Research Article

Asymptotic Bound of Secrecy Capacity for MIMOME-Based Transceivers: A Suboptimally Tractable Solution for Imperfect CSI

Makan Zamanipour

Freelance Scholar, Tehran 1634776616, Iran

Correspondence should be addressed to Makan Zamanipour; makan.zamanipour.2015@ieee.org

Received 28 July 2017; Accepted 8 November 2017; Published 14 December 2017

Academic Editor: Dane Quinn

Copyright © 2017 Makan Zamanipour. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The paper principally proposes a suboptimally closed-form solution in terms of a general asymptotic bound of the secrecy capacity in relation to MIMOME-based transceivers. Such pivotal solution is essentially tight as well, fundamentally originating from the principle *convexity*. The resultant novelty, per se, is strictly necessary since the absolutely central criterion *imperfect knowledge* of the wiretap channel at the transmitter should also be highly regarded. Meanwhile, ellipsoidal channel uncertainty set-driven strategies are physically taken into consideration. Our proposed solution is capable of perfectly being applied for other general equilibria such as multiuser ones. In fact, this in principle addresses an entirely appropriate alternative for worst-case method-driven algorithms utilising some provable inequality-based mathematical expressions. Our framework is adequately guaranteed regarding a totally acceptable outage probability (as $1 - \text{preciseness coefficient}$). The relative value is almost 10% for the estimation error values (EEVs) ≤ 0.5 for 2×2 -based transceivers, which is noticeably reinforced at nearly 5% for EEVs ≤ 0.9 for the case 4×4 . Furthermore, our proposed scheme basically guarantees the secrecy outage probability (SOP) less than 0.05% for the case of having EEVs ≤ 0.3 , for the higher power regime.

1. Introduction

In order to highlight a significantly more favourable system performance in terms of higher security in wireless networks, a programmable beamformer is set up at the transmitter [1–4]. Such technologically advanced equipment (precoder) is undoubtedly able to manage the users' links in totally different paradigms, originated from the fact of *resource allocation*. In the context of the forenamed widely supported principle, it is also highly motivated to provide the fashions convex, without loss of optimality.

The convexity cited above has a vast range of beneficial knock-on effects such as markedly more adequate *convergence* in design problem. Thus, the enlightening concept convexity is highly emphasised in order to guarantee an absolute robustness in terms of tractability in association with the optimisation problem.

The optimisation problem (where the precoder is computed) optimally/suboptimally features a guarantee of the

quality of service (QoS) in multiuser games, for example, multi-input multioutput multiantenna eavesdropper (MIMOME-) based ones. QoS should be fairly taken into account among all *players*, since eavesdroppers (Eaves) may be licensed or unauthorised ones in the mentioned futuristic transceivers.

The suboptimality expressed above advances a trade-off between two criteria such as convexity which suffers from, for example, channel uncertainties (originated from imperfect channel state information, which necessarily causes information deficiency) and a tractable response. In this paper, such trade-off is addressed as well.

1.1. Related Work. In this part, we generally provide a comprehensive overview over the existing work in relation to secrecy enhancement.

1.1.1. General Perspective. Chiefly according to the principle *Convexification* [5, 6], security is an absolutely central criterion in designing transceivers, in the context of telemedicine

games [7, 8]; cooperative relay networks [9, 10]; *wireless information power transfer* and *energy harvesting* scenarios [11, 12]; or *low-rank beamforming* issue [13].

1.1.2. Algorithms: An Overview. In [14], a secure game theory-driven transmission framework was conducted for MIMO-MEs proposing three algorithms aimed at maximising sum secrecy rate. A trade-off was theoretically defined in [15] for the principles sum secrecy rate reinforcement and *energy efficiency* which could provide a balance in physical-layer-security-based transceiver designs. In [16], three general approaches were proposed in order to choose a paradigm for *two-objective* design problems, namely, *Nash bargaining* (the most efficient one), *Jain's index*, and the *Kalai-Smorodinsky bargaining*. In [17], utilising a dynamic programming algorithm, a multilayer wiretap coding framework was fundamentally proposed.

1.1.3. Closed-Form Solutions: An Overview. Regarding *main-to-eavesdropper ratio*, SOP's diversity order remaining fixed was proven in [18]. In [19], taking into account various receiver arrangements for MIMOME transceivers over Nakagami- m fading channels, SOP was precisely computed. In [20], it was proven that the intercept probability does not rely on Eave's numbers in a cooperative-based network; instead, it relies specifically upon the number of relays. Asymptotic bounds for the outage probability defined for the secrecy rate and the achievable diversity were explored in [21]. Investigating the information's *exponential decay rate* intercepted by Eave when using an average wiretap channel code, a tight and achievable secrecy rate was mathematically derived in [22]. Taking into account the generalised degrees of freedom, an investigation was basically provided in relation to the optimality of *treating interference as noise* over $M \times 2X$ -channels in [23]. Integrating a *chaos stream cipher* with the *secure polar coding strategy*, a general secure framework was technically fulfilled in [24].

1.2. Motivation. Regarding the literature, still suboptimal solutions are needed as favourable as possible, which basically guarantee a closed-form solution in relation to the channel uncertainty-based scenarios.

1.3. Contribution. We generally calculate the asymptotic bound of the secrecy capacity which is totally acceptable providing an adequately solvable and convex equivalent problem, correspondingly.

Main Contributions. Overall, our main contribution over the existing work is to achieve a generally closed-form solution for the secrecy capacity while simultaneously guaranteeing

- (i) *convexity* which highlights a significantly more adequate response,
- (ii) *near optimality* in terms of a logically deniable outage probability of error (a principally acceptable preciseness coefficient, which also guarantees an acceptable SOP), which are absolutely defined in parallel with each other.

FIGURE 1: MIMOME-based transceiver.

In other words, we mathematically provide a general solution as a newly discovered *trade-off* irrespective of the kind of fading channels, the type of strategies, and so on. Such novel trade-off is able to be deployed to other schemes and has not been examined so far, which simultaneously is satisfied with a tight (correct) response and a deniable SOP (computation error). The mentioned trade-off is interpreted with the aim of near-optimally finding the upper-bound (worst-case) of Eave's received power.

1.4. Notation and Organisation. $(\cdot) \searrow$ means that a term falls, whereas $(\cdot) \nearrow$ means that a term rises. Additionally, $\mathbf{A}$, $\mathbf{a}$, and a stand for, respectively, matrices, vectors, and scalars. $\otimes$ stands for the Kronecker product. The other symbols and notations utilised throughout the paper are listed in Notations. Finally, all matrices and vectors are, respectively, $N \times N$ and $N \times 1$, without loss of generality.

The rest of the paper is organised as follows. Firstly, the main problem and the proposed solution are addressed in Section 2. Additionally, the simulation-based analytical results are discussed in more detail in Section 3. Finally, conclusion and proofs are given in Section 4 and the appendix, respectively.

2. Problem Description

A MIMOME-based transceiver is literally given in Figure 1. The MIMO channels between the legitimate transmitter and the legitimate user as well as Eave are principally denoted by $\mathbf{H}$ and $\mathbf{G}$ (please note that our scheme undoubtedly satisfies $\mathbf{H}$ and $\mathbf{G}$ of sizes $M \times N$ and $M \neq N$; however, we considered them as $N \times N$ (*square*) for more convenience), in a Down-link paradigm. For $\mathbf{G}$, we experience imperfect knowledge (which degrades QoS): that is, $\mathbf{G} \triangleq \mathbf{G}_1 \pm \mathbf{\Gamma}$ (our scheme is not applicable for some other frameworks [25, 26] in which, for example, the channel matrix is an arbitrary known matrix physically multiplied by a clear matrix [27, p. 4]). Now, regarding the threshold θ , for $\mathbf{G}$ we merely define the ellipsoidal uncertainty set $\mathbf{\Gamma} \triangleq \{\mathbf{\Gamma} \in \mathbb{C}^{N \times N} : \|\mathbf{\Gamma}\|^2 \leq \theta\}$. Instantaneous Ergodic capacity and also the undesired capacity (in connection with Eave) are, respectively, determined as

$$\begin{aligned} C_r &= \log \left\{ \det \left\{ \mathbf{I} + \frac{1}{\delta_r^2} \mathbf{H} \mathbf{Q} \mathbf{H}^H \right\} \right\}, \\ C_e &= \log \left\{ \det \left\{ \mathbf{I} + \frac{1}{\delta_e^2} \mathbf{G} \mathbf{Q} \mathbf{G}^H \right\} \right\}, \end{aligned} \quad (1)$$

with respect to the noise variance terms δ_r^2 and δ_e^2 at the receiver sides and the transmit covariance matrix $\mathbf{Q} \triangleq E\{\mathbf{x}\mathbf{x}^H\}$.

2.1. Our Proposed Solution

Property 1. Since we technically aim at maximising the secrecy capacity $C_S \triangleq |C_r - C_e|$ which can be logically interpreted as $\max\{0, C_r - C_e\}$, we should theoretically provide the physical implication $C_S(C_r, C_e; \theta) \in [0, \mathcal{R})$ instead of $C_S(C_r, C_e; \Gamma) \in [0, \mathcal{R})$. $\mathcal{R}$ is the target secrecy capacity.

The mapping decomposition $E\{\mathbf{x}\mathbf{x}^H\} \mapsto \mathbf{Q}$ cited above fundamentally requires the constraint $\text{rank}(\mathbf{Q}) = 1$ [28–31]. Inversely, $\mathbf{Q}$ being rank-1 unfavourably causes nonconvexity [29–31]. Of course under some circumstances, the aforementioned constraint holds and it can be alternatively dropped (e.g., in [32] in which nearly 99.79% rank-1 results in the simulations were witnessed). However, in order to guarantee the considerably more acceptable system with the higher reliability, we should ensure the design problem further.

As newly recently proposed in [33, 34], the rank-1 constraint can be basically relaxed as the dual constraints

$$\begin{bmatrix} \mathbf{A}_1 & \mathbf{Q} & \mathbf{x} \\ \mathbf{Q}^H & \mathbf{A}_2 & \mathbf{x} \\ \mathbf{x}^H & \mathbf{x}^H & 1 \end{bmatrix} \geq \mathbf{0}, \quad (2a)$$

$$\text{Tr}\{\mathbf{A}_1 - \mathbf{x}\mathbf{x}^H\} \leq 0, \quad (2b)$$

where $\mathbf{A}_1$ and $\mathbf{A}_2$ are *slack variable* matrices, correspondingly.

Fully take into account the optimisation problem below as Problem $\mathcal{P}_1$

$$\underset{\mathbf{Q} \geq \mathbf{0}}{\text{maximise}} \quad C_S, \quad (3a)$$

$$\text{Tr}\{\mathbf{Q}\} \leq P_{\text{Transmit}}, \quad (3b)$$

$$(2a), (2b), \quad (3c)$$

where P_{Transmit} is a threshold for the transmit power.

Lemma 1 (see [35]). *As described in [35], multiplying (pre or post one) by any matrix (of any rank) does not cause any change on positive semidefinite matrices' rank (see, e.g., [36, 9.6.10] for the proof).*

Corollary 2. *With respect to Lemma 1, $\text{rank}(\mathbf{M}) = \text{rank}(\mathbf{Q}) = 1$, while $\mathbf{M} \triangleq \mathbf{M}_1 \mathbf{Q} \mathbf{M}_1^H$, $\forall \mathbf{M}_1 \in \{\mathbf{H}, \mathbf{G}\}$ from (1). See, for example, [36, 9.6.10] as the positive definite property.*

Corollary 3. *After carefully writing the dual Lagrange problem, then principally taking the derivative with respect to the defined Lagrange variables, then unifying the resultant term by zero, and finally right multiplying both sides of the resultant mathematical expression by $\mathbf{Q}$, a positive semidefinite matrix would theoretically hold. Regarding Lemma 1, the exact value in relation to the rank can be conveniently calculated.*

Lemma 4 (see [37]). *If and only if $\text{rank}(\mathbf{M}) \leq 1$,*

$$\det\{\mathbf{I} + \mathbf{M}\} \geq 1 + \text{Tr}\{\mathbf{M}\}. \quad (4)$$

Corollary 5. *Simultaneously using Corollary 2 and Lemma 4, and since the $\log(\cdot)$ function has no technical influence on minimisation or maximisation in principle, we can accordingly maximise $\text{Tr}\{\mathbf{H}\mathbf{Q}\mathbf{H}^H\}$, as well as maximising $-\text{Tr}\{\mathbf{G}\mathbf{Q}\mathbf{G}^H\}$, which is in correspondence with the signal-to-noise ratio (SNR) and Eave's received power, respectively. Now, with the aid of SNR instead of $\text{Tr}\{\mathbf{H}\mathbf{Q}\mathbf{H}^H\}$, and defining ξ as a threshold for the maximum of Eave's received power, Problem $\mathcal{P}_2$ is*

$$\underset{\mathbf{Q} \geq \mathbf{0}}{\text{maximise}} \quad \text{SNR}, \quad (5a)$$

$$\max_{\|\Gamma\|^2 \leq \theta} \{\text{Tr}\{\mathbf{G}\mathbf{Q}\mathbf{G}^H\}\} \leq \xi, \quad (5b)$$

$$\text{Tr}\{\mathbf{Q}\} \leq P_{\text{Transmit}}, \quad (5c)$$

$$(2a), (2b). \quad (5d)$$

Methodology. We remove the constraint (5b) and accurately add it to the cost-function as a penalty: namely, $I_{\text{Old}}(\mathbf{Q}, \mathbf{G}_1; \Gamma)$. According to the *penalty method* (see, e.g., [17]), Problem $\mathcal{P}_3$ is alternatively expressed as

$$\underset{\mathbf{Q} \geq \mathbf{0}}{\text{maximise}} \quad \text{SNR} - \mathcal{D}_1^-, \quad (6a)$$

$$(5c), (5d), \quad (6b)$$

for which we have

$$\mathcal{D}_1^- \triangleq \min \left\{ \xi, \max_{\|\Gamma\|^2 \leq \theta} \underbrace{\{\text{Tr}\{\mathbf{G}\mathbf{Q}\mathbf{G}^H\}\}}_{I_{\text{Old}}(\mathbf{Q}, \mathbf{G}_1; \Gamma)} \right\}. \quad (7)$$

$\mathcal{P}_3$ is nonconvex, per se, owing to the lack of control on the error in the estimation of $\mathbf{G}$, originated from the channel uncertainty parameter Γ . Since $\mathcal{P}_3$ has no closed-form solution with respect to its existing format, consequently, it needs an entirely appropriate alternative. See the following theorem.

Theorem 6. $\mathcal{P}_3$ *unhesitatingly has a solvable and relaxed alternative as Problem $\mathcal{P}_4$ as*

$$\underset{\mathbf{Q} \geq \mathbf{0}}{\text{maximise}} \quad \text{SNR} - \mathcal{D}_2^-, \quad (8a)$$

$$(5c), (5d), \quad (8b)$$

in which

$$\mathcal{D}_2^- \triangleq \min \{\xi, I_{\text{New}}(\mathbf{Q}, \mathbf{G}_1; \theta)\}, \quad (9)$$

$$I_{\text{New}}(\mathbf{Q}, \mathbf{G}_1; \theta) \triangleq \max_{\|\Gamma\|^2 \leq \theta} \{\text{Tr}\{\mathbf{G}\mathbf{Q}\mathbf{G}^H\}\}, \quad (10)$$

while the upper-bound of (10) can be conveniently expressed as

$$\mathcal{B} \triangleq \text{Tr}\{\mathbf{G}_1 \mathbf{Q} \mathbf{G}_1^H\} + \text{Tr}\{\mathbf{Q} \odot \mathbf{Q}\} \times \underbrace{\max\{\|\Gamma\|^4\}}_{\theta^2}. \quad (11)$$

See the Appendix for the proof.

Therefore, the upper-bound of (10) is recasted to $\mathcal{B}$ as well. See the following lemma.

Lemma 7. *Defining the deterministic value $I_{\text{New}}(\mathbf{Q}, \mathbf{G}_1; \theta)$ instead of $I_{\text{Old}}(\mathbf{Q}, \mathbf{G}_1; \Gamma)$ as its worst-case (upper-bound) and simultaneously maximising $-I_{\text{New}}(\mathbf{Q}, \mathbf{G}_1; \theta)$ provide the asymptotic bound of the optimisation problem in terms of θ , which efficiently guarantees convexity and then tractability. Indeed, we merely provided a technical segregation between the terms q_{ii} and e_{ii} (in the Appendix), which chiefly provided an opportunity where the inaccessible and unrecognised (in relation to the ellipsoidal channel uncertainty sets) term e_{ii} is generally formulated from another viewpoint.*

Lemma 8. *According to Schur product theorem [38, Theorem 7.5.3], $\mathbf{Q} \odot \mathbf{Q}$ would be inevitably a positive semidefinite matrix; therefore, the key features (intrinsic physical and statistical properties) sufficiently remain stable.*

3. Results

In this section, we analyse the system performance as well.

Some parameters and assumptions in the simulations are as follows. P_{Transmit} is equal to SNR. Correlations at the MIMO antenna array are defined as 0%. The number of randomly generated Rayleigh fading channel realisations is 1000. N , θ , and ξ are separately defined for each figure.

Figure 2 strongly proves the tremendously sensible reliability in terms of the noticeably acceptable outage probability error (which is mathematically defined in (12)), which is plotted versus the θ regime while changing N . The relative content is repeated in the subfigure (b) for 3 dimensions

against θ and N . Meanwhile, we should inform that $\theta = 0$ technically means the perfect CSI case.

Analytically, the outage probability error is written as

$$\mathcal{O}_{\text{Prob}} := E_{\Gamma, \theta} \left\{ \frac{|\mathcal{D}_2^- - \mathcal{D}_1^-|}{\mathcal{D}_1^-} \right\}, \quad (12)$$

according to which *preciseness coefficient* is calculated as $1 - \mathcal{O}_{\text{Prob}}$.

It should be noted that, for $N = 4$ or higher, our proposed solution is completely trustable or even for $N = 2$ while having the lower error rates in the estimation, that is, $\forall \theta \leq 0.5$. Inversely, for $N = 1$ (Single-Input Single-Output schemes) such closed-form solution has a remarkably less reliable performance. The case 1×1 is discovered in detail in the second subsection.

Figure 3 repeats the previous one for $1 - \mathcal{O}_{\text{Prob}}$ in the context of *preciseness coefficient*. As can be seen, for $N = 2$ and $\forall \theta \leq 0.5$, preciseness coefficient is higher than 90%, which is enhanced at $\geq 95\%$ for higher N s. Again, the relative content is repeated in the subfigure (b) for 3 dimensions against θ and N . Meanwhile, we should inform that $\theta = 0$ technically means the perfect CSI case.

Figure 4 shows the observably more efficient secrecy capacity for our approach compared to the *worst-case method* prevalently utilised in the literature [39–41], while changing N and θ and also having $\xi = 50$ mWatt. Such strong reinforcement is effectively justified by the markedly more adequate convergence for $\mathcal{P}_4$, analytically caused by convexity comprehensively originated from solvability. Worst-case method in our simulation is applied according to S-Lemma (see, e.g., [39, eq. 20–21], [40, eq. 11–15], [41, eq. 58–61]) which indicates that (5b) can be relaxed as

$$\begin{bmatrix} \text{vec}(\mathbf{G}_1)^H (\mathbf{Q}^H \otimes \mathbf{I}_N) \text{vec}(\mathbf{G}_1) - \xi - \theta A_1 & \text{vec}(\mathbf{G}_1)^H (\mathbf{Q}^H \otimes \mathbf{I}_N) \\ (\mathbf{Q}^H \otimes \mathbf{I}_N) \text{vec}(\mathbf{G}_1) & (\mathbf{Q}^H \otimes \mathbf{I}_N) + A_1 \mathbf{I}_N \end{bmatrix} \succeq \mathbf{0}. \quad (13)$$

In the *linear matrix inequality*-based expression (13), A_1 is the slack variable.

In Figure 5, the secrecy capacity for our approach compared to the *worst-case method* is depicted against SNR (dB), while changing N and θ and also having $\xi = 100$ mWatt. It is revealed that the higher ξ we adjust, the larger values for the secrecy capacity can be mathematically achieved. This point can be theoretically analysed as follows. For example, assume that the general convex optimisation problem maximise $\mathcal{M}_1 = a_1 x - b_1 x$, subjected to $b_1 x \leq \xi$. In general, $\mathcal{M}_1 \nearrow$ when $\xi \nearrow$. It is sufficient to write *Lagrange function* for the problem, after taking the derivative with respect to one *Lagrange variable* in connection with the unique constraint and also x and then unifying the resultant terms by zero; $\mathcal{M}_1 = \xi(a_1/a_2 - 1)$. Indeed, $\mathcal{M}_1 \propto \xi$. In other words, the higher ξ physically causes the bigger *search region*. Finally, how to take the derivative needed for our scheme is essentially obvious according to the fact

$(\sigma/\sigma\mathbf{Q})\text{Tr}\{\mathbf{M}_1\mathbf{Q}\mathbf{M}_1^H\} = \mathbf{M}_1^H\mathbf{M}_1$, while $\mathbf{M}_1 \in \{\mathbf{H}, \mathbf{G}\}$, which is proven with regard to $(\sigma/\sigma\mathbf{X})\text{Tr}\{\mathbf{A}\mathbf{X}\mathbf{B}\} = \mathbf{A}^H\mathbf{B}^H$, which is given in [36, eq. 101].

Figure 6 illustrates SOP against SNR (dB) as well for the different values of ξ , θ , and N . Analytically, SOP is expressed as

$$\text{SOP} := E_{\Gamma, \theta} \left\{ \frac{|C_W - C_{\text{WO}}|}{C_{\text{WO}}} \right\}, \quad (14)$$

in which C_W and C_{WO} conventionally denote the optimised secrecy capacity achieved, respectively, from the case of applying our scheme ($\text{SNR} - \mathcal{D}_2^-$) (see (8a)) and of not applying our scheme ($\text{SNR} - \mathcal{D}_1^-$) (see (6a)). SOP fairly seems acceptable even for the case 1×1 , which is technically less than 0.0005 for the case where $\xi = 50$ mWatt and $\theta = 0.3$, $\forall \text{SNR} \in [12 \text{ dB}, \infty)$.

FIGURE 2: Outage probability.

FIGURE 3: 1 - outage probability.

Figure 6 is briefly analysed in Table 1. In this table, the values in connection with ξ are in terms of mWatt which are ignored (not written) for more convenience. Indeed, the asymptotic bound of the secrecy capacity is technically equal to SNR while mathematically subtracting Eave's received power. The penalty in relation to Eave's received power is basically equal to $\min\{\xi, I_{\text{New}}(\theta)\}$, which would be evidently fixed at ξ in our simulations in the high SNR regime; that is, -10 dB for the case where $\xi = 100$ mWatt and $\forall \text{SNR} \in [17 \text{ dB}, \infty)$.

In Figure 7, the penalty function in connection with Eave's received power (undesired power) against SNR (dB) is shown while changing ξ . It is in parallel with Figure 6.

Secrecy capacity in Figure 8 is depicted against SNR (dB) for the cases of perfect CSI ($\theta = 0$) and imperfect one ($\theta \neq 0$), while $\xi = 100$ mWatt and $N = 8$. In this figure, our method is compared with the worst-case one [39–41].

3.1. Complexity. In relation to the complexity, we should compare (11) with (13). To this end, among the methods in the

FIGURE 4: Secrecy capacity versus SNR, while $\xi = 50$ mWatt.TABLE 1: SNRs needed for guaranteeing $\text{SOP} \leq 0.1\%$.

	$\xi = 50,$ $\theta = 0.3$	$\xi = 50,$ $\theta = 0.6$	$\xi = 100,$ $\theta = 0.3$	$\xi = 100,$ $\theta = 0.6$
$N = 1$	7	11	13	∞
$N = 2$	0	0	7	10

literature (e.g., [5, 32, 42]), we use the procedure of counting the flip-flops, as described in [5, Table 3]. In this method, for example, the complexity of the matrix product for two matrices of sizes, respectively, $N \times K$ and $K \times L$ is $\mathcal{O}(NL(2K - 1))$.

Regarding an extreme range of operations in (13), our scheme has a more favourable complexity, which is $\approx \mathcal{O}(4N^3)$ compared to $\approx \mathcal{O}(14N^4)$ in which $\mathcal{O}(\cdot)$ is Big-O function.

3.2. 1×1 Case

Feature 1. According to $\mathcal{O}_{\text{Prob}}$, the reliability for $N = 1$ is crucially lower than that of the cases with larger values for N . However, because of the term SNR which is extremely larger than $\mathcal{D}_2^-$ (see (8a)), SOP can be guaranteed instead, which perfectly highlights the importance of the outperformance, correctness, and effectiveness of our work.

Feature 2. For the case 1×1 , convexity theoretically is satisfied.

FIGURE 5: Secrecy capacity versus SNR, while $\xi = 100$ mWatt.

3.3. Quick Overview

Feature 3. In general, from (14) it can be seen that $\lim_{\text{SNR (dB)} \rightarrow \infty} \text{SOP} = 0$ since $\text{SNR} \gg \mathcal{D}_1^-, \mathcal{D}_2^-$.

Feature 4. In general, $\text{SOP} \searrow$ when $N \nearrow$.

Feature 5. In general, $\mathcal{O}_{\text{Prob}} \searrow$ when $N \nearrow$; accordingly, $1 - \mathcal{O}_{\text{Prob}} \nearrow$ when $N \nearrow$.

With respect to the main advantages thoroughly discussed in relation to the proposed scheme, its outperformance, correctness, and effectiveness are obviously highlighted over the existing methods (conventionally utilised in the literature, specifically the worst-case one).

4. Conclusion

An asymptotic bound for the secrecy capacity in the context of resource allocation was suboptimally defined for MIMOME-based systems for a general channel uncertainty fashion, supporting one theorem and also some lemmas and corollaries. The suboptimality cited above was principally highlighted in terms of a significantly acceptable trade-off between tractability and a less outage probability. Indeed, the deniable values obtained for the relative outage probability guaranteed our framework, which also fundamentally highlighted a tight and acceptable response for the system as well. The relative outage probability was almost 5% for EEVs ≤ 0.9 for 4×4 MIMO antenna arrays. Our proposed framework is

FIGURE 6: SOP versus SNR (dB).

completely implementable for other general equilibria, which basically provided SOPs less than 5×10^{-4} for the case where $\xi = 50 \text{ mWatt}$ and $\theta = 0.3$, $\forall \text{SNR} \in [12 \text{ dB}, \infty)$.

Appendix

Proof of Theorem 6. (10) is written as

$$\begin{aligned} & \text{Tr} \{ \mathbf{G}_1 \mathbf{Q} \mathbf{G}_1^H \} + \max_{\|\mathbf{\Gamma}\|^2 \leq \theta} \left\{ \text{Tr} \{ \mathbf{\Gamma} \mathbf{Q} \mathbf{\Gamma}^H \} \right\} = \mathcal{D}_3 \\ & + \left\{ \sum_{i=1}^N q_{ii} e_{ii} \right\} + \mathcal{L} \{ e_{ij}, e_{ji}, q_{ji}, q_{ij} \}_{i \neq j} \stackrel{(a)}{\lesssim} \mathcal{D}_3 \end{aligned}$$

$$\begin{aligned} & + \sum_{i=1}^N q_{ii} e_{ii} \stackrel{(b)}{\leq} \mathcal{D}_3 + \left\{ \sum_{i=1}^N q_{ii} e_{ii} \right\}^2 \stackrel{(c)}{\leq} \mathcal{D}_3 + \sum_{i=1}^N \{q_{ii}\}^2 \\ & \cdot \sum_{i=1}^N \{e_{ii}\}^2 \leq \mathcal{B}, \end{aligned} \tag{A.1}$$

in which $\mathcal{B}$ is provided in (11) and

$$\mathcal{D}_3 = \text{Tr} \{ \mathbf{G}_1 \mathbf{Q} \mathbf{G}_1^H \}. \tag{A.2}$$

$e_{ii} \in \mathbb{R}$ (unclear) and q_{ii} are, respectively, the ii th main diagonals elements of $\mathbf{\Gamma}^H \mathbf{\Gamma}$ and $\mathbf{Q}$; also $\mathcal{L}(\cdot)$ is a linear

FIGURE 7: Penalty versus SNR, while changing ξ . FIGURE 8: Secrecy capacity versus SNR (dB) for the cases of perfect ($\theta = 0$) and imperfect CSI, while $\xi = 100$ mWatt and $N = 8$.

function of the off-main diagonal elements ($\in \mathbb{R}$). (A.1) is analytically written by knowing

$$\begin{aligned} \text{Tr}\{\mathbf{AB}\} &= \text{Tr}\{\mathbf{BA}\}, \\ \text{Tr}\{\mathbf{A} + \mathbf{B}\} &= \text{Tr}\{\mathbf{A}\} + \text{Tr}\{\mathbf{B}\}. \end{aligned} \quad (\text{A.3})$$

The proof can be conveniently completed regarding the detailed Remarks A.1, A.2, and A.3.

Remark A.1. The fourth line in (A.1) is literally approximated while generally ignoring $\mathcal{L}(\cdot)$. Succinctly speaking, the general perspective and theoretical background behind

the forenamed negligence lie mostly in the influence of the norms of the relative terms. The aforementioned logic can be theoretically observed in Figure 2.

Remark A.2. The logic behind the fifth line in (A.1) comes technically from the physical and casual behaviour of both precoder and error matrices. Indeed, since the forenamed matrices are positive semidefinite, hence, they should principally exist.

Remark A.3. The penultimate line in (A.1) straightforwardly originates from *Cauchy-Schwarz-Bunyakovsky inequality* [43, eq. 11–112].

The proof of Theorem 6 is completed. $\square$

Notations

$(\cdot)^H$:	Hermitian
$\det\{\cdot\}$:	Determinant
$\log\{\cdot\}$:	Logarithm
$\text{Tr}(\cdot)$:	Trace of matrix
$\max\{\cdot\}$:	Maximum value
$\min\{\cdot\}$:	Minimum value
$\ \cdot\ _F$:	Frobenius norm
$\mathbf{0}$:	All-zeros matrix
$\mathbf{I}_N$:	N -by- N identity matrix
$\mathbf{A} \geq \mathbf{0}$:	Hermitian positive semidefinite matrix
$\mathbb{C}^{N \times N}$:	N -by- N dimension complex space
$\odot$:	Hadamard product
$ \cdot $:	Absolute value
$E_z(\cdot)$:	Expected value over z .

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

References

- [1] H. Zhang, J. Du, J. Cheng, and V. C. M. Leung, "Resource allocation in SWIPT enabled heterogeneous cloud small cell networks with incomplete CSI," in *Proceedings of the 59th IEEE Global Communications Conference, GLOBECOM 2016*, Washington, DC, USA, December 2016.
- [2] B. Han, S. Zhao, B. Yang, H. Zhang, P. Chen, and F. Yang, "Historical PMI Based multi-user scheduling for FDD massive MIMO systems," in *Proceedings of the 83rd IEEE Vehicular Technology Conference, VTC Spring 2016*, Nanjing, China, May 2016.
- [3] L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, Article ID e2992, 2017.
- [4] S. Soderi, L. Mucchi, M. Hämmäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 7, Article ID e3142, 2016.
- [5] M. Zamanipour, "Probabilistic-based secrecy rate maximisation for MIMOME wiretap channels: Towards novel convexification procedures," *Transactions on Emerging Telecommunications Technologies*, Article ID e3154, 2017.

- [6] S.-H. Lee, W. Zhao, and A. Khisti, "Secure degrees of freedom of the Gaussian diamond-wiretap channel," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 63, no. 1, pp. 496–508, 2017.
- [7] B. C. Akdeniz, B. Tepekule, A. E. Pusane, and T. Tuğcu, "Novel network coding approaches for diffusion-based molecular nanonetworks," *Transactions on Emerging Telecommunications Technologies*, 2016.
- [8] C. Han, L. Sun, and Q. Du, "Securing Image Transmissions via Fountain Coding and Adaptive Resource Allocation," in *Proceedings of the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 15–18, Nanjing, China, May 2016.
- [9] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, 2016.
- [10] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 7971–7984, 2016.
- [11] M. Zhang and Y. Liu, "energy harvesting for physical-layer security in OFDMA networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 154–162, 2016.
- [12] M. Zhang, Y. Liu, and R. Zhang, "artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 3085–3096, 2016.
- [13] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE Journal of Selected Topics in Signal Processing*, vol. PP, no. 99, 2016.
- [14] P. Siyari, M. Krunz, and D. N. Nguyen, "Friendly Jamming in a MIMO Wiretap Interference Network: A Nonconvex Game Approach," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 601–614, 2017.
- [15] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure Green Communication via Untrusted Two-Way Relaying: A Physical Layer Approach," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1861–1874, 2016.
- [16] A. Garnaeve and W. Trappe, "Bargaining over the fair trade-off between secrecy and throughput in OFDM communications," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 242–251, 2017.
- [17] M. Jafari Siavoshani, S. Mishra, C. Fragouli, and S. N. Diggavi, "Multi-party secret key agreement over state-dependent wireless broadcast channels," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, 2016.
- [18] D. Deng, L. Fan, R. Zhao, and R. Q. Hu, "Secure communications in multiple amplify-and-forward relay networks with outdated channel state information," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 4, pp. 494–503, 2016.
- [19] D. B. Da Costa, N. S. Ferdinand, U. S. Dias, R. T. De Sousa, and M. Latva-Aho, "Secrecy performance of MIMO Nakagami-m wiretap channels with optimal TAS and different antenna schemes," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 6, pp. 828–841, 2016.
- [20] X. Ding, T. Song, Y. Zou, and X. Chen, "Improving secrecy for multi-relay multi-eavesdropper wireless systems through relay selection," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 7, pp. 982–991, 2016.
- [21] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 335–346, 2017.
- [22] M. Bastani Parizi, E. Telatar, and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 63, no. 1, pp. 509–531, 2017.
- [23] S. Gharekhloo, A. Chaaban, and A. Sezgin, "Expanded GDoF-optimality regime of treating interference as noise in the $M \times 2$ X-channel," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 63, no. 1, pp. 355–376, 2017.
- [24] Y. Zhao, X. Zou, Z. Lu, and Z. Liu, "Chaotic encrypted polar coding scheme for general wiretap channel," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2017.
- [25] C. Du, X. Chen, and L. Lei, "Energy-efficient optimisation for secrecy wireless information and power transfer in massive MIMO relaying systems," *IET Communications*, vol. 11, no. 1, pp. 10–16, 2017.
- [26] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 956–968, 2017.
- [27] M. Sadeghzadeh, H. R. Bahrami, and N. H. Tran, "Clustered linear precoding for downlink network MIMO systems with partial CSI," *Wireless Communications and Mobile Computing*, vol. 16, no. 15, pp. 2340–2355, 2016.
- [28] M. Xie, X. Jia, M. Zhou, and L. Yang, "Secure massive MIMO-enabled full-duplex 2-tier heterogeneous networks by exploiting in-band wireless backhauls," *Transactions on Emerging Telecommunications Technologies*, 2017.
- [29] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677–689, 2017.
- [30] F. S. Al-Qahtani, Y. Huang, S. Hessien, R. M. Radaydeh, C. Zhong, and H. Alnuweiri, "Secrecy analysis of MIMO wiretap channels with low-complexity receivers under imperfect channel estimation," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, 2016.
- [31] M. R. A. Khandaker, K.-K. Wong, Y. Zhang, and Z. Zheng, "Probabilistically robust SWIPT for secrecy MISOME systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 211–226, 2017.
- [32] K.-Y. Wang, A. M. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization," *IEEE Transactions on Signal Processing*, vol. 62, no. 21, pp. 5690–5705, 2014.
- [33] Z. Chu, Z. Zhu, and J. Hussein, "Robust optimization for AN-aided transmission and power splitting for secure MISO SWIPT system," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1571–1574, 2016.
- [34] J. Yang, Q. Li, Y. Cai, Y. Zou, L. Hanzo, and B. Champagne, "Joint secure AF relaying and artificial noise optimization: a penalized difference-of-convex programming framework," *IEEE Access*, vol. 4, pp. 10076–10095, 2016.
- [35] M. R. A. Khandaker and K.-K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 10–13, 2015.

- [36] K. Petersen and M. Pedersen, *The Matrix Cookbook*, Technical University of Denmark, Kongens Lyngby, Denmark, 2012.
- [37] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, 2016.
- [38] R. Horn and C. Johnson, *Matrix Analysis*, Cambridge University Press, New York, NY, USA, 2013.
- [39] Y. Tan, Q. Li, C. Xu, Q. Zhang, and J. Qin, "Robust transceiver design in multiuser MIMO system with energy harvesting constraints," *Wireless Personal Communications*, pp. 1–12, 2017.
- [40] S. Wang and B. Wang, "Robust secure transmit design in MIMO channels with simultaneous wireless information and power transfer," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 2147–2151, 2015.
- [41] H. Zhang, Y. Huang, C. Li, and L. Yang, "Secure beamforming design for SWIPT in MISO broadcast channel with confidential messages and external eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7807–7819, 2016.
- [42] T. A. Le, Q. Vien, H. X. Nguyen, D. W. Ng, and R. Schober, "Robust chance-constrained optimization for power-efficient and secure SWIPT systems," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 3, pp. 333–346, 2017.
- [43] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 2015.