrac{\mathrm{snr}_r}{n_t}\right)^{-n_e/(n_t+1)}+o\big(\mathrm{snr}_r^{-n_e/(n_t+1)}\big), & \text{otherwise}\end{cases} \quad (42)$$

design a simple switched strategy such that the δ-secrecy SEP is still near-optimal with low-computational complexity. Specifically, we put forward a switched power allocation as follows

$$\lambda_s = \arg\min_{\lambda \in \{1, \lambda^\star\}} P_e^{(s)}(\delta) \tag{45}$$

Remark 7: The term 'switched' reflects a change in λ depending on snr_r and snr_e. It is obvious that the switched allocation λ_s goes back to the optimal value of λ in the low- and high-SNR regimes.

5 Numerical results

In this section, we provide some numerical results to demonstrate: (i) the effect of artificial noise on the δ-secrecy SEP and secrecy diversity; and (ii) the effectiveness of the switched power allocation for secure beamforming with artificial noise to minimise the δ-secrecy SEP.

5.1 δ-secrecy SEP and secrecy diversity

Fig. 2 shows the δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for colluding and non-colluding eavesdroppers at $\delta =$ 1, 3 and 5 when $n_t = 3$, $n_e = 2$, $\lambda = 0.5$ and $\text{snr}_e = \text{snr}_r$. We see that there is a tradeoff between the confidentiality level δ and the communication reliability. A large value of δ (strong confidentiality) produces a parallel shift of the δ-secrecy SEP curve in the high-SNR regime. It can be further seen that colluding eavesdropping attacks significantly degrade the δ-secrecy SEP. To ascertain the effect of artificial noise on the secrecy diversity, the δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK is depicted in Fig. 3 for (*a*) $n_e = 1$, 2 and 3 (colluding eavesdroppers) and (*b*) $n_e = 1$, 5, 10, 50 and 100 (non-colluding eavesdroppers) when $\delta = 2$, $n_t = 4$, $\lambda = 0.5$ and $\text{snr}_e = \text{snr}_r$. This example confirms Theorem 1: the

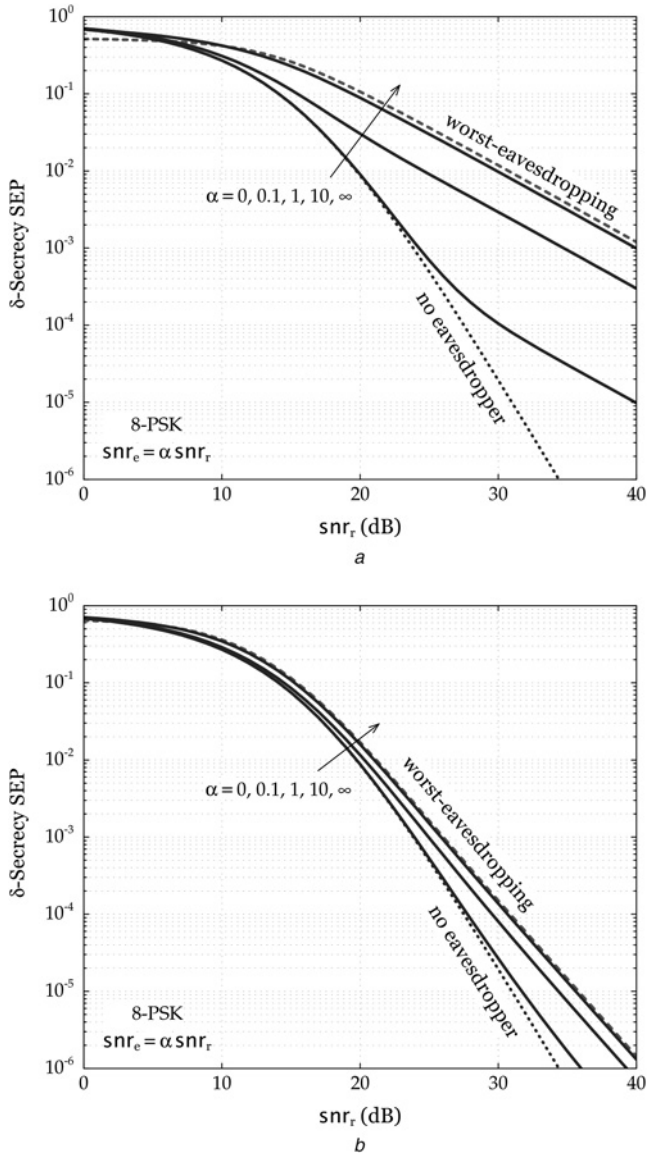

Fig. 4 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for*

a Colluding eavesdroppers

b Non-colluding eavesdroppers when $n_t = 3$, $n_e = 2$, $\lambda = 0.5$, $\delta = 2$ and $\text{snr}_e = \alpha\text{snr}_r$ for $\alpha = 0$ (no eavesdropper), 0.1, 1, 10 and ∞ (worst eavesdropping)

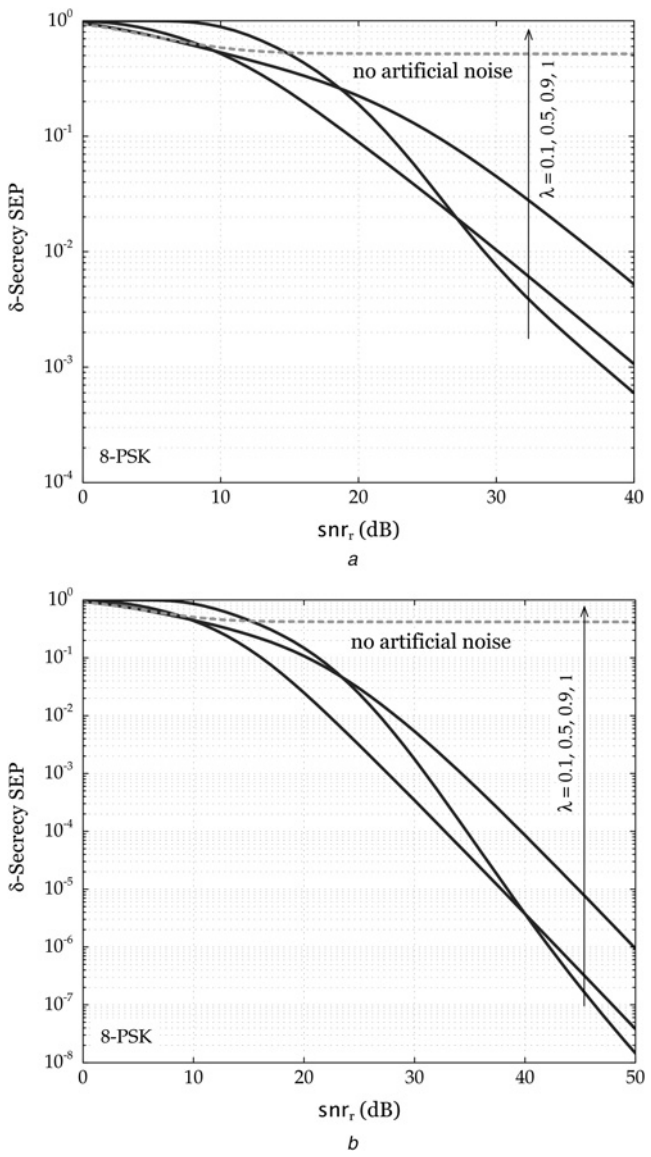

Fig. 5 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for*

a Colluding eavesdroppers

b Non-colluding eavesdroppers when $n_t = 3$, $n_e = 2$, $\delta = 2$ and $\text{snr}_e = \text{snr}_r$ for $\lambda = 0.1$, 0.5, 0.9 and 1 (no artificial noise)

doi: 10.1049/iet-com.2013.0564

secrecy diversity orders are equal to $d_s = n_t - n_e = 3, 2$ and 1 for $n_e = 1, 2$ and 3, respectively (colluding cases) and $d_s = n_t - 1 = 3$ (non-colluding cases). This implies that the transmitter sacrifices large degrees of freedom to protect the confidential information from the colluding eavesdropping attacks. The colluding eavesdropping reduces the slope (diversity order) of $P_e^{(s)}(\delta)$ with the number of eavesdroppers, whereas the non-colluding only reduces one degree of the slope and produces a parallel shift of $P_e^{(s)}(\delta)$. Fig. 4 shows the δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for both colluding and non-colluding cases when $n_t = 3$, $n_e = 2$, $\lambda = 0.5$, $\delta = 2$ and $\text{snr}_e = \alpha \text{snr}_r$ for $\alpha = 0$ (no eavesdropper), 0.1, 1, 10 and ∞ (worst-eavesdropping). In the absence of eavesdropping ($\alpha = 0$), the δ-secrecy SEP boils down to the ordinary SEP without accounting for physical-layer security. This figure also demonstrates that the artificial noise guarantees to attain the reliability of confidential transmission even against very strong eavesdropping attacks.

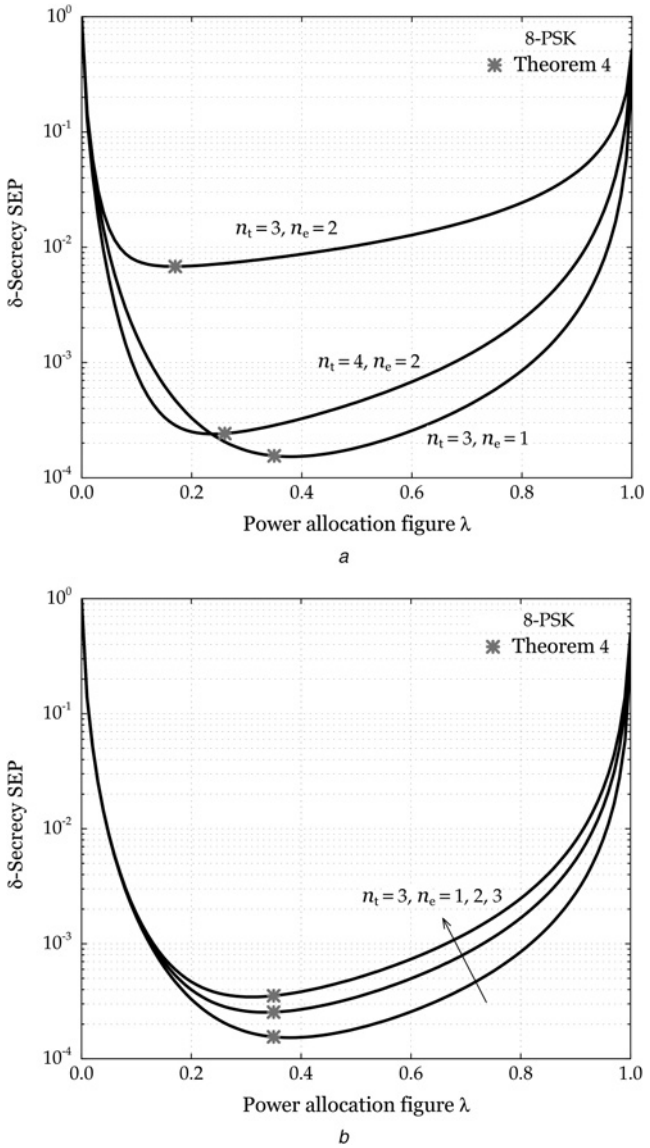

Fig. 6 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of the power allocation figure λ at $\delta = 2$ and $snr_r = snr_e = 30$ dB for*

a Colluding eavesdroppers (when $n_t = 3, n_e = 1$; $n_t = 3, n_e = 2$; and $n_t = 4, n_e = 2$)
b Non-colluding eavesdroppers (when $n_t = 3$ and $n_e = 1, 2, 3$)

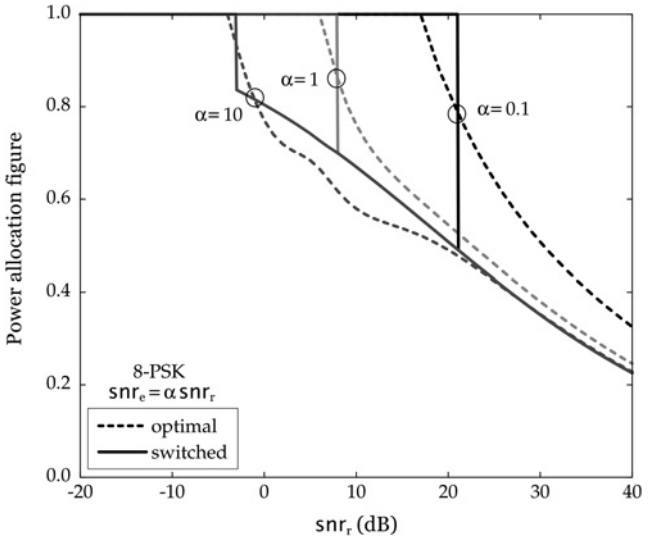

Fig. 7 *Power allocation figures λ as a function of snr_r for 8-PSK with the switched (solid line) and optimal (dashed line) strategies when $n_t = 3$, $n_e = 1$ and $snr_e = \alpha snr_r$ for $\alpha = 0.1$, 1 and 10*

The effect of the power allocation figure λ on the δ-secrecy SEP can be ascertained by referring to Figs. 5 and 6. Fig. 5 shows the δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r for both colluding and non-colluding cases when $n_t = 3$, $n_e = 2$, $\delta = 2$ and $\text{snr}_e = \text{snr}_r$ for $\lambda = 0.1$, 0.5, 0.9 and 1 (no artificial noise). The δ-secrecy SEP of 8-PSK is further depicted in Fig. 5 as a function of λ at $\delta = 2$ and $\text{snr}_r = \text{snr}_e = 30$ dB for (*a*) colluding eavesdroppers (when $n_t = 3$, $n_e = 1$; $n_t = 3$, $n_e = 2$; and $n_t = 4$, $n_e = 2$) and (*b*) non-colluding eavesdroppers (when $n_t = 3$ and $n_e = 1$, 2, 3). In these figures, we can see that there exists a saddle point in λ that minimises the δ-secrecy SEP for a pair of operating snr_r and snr_e, whereas the high-SNR slope of $P_e^{(s)}(\delta)$ – the secrecy diversity – vanishes with no artificial noise ($\lambda = 1$). It can be also observed that the first-order optimal $\lambda^\star$ in Theorem 4 is highly effective and near-optimal in the high-SNR regime.

5.2 Switched power allocation

Fig. 7 shows the power allocation figures λ as a function of snr_r for 8-PSK with the switched and optimal allocations when $n_t = 3$, $n_e = 1$ and $\text{snr}_e = \alpha \text{snr}_r$ for $\alpha = 0.1$, 1 and 10. The switched power allocation λ_s is determined by (45), whereas the optimal power allocation is found directly from (19) by using numerical methods. We can see that the switched allocation λ_s tracks the optimal solution well and converges even to the optimal value in low- and high-SNR regimes as stated in Theorems 3 and 4. Hence, we can use effectively the switched power allocation in practical design. The behaviour of the power allocation figures can be further observed in Fig. 8 as a function of snr_r for 8-PSK with the switched (solid line) and optimal (dashed line) allocations for both colluding and non-colluding eavesdroppers at $\delta = 2$ and $\text{snr}_e = \text{snr}_r$ when $n_e = 2$, $n_t = 3$, 4 and 5. In the high-SNR regime, we observe that the power allocation figures increase with n_t while decreasing with snr_r (see Remark 6). The transmitter should dedicate more power for transmission of the information-bearing signal to reduce the δ-secrecy SEP as n_t increases, whereas more power should be allocated to the artificial noise for interference with the eavesdroppers as n_e increases.

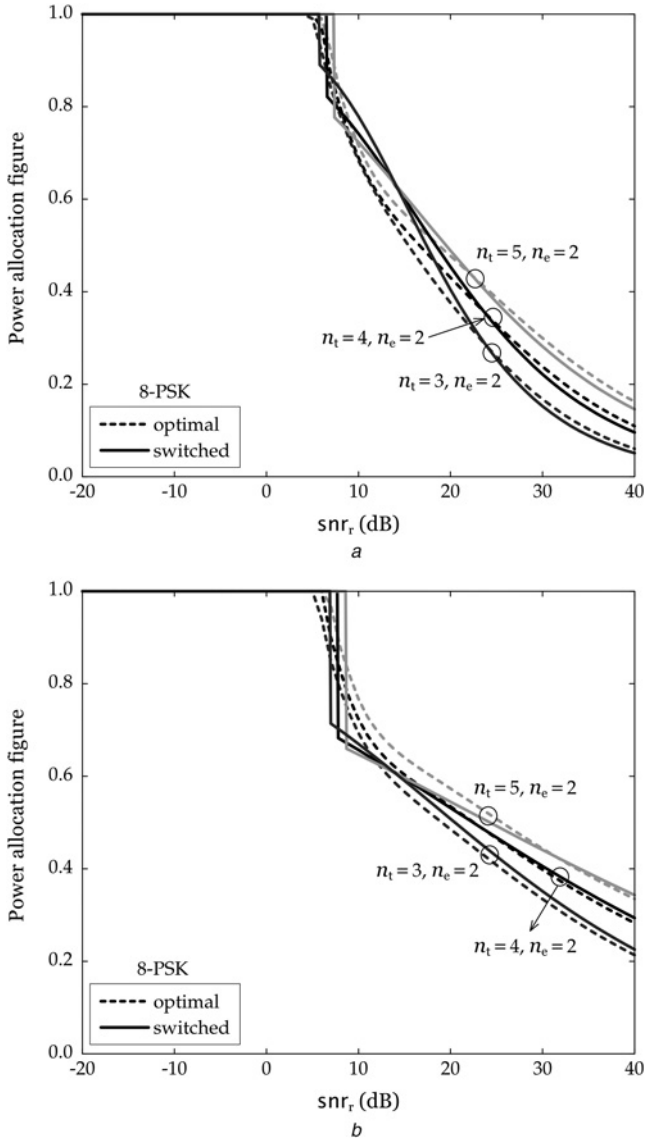

Fig. 8 *Power allocation figures λ as a function of snr$_r$ for 8-PSK with the switched (solid line) and optimal (dashed line) allocations for*

a Colluding eavesdroppers
b Non-colluding eavesdroppers at $\delta = 2$ and $\text{snr}_e = \text{snr}_r$ when $n_e = 2$, $n_t = 3$, 4 and 5

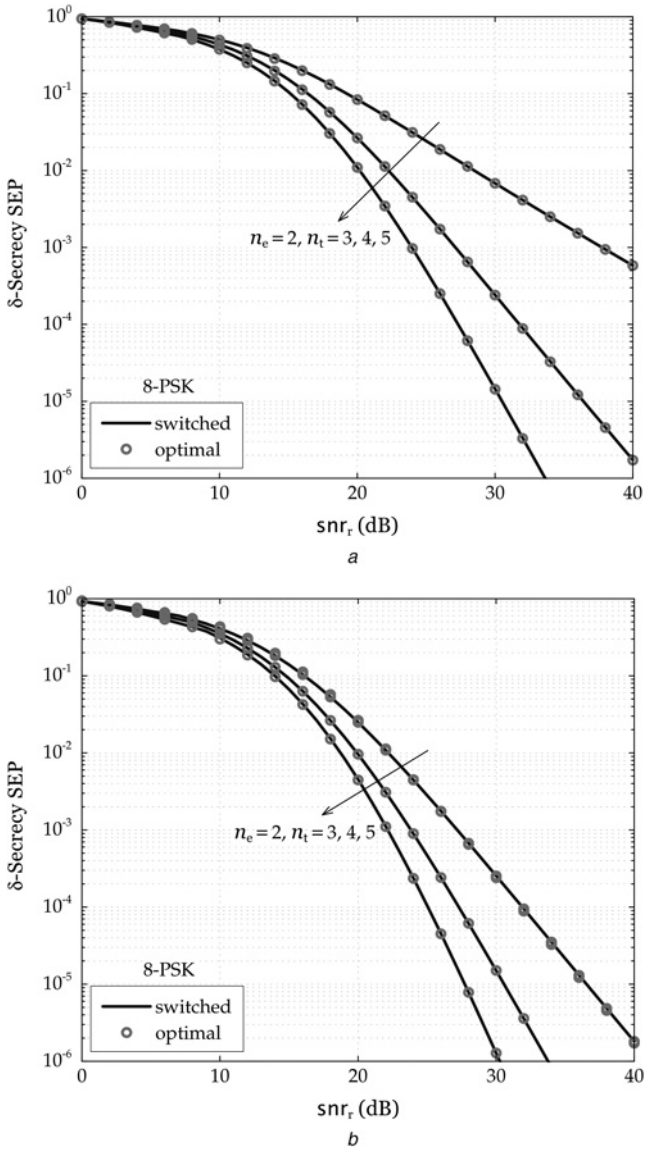

Fig. 9 *δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr$_r$ with the switched and optimal allocations for*

a Colluding eavesdroppers
b Non-colluding eavesdroppers at $\delta = 2$ and $\text{snr}_r = \text{snr}_e$ when $n_e = 2$, $n_t = 3$, 4 and 5

Finally, Fig. 9 shows the δ-secrecy SEP $P_e^{(s)}(\delta)$ of 8-PSK as a function of snr_r with the switched and optimal allocations for both the colluding and non-colluding cases at $\delta = 2$ and $\text{snr}_e = \text{snr}_r$ when $n_e = 2$, $n_t = 3$, 4 and 5. We can see that the δ-secrecy SEP for the switched power allocation agrees almost exactly with the optimal $P_e^{(s)}(\delta)$ over the whole SNR regime, revealing the effectiveness of the switched power allocation.

6 Conclusions

In this second part of the paper, we investigated secure beamforming with artificial noise in MISOME wiretap channels for both colluding and non-colluding eavesdroppers. We introduced the δ-secrecy SEP to measure the reliability of legitimate communication with accounting for physical-layer confidentiality. Using the notion of δ-secrecy SEP, we also assessed the effect of secure beamforming with artificial noise on the secrecy diversity (i.e. the high-SNR slope of the δ-secrecy SEP), which is analogy to the diversity order without accounting for the communication confidentiality. It has turned out that the artificial-noise strategy n_t transmit antennas sustains the secrecy diversity of order $n_t - n_e$ and $n_t - 1$ for n_e single-antenna colluding and non-colluding eavesdroppers, respectively. We further determined the optimal power allocations between the information-bearing signal and artificial noise to minimise the δ-secrecy SEP for weak (low SNR) or strong (high SNR) eavesdroppers. Using these first-order optimal solutions, we developed a simple near-optimal power allocation policy for general eavesdropping attacks. It would be of interest to extend this work in the direction of (i) exploiting the MIMO potentials whereby we can utilise the well-equipped ability of multiple antennas at the legitimate receiver to enhance the secrecy rate and reduce the δ-secrecy SEP; and (ii) accounting for the effect of network interference on both the legitimate and eavesdropper links for secure communication.

doi: 10.1049/iet-com.2013.0564

7 Acknowledgments

This work was supported, in part, by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2009-0083495) and NRF-2011-220-D00076 by the Ministry of Education.

8 References

1 Goldsmith, A., Jafar, S.A., Jindal, N., Vishwanath, S.: 'Capacity limits of MIMO channels', *IEEE J. Sel. Areas Commun.*, 2003, **21**, (5), pp. 684–702
2 Shin, H., Lee, J.H.: 'Capacity of multiple-antenna fading channels: spatial fading correlation, double scattering, and keyhole', *IEEE Trans. Inf. Theory*, 2003, **49**, (10), pp. 2636–2647
3 Zheng, L., Tse, D.N.C.: 'Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels', *IEEE Trans. Inf. Theory*, 2003, **49**, (5), pp. 1073–1096
4 Shin, H., Win, M.Z., Lee, J.H., Chiani, M.: 'On the capacity of doubly correlated MIMO channels', *IEEE Trans. Wirel. Commun.*, 2006, **5**, (8), pp. 2253–2265
5 Shin, H., Win, M.Z., Chiani, M.: 'Asymptotic statistics of mutual information for doubly correlated MIMO channels', *IEEE Trans. Wirel. Commun.*, 2008, **7**, (2), pp. 562–573
6 Shin, H., Win, M.Z.: 'Gallager's exponent for MIMO channels: a reliability–rate tradeoff', *IEEE Trans. Commun.*, 2009, **57**, (4), pp. 972–985
7 Shin, H., Win, M.Z.: 'MIMO diversity in the presence of double scattering', *IEEE Trans. Inf. Theory*, 2008, **54**, (7), pp. 2976–2996
8 Shin, H., Song, J.B.: 'MRC analysis of cooperative diversity with fixed-gain relays in Nakagami-*m* fading channels', *IEEE Trans. Wirel. Commun.*, 2008, **7**, (6), pp. 2069–2074
9 Song, Y., Shin, H., Hong, E.K.: 'MIMO cooperative diversity with scalar-gain amplify-and-forward relaying', *IEEE Trans. Commun.*, 2009, **57**, (7), pp. 1932–1938
10 Jeong, Y., Shin, H.: 'Effect of joint spatial correlation on the diversity performance of space-time block codes', *IEEE Commun. Lett.*, 2009, **13**, (7), pp. 477–479
11 Chiani, M., Win, M.Z., Shin, H.: 'MIMO networks: the effects of interference', *IEEE Trans. Inf. Theory*, 2010, **56**, (1), pp. 336–349
12 Jeong, Y., Shin, H., Win, M.Z.: 'Superanalysis of optimum combining with application to femtocell networks', *IEEE J. Sel. Areas Commun.*, 2012, **30**, (3), pp. 509–524
13 Khisti, A., Wornell, G.W.: 'Secure transmission with multiple antennas I: the MISOME wiretap channel', *IEEE Trans. Inf. Theory*, 2010, **56**, (7), pp. 3088–3104
14 Khisti, A., Wornell, G.W.: 'Secure transmission with multiple antennas – Part II: the MIMOME wiretap channel', *IEEE Trans. Inf. Theory*, 2010, **56**, (11), pp. 5515–5532
15 Nguyen, T.V., Shin, H.: 'Power allocation and achievable secrecy rates in MISOME wiretap channels', *IEEE Commun. Lett.*, 2011, **15**, (11), pp. 1196–1198
16 Goel, S., Negi, R.: 'Guaranteeing secrecy using artificial noise', *IEEE Trans. Wirel. Commun.*, 2008, **7**, (6), pp. 2180–2189
17 Zhou, X., McKay, M.R.: 'Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation', *IEEE Trans. Veh. Technol.*, 2010, **59**, (8), pp. 3831–3842
18 Nguyen, T.V., Jeong, Y., Kwak, J.S., Shin, H.: 'Secure MISO communication – Part I: secrecy rates and switched power allocation', *IET Commun.*, accepted (Invited Paper)
19 Liang, Y., Poor, H.V., Shamai, S.: 'Secure communication over fading channels', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2470–2492
20 Prabhu, V.U., Rodrigues, M.R.D.: 'On wireless channels with *M*-antenna eavesdroppers characterization of the outage probability and ε-outage secrecy capacity', *IEEE Trans. Inf. Forensics Sec.*, 2011, **6**, (3), pp. 853–860
21 Zhou, X., McKay, M.R., Maham, B., Hjørungnes, A.: 'Rethinking the secrecy outage formulation: a secure transmission design perspective', *IEEE Commun. Lett.*, 2011, **15**, (3), pp. 302–304
22 Zhang, X., Zhou, X., McKay, M.R.: 'On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels', *IEEE Trans. Veh. Technol.*, 2013, **62**, (5), pp. 2170–2181
23 Yuksel, M., Erkip, E.: 'Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel', *IEEE Trans. Wirel. Commun.*, 2011, **10**, (3), pp. 762–771
24 Gowda, K.T., Quek, T.Q.S., Shin, H.: 'Secure diversity-multiplexing tradeoffs in MIMO relay channels'. Proc. IEEE Int. Symp. Information Theory, Seoul, Korea, June 2009, pp. 1433–1437
25 Ding, Z., Leung, K.K., Goeckel, D.L., Towsley, D.: 'On the application of cooperative transmission to secrecy communications', *IEEE J. Sel. Areas Commun.*, 2012, **30**, (2), pp. 359–368
26 Rezki, Z., Alouini, M.: 'Secure diversity-multiplexing tradeoff of zero-forcing transmit scheme at finite-SNR', *IEEE Trans. Commun.*, 2012, **60**, (4), pp. 1138–1147
27 Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: 'Wireless information-theoretic security', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2515–2534
28 Polyanskiy, Y., Poor, H.V., Verdú, S.: 'Channel coding rate in the finite blocklength regime', *IEEE Trans. Inf. Theory*, 2010, **56**, (5), pp. 2307–2359
29 Mukherjee, A., Swindlehurst, A.L.: 'Robust beamforming for security in MIMO wiretap channels with imperfect CSI', *IEEE Trans. Signal Process.*, 2011, **59**, (1), pp. 351–361
30 Liao, W.-C., Chang, T.-H., Ma, W.-K., Chi, C.-Y.: 'QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach', *IEEE Trans. Signal Process.*, 2011, **59**, (3), pp. 1202–1216
31 Tang, X., Liu, R., Spasojević, P., Poor, H.V.: 'On the throughput of secure hybid-ARQ protocols for Gaussian block-fading channels', *IEEE Trans. Inf. Theory*, 2009, **55**, (4), pp. 1575–1591
32 Shin, H., Lee, J.H.: 'On the error probability of binary and *M*-ary signals in Nakagami-*m* fading channels', *IEEE Trans. Commun.*, 2004, **52**, (4), pp. 536–539

9 Appendix

9.1 Appendix 1: Proof of Theorem 1

9.1.1 Derivation of P_1: By definition, we have (46)

$$
\begin{aligned}
P_1 &= \int_{\varrho_\lambda}^{\infty}\int_{\gamma_\lambda}^{\delta v+\delta-1}\frac{f_{\Gamma_r}(u)f_{\Gamma_e}(v)}{1-F_{\Gamma_r}(\gamma_\lambda)}\mathrm{d}u\mathrm{d}v = \int_{\varrho_\lambda}^{\infty}\frac{F_{\Gamma_r}(\delta v+\delta-1)-F_{\Gamma_r}(\gamma_\lambda)}{1-F_{\Gamma_r}(\gamma_\lambda)}f_{\Gamma_e}(v)\,\mathrm{d}v \\
&\overset{(a)}{=}\frac{1-F_{\Gamma_e}(\varrho_\lambda)}{1-F_{\Gamma_r}(\gamma_\lambda)}\Big[F_{\Gamma_r}(\delta\varrho_\lambda+\delta-1)-F_{\Gamma_r}(\gamma_\lambda)\Big]+\delta\int_{\varrho_\lambda}^{\infty}\frac{1-F_{\Gamma_e}(\varrho_\lambda)}{1-F_{\Gamma_r}(\gamma_\lambda)}f_{\Gamma_r}(\delta v+\delta-1)\mathrm{d}v \\
&=\frac{1-F_{\Gamma_e}(\varrho_\lambda)}{1-F_{\Gamma_r}(\gamma_\lambda)}\Big[F_{\Gamma_r}\big(\delta\varrho_\lambda+\delta-1\big)-F_{\Gamma_r}(\gamma_\lambda)\Big]+\frac{1}{1-F_{\Gamma_r}(\gamma_\lambda)}\frac{e^{(1-\delta)n_t/(\lambda\mathrm{snr}_r)}}{(n_t-1)!}\left(\frac{n_t}{\lambda\mathrm{snr}_r}\right)^{n_t}\sum_{i=1}^{n_e}\sum_{j=0}^{[[n_e-i,0]]} \\
&\quad\times\sum_{k=0}^{n_t-1}\left\{(-1)^{[[0,i-1]]}\binom{n_e}{[[0,i]]}\binom{n_t-1}{j}\binom{n_t-1}{k}\frac{a_\lambda^j}{[[i-1,0]]!}(\delta-1)^{n_t-1-k}\delta^{k+1}\left(\frac{n_t}{\lambda\mathrm{snr}_e}\right)^{[[i-1,0]]+j}\right. \\
&\quad\left.\times\int_{\varrho_\lambda}^{\infty}\frac{v^{[[i-1,0]]+j+k}}{\big(1+(1-\lambda/\lambda(n_t-1))v\big)^{(n_t-1)[[1,i]]}}e^{-\left(\delta/\mathrm{snr}_r+([[1,i]]/\mathrm{snr}_e)\right)(n_t/\lambda)v}\,\mathrm{d}v\right\}
\end{aligned}
\tag{46}
$$

where (a) is obtained by using the integral by parts. Using (46), we readily obtain the closed-form expression for P_1 as in (20).

9.1.2 Derivation of P_2: By definition and using the SEP expression for M-PSK signalling in [32], we have (see (47)) from which we can readily obtain (21). □

$$
\begin{aligned}
P_2 &= \frac{1}{\pi}\int_0^{\Theta}\int_{\xi_\lambda}^{\infty}\int_0^{(u/\delta)+(1/\delta)-1} \exp\left(-\frac{c_{\mathrm{PSK}}}{\sin^2\theta}u\right) f_{\Gamma_\mathrm{e}}(v)\frac{f_{\Gamma_\mathrm{r}}(u)}{1-F_{\Gamma_\mathrm{r}}(\gamma_\lambda)}\mathrm{d}v\mathrm{d}u\ \mathrm{d}\theta \\
&= \frac{1}{\pi}\int_0^{\Theta}\int_{\xi_\lambda}^{\infty} \exp\left(-\frac{c_{\mathrm{PSK}}}{\sin^2\theta}u\right) F_{\Gamma_\mathrm{e}}\left(\frac{u}{\delta}+\frac{1}{\delta}-1\right)\frac{f_{\Gamma_\mathrm{r}}(u)}{1-F_{\Gamma_\mathrm{r}}(\gamma_\lambda)}\mathrm{d}u\ \mathrm{d}\theta \\
&= \frac{1}{\pi}\int_0^{\Theta}\left(1+\frac{\lambda\mathrm{snr}_\mathrm{r}}{n_\mathrm{t}}\frac{c_{\mathrm{PSK}}}{\sin^2\theta}\right)^{-n_\mathrm{t}}\frac{1-F_{\Gamma_\mathrm{r}}\left(\left(1+(\lambda\mathrm{snr}_\mathrm{r}/n_\mathrm{t})(c_{\mathrm{PSK}}/\sin^2\theta)\right)\xi_\lambda\right)}{1-F_{\Gamma_\mathrm{r}}(\gamma_\lambda)}\ \mathrm{d}\theta \\
&\quad -\frac{\left(n_\mathrm{t}/(\lambda\mathrm{snr}_\mathrm{r})\right)^{n_\mathrm{t}}}{1-F_{\Gamma_\mathrm{r}}(\gamma_\lambda)}\sum_{i=1}^{n_\mathrm{e}}\sum_{j=0}^{[[n_\mathrm{e}-i,0]]}\sum_{k=0}^{[[i+j-1,0]]}\left\{(-1)^{[[0,i-1]]}\binom{n_\mathrm{e}}{[[0,\,i]]}\binom{n_\mathrm{t}-1}{j}\right. \\
&\quad \times\binom{[[i-1,\,0]]+j}{k}\frac{\left(n_\mathrm{t}/(\lambda\delta\mathrm{snr}_\mathrm{e})\right)^{[[i-1,0]]+j}}{(1-\delta)^{k+[[1-i,0]]-j}}\frac{e^{[[1,i]](\delta-1)n_\mathrm{t}/(\lambda\delta\mathrm{snr}_\mathrm{e})}}{\pi(n_\mathrm{t}-1)!}\frac{a_\lambda^j}{[[i-1,\,0]]!} \\
&\quad \left.\times\int_0^{\Theta}\int_{\xi_\lambda}^{\infty}u^{n_\mathrm{t}+k-1}\left(1+\frac{1-\lambda}{\lambda\delta(n_\mathrm{t}-1)}(u+1-\delta)\right)^{(1-n_\mathrm{t})[[1,i]]}e^{-(u/\chi_{\theta i})}\mathrm{d}u\ \mathrm{d}\theta\right\}
\end{aligned}
\tag{47}
$$

doi: 10.1049/iet-com.2013.0564