An Algorithm for Optimal Secure Signaling over Cognitive Radio MIMO Channels

Limeng Dong, Sergey Loyka, Yong Li

***Abstract*—The multiple-input multiple-output (MIMO) Gaussian wire-tap channel (WTC) model is considered in the cognitive radio (CR) setting, where there is a interference power constraint (IPC), in addition to the total transmit power constraint (TPC). Based on the recently established mini-max characterization of its secrecy capacity, a numerical algorithm for global maximization of secrecy rates over such channels is proposed, which is based on the barrier method in combination with the residual-form Newton method and backtracking line search. Unlike the known algorithms, the proposed algorithm is guaranteed to converge to a global (rather than local) optimum. Its efficient performance is illustrated by examples.**

I. Introduction

Exponential growth of wireless systems and services in the past two decades has made the wireless spectrum a very scarce resource. The traditional model of fixed frequency allocation became a bottleneck and a new approach, term ’cognitive radio’ (CR) has gained considerable attention recently [1], where secondary users are allowed to transmit provided that they do not create significant interference to primary users (the spectrum license holders). Hence, interference management becomes a key issue. To this end, multiple-input multiple-output (MIMO) systems become a valuable design approach in the CR settings. A number of approaches have been proposed to maximize the capacity of secondary users’ channels subject to the total transmit and interference power constraints (TPC and IPC) [2]-[3]. The CR Gaussian MIMO channel is studied in [2] and a game-theoretic approach is employed to control the interference as well as to maximize the achievable transmission rates. Similar approach in the multiple-input single-output (MISO) setting is considered in [3] and several closed-form solutions and sub-optimal beamforming are proposed.

In addition to interference, wireless systems are vulnerable to various attacks such as eavesdropping by malicious (unauthorized) users due to the broadcast nature of wireless channels (this is especially true in the CR setting). To address this issue, the physical-layer security approach has recently emerged as a valuable complement to cryptography-based approaches [4][5]. In this approach, the secrecy of communications is ensured at the physical layer by exploiting the properties of physical communication channels so that no transmitted information can be recovered by an eavesdropper. Using this approach in combination with MIMO systems offers significant new opportunities for enhancing the secrecy of CR wireless communications via space-domain processing. The wiretap channel (WTC) model became a popular tool to study physical-layer security, where the transmitter (Tx) sends information to the receiver (Rx) while an eavesdropper (Ev) observes the transmission. The key performance metric is the secrecy capacity, defined operationally as the maximum achievable rate on the Tx-Rx link subject to the reliability (low error probability) and secrecy (low information leakage on the Tx-Ev link) criteria [4]. The secrecy capacity of Gaussian MIMO WTC has been established in [6][7], where the optimality of Gaussian signaling has been proved. However, while some special cases have been settled [8][9], the optimal Tx covariance matrix is unknown in the general case, which remains a difficult open problem due to the non-convex nature of the underlying optimization problem.

To this end, a number of numerical optimization algorithms have been developed [10]-[12]. Unfortunately, they lack provable *global* convergence due to the non-convex nature of the problem (since Karush-Kuhn-Tucker (KKT) conditions are *not* sufficient for global optimality as the problem is not convex). A *globally*-convergent algorithm was proposed in [13], which overcomes this fundamental difficulty by using the max-min reformulation of the original non-convex problem, and its global convergence was proved. However, no interference power constraint (IPC) was considered so it cannot be used in the CR setting. The absence of the IPC significantly simplifies the problem since (i) the feasible set of Tx covariance matrices is isotropic (no limitations on eigenvectors) and (ii) the TPC is always active. Neither of these is true in the CR setting, which posses additional difficulties: (i) the feasible set is not isotropic anymore, due to the interference power constraint, and (ii) the TPC can be inactive (when the IPC dominates) and, furthermore, it is not known in advance which constraint is active or not.

In this paper, we overcome these difficulties by using the recently-established max-min reformulation of the original non-convex problem in the CR setting [16], and develop a numerical algorithm for global maximization of secrecy rates over Gaussian MIMO CR channels based on the barrier method in combination with the residual-form Newton method and backtracking line search. The global (rather than local) convergence of this algorithm follows from the fact that the reformulated objective function is convex-concave in the right way so that the KKT conditions are sufficient for global optimality.

It should be noted that the Gaussian MISO WTC channel (with single-antenna receivers) in the CR setting has been considered in [14][15] and several algorithms for globally-

L. Dong is with the School of Electronics and Information, Northwestern Polytechnical University, Xian, China, e-mail: dlm nwpu@hotmail.com. This work was done when L.Dong was visiting the School of Electrical Engineering and Computer Science, University of Ottawa, Canada and was supported by the China Scholarship Council.

S. Loyka is with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada, e-mail: sergey.loyka@ieee.org.

Y. Li is with the School of Electronics and Information, Northwestern Polytechnical University, Xian, China, e-mail: ruikel@nwpu.edu.cn.

978-1-5090-5990-4/17/$31.00 ©2017 IEEE

optimal signaling were proposed exploiting the quasi-convex nature of the problem. Unfortunately, this approach fails in the MIMO setting (since the MIMO channel cannot be equivalently reduced to a single scalar channel, unlike the MISO channel), which thus remains an open problem addressed in this paper.

Notations: bold lower-case letters $(\mathbf{a})$and capitals $(\mathbf{A})$ denote vectors and matrices respectively; $\mathbf{A} \geq \mathbf{0}$ denotes positive semi-definite matrix $\mathbf{A}$; $\mathbf{A}'$ and $\mathbf{A}^{+}$ denote transpose and conjugate transpose; $tr(\mathbf{A})$ is the trace; *vec*$(\mathbf{A})$ is the vector obtained by stacking all columns of matrix $\mathbf{A}$ on top of each other and *vech*$(\mathbf{A})$ is the vector obtained by vectorizing only the lower triangular part of $\mathbf{A}$; *diag*$(\mathbf{A})$ is a diagonal matrix with the same diagonal entries as in $\mathbf{A}$; $E\{\cdot\}$ is a statistical expectation; $|\mathbf{a}|$ and $|\mathbf{A}|$ are the Euclidian norm of vector $\mathbf{a}$ and determinant of matrix $\mathbf{A}$; $\mathbf{I}$ is the identity matrix of appropriate size.

II. System Model

Let us consider the standard AWGN WTC model in Fig.1, where a Tx sends confidential information to a Rx while an Ev intercepts the transmission. The objective is to ensure reliable communications between the Tx and Rx (the reliability criterion) while keeping the Ev ignorant about transmitted information (the secrecy criterion). The secrecy capacity is the largest transmission rate subject to the reliability and secrecy criteria [4].

In the discrete-time AWGN MIMO channel model, the signals received by the Rx and the Ev can be expressed as

$$\mathbf{y}_1 = \mathbf{H}_1\mathbf{x} + \boldsymbol{\xi}_1, \quad \mathbf{y}_2 = \mathbf{H}_2\mathbf{x} + \boldsymbol{\xi}_2 \tag{1}$$

where $\mathbf{y}_1, \mathbf{y}_2$ are the respective received signals, $\mathbf{x}$ is the transmitted signal, $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2$ represent zero-mean unit-variance i.i.d. noise at the Rx and Ev end respectively; $\mathbf{H}_1, \mathbf{H}_2$ are the channel matrices collecting channel gains from the Tx to the Rx and Ev respectively. We assume that the Tx has m antennas, while the Rx and Ev have n_1 and n_2 antennas. In addition to this, following the CR model, there is a primary receiver (PR) whose received signal is

$$\mathbf{y}_3 = \mathbf{H}_3\mathbf{x} + \boldsymbol{\xi}_3 \tag{2}$$

where $\mathbf{H}_3$ and $\boldsymbol{\xi}_3$ are the channel matrix and noise of the PR. We assume that full channel state information (CSI) is available to the Tx, Rx and Ev (but not necessarily to the PR). In the following, we will use $\mathbf{W}_k = \mathbf{H}_k^{+}\mathbf{H}_k, k = 1, 2, 3$.

In the CR setting, the transmission is subject to TPC and IPC, so that any Tx covariance matrix $\mathbf{R} = E\{\mathbf{x}\mathbf{x}^{+}\}$ must be in the following feasible set $S_{\mathbf{R}}$:

$$S_{\mathbf{R}} = \left\{\mathbf{R} : tr(\mathbf{R}) \leq P_T,\ tr(\mathbf{H}_3\mathbf{R}\mathbf{H}_3^{+}) \leq P_I,\ \mathbf{R} \geq \mathbf{0}\right\} \tag{3}$$

where $P_T,\ P_I$ are the maximum allowed Tx and interference powers respectively. The interference power constraint $tr(\mathbf{H}_3\mathbf{R}\mathbf{H}_3^{+}) \leq P_I$ ensures that the total interference power at the PR does not exceed the threshold P_I so that its performance is not distorted. The secrecy capacity of the CR WTC is defined operationally as the largest achievable rate subject to the power, reliability and interference constraints simultaneously.

III. Secrecy Capacity of CR MIMO Wiretap Channel

The following characterization of the secrecy capacity of the Gaussian CR MIMO WTC established recently in [16] will be instrumental below to develop a numerical optimization algorithm with a guaranteed convergence to a global optimum.

Theorem 1. *The secrecy capacity of Gaussian MIMO CR channel under the TPC and the IPC can be equivalently expressed as*

$$C = \max_{\mathbf{R} \in S_{\mathbf{R}}} C(\mathbf{R}) = \max_{\mathbf{R} \in S_{\mathbf{R}}} \min_{\mathbf{K} \in S_{\mathbf{K}}} f(\mathbf{R}, \mathbf{K}) \tag{4}$$

where $\mathbf{H} = [\mathbf{H}_1^{+}, \mathbf{H}_2^{+}]^{+}$, $\mathbf{N} = E\left\{\boldsymbol{\xi}_1\boldsymbol{\xi}_2^{+}\right\}$ *and*

$$\begin{aligned}
&C(\mathbf{R}) = \ln|\mathbf{I} + \mathbf{W}_1\mathbf{R}| - \ln|\mathbf{I} + \mathbf{W}_2\mathbf{R}|,\\
&f(\mathbf{R}, \mathbf{K}) = \ln|\mathbf{I} + \mathbf{K}^{-1}\mathbf{H}\mathbf{R}\mathbf{H}^{+}| - \ln|\mathbf{I} + \mathbf{W}_2\mathbf{R}|,\\
&S_{\mathbf{R}} = \{\mathbf{R} : \mathbf{R} \geq \mathbf{0},\ \mathrm{tr}(\mathbf{R}) \leq P_T,\ \mathrm{tr}(\mathbf{W}_3\mathbf{R}) \leq P_I\},\\
&S_{\mathbf{K}} = \left\{\mathbf{K} : \mathbf{K} = \begin{bmatrix} \mathbf{I} & \mathbf{N} \\ \mathbf{N}^{+} & \mathbf{I} \end{bmatrix}, \mathbf{K} \geq \mathbf{0}\right\}.
\end{aligned} \tag{5}$$

Proof. The proof is based on the method of [6] judiciously incorporating the IPC in each step. Even though the feasible set $S_{\mathbf{R}}$ above is not isotropic anymore (due to the IPC *tr*$(\mathbf{W}_3\mathbf{R}) \leq P_I$), unlike that in [6], it can still be shown that the saddle point property and all key inequalities do hold, which allow one to establish the capacity. See [16] for further details and all steps of the proof. □

It can be further shown that

$$C(\mathbf{R}) \leq f(\mathbf{R}, \mathbf{K}) \tag{6}$$

so that $f(\mathbf{R}, \mathbf{K})$ serves as an upper bound to the achievable secrecy rate $C(\mathbf{R})$ and $\max_{\mathbf{R} \in S_{\mathbf{R}}} f(\mathbf{R}, \mathbf{K})$ serves as an (convex) upper bound to the secrecy capacity C:

$$C \leq \max_{\mathbf{R} \in S_{\mathbf{R}}} f(\mathbf{R}, \mathbf{K}) \tag{7}$$

It follows from Theorem 1 that the secrecy capacity can be equivalently represented in 2 different ways, involving optimizations over $\mathbf{R}$ and $\mathbf{K}$. Since no closed-form solution is known to either one in the general case, we develop below a numerical algorithm to find the optimal Tx covariance matrix. While the 1st representation looks simpler (due to single optimization), it is not a convex problem in general (unless the WTC is degraded) so that KKT conditions are *not* sufficient for global optimality and numerical optimization with guaranteed convergence to a *global* optimum is out of reach. On the other hand, while 2nd max-min representation looks more complex, it is in fact much more trackable since both optimizations are convex (since $f(\mathbf{R}, \mathbf{K})$ is concave in $\mathbf{R}$ and convex in $\mathbf{K}$), the KKT conditions (for both optimizations) are sufficient for global optimality and hence a numerical algorithm can be developed with guaranteed convergence to a global optimum following the approach originally developed in [13] for the MIMO WTC without the interference constraint, as explained below.

IV. An Algorithm for Global Maximization of Secrecy Rates Under Interference Constraint

Performing separately $\max$ and $\min$ optimizations in the max-min part of (4) immediately faces a serious difficulty of achieving or proving convergence of the algorithm due to its oscillatory behaviour. To overcome this difficulty, we use the residual form of Newton method where both optimizations (max and min) are done simultaneously, as discussed in details in [13]. This opens up a way to provable global convergence. Since only the TPC was considered in [13], (i) the feasible set there was isotropic, and (ii) the TPC was always active, i.e. transmission with full available power was always optimal and hence was implemented as an equality constraint. Neither of these are true in the present CR setting: the feasible set $S_{\mathbf{R}}$ is not isotropic anymore, due to the IPC $tr(\mathbf{W}_3\mathbf{R}) \leq P_I$, and the TPC can be inactive due to the IPC (when the latter dominates). Furthermore, it is *not* known in advance which constraint is active or not.

To address these issues, we propose the following iterative algorithm to solve the max-min problem in (4) based on the barrier method combined with the residual form of Newton method and the backtracking line search (see e.g. [17] for more details on these basic algorithms). For numerical implementation, we use real rather than complex variables. Following the barrier method, let us introduce the barrier parameter $t > 0$ to absorb the inequality constraints so that the new objective function $f_t(\mathbf{R}, \mathbf{K})$ becomes

$$f_t(\mathbf{R}, \mathbf{K}) = f(\mathbf{R}, \mathbf{K}) + I_1(\mathbf{R}) + I_2(\mathbf{R}) + I_3(\mathbf{R}) - I_4(\mathbf{K})$$

where

$$I_1(\mathbf{R}) = t^{-1} \ln |\mathbf{R}|, \quad (8)$$

$$I_2(\mathbf{R}) = t^{-1} \ln(P_T - tr(\mathbf{R})), \quad (9)$$

$$I_3(\mathbf{R}) = t^{-1} \ln(P_I - tr(\mathbf{W}_3\mathbf{R})), \quad (10)$$

$$I_4(\mathbf{K}) = t^{-1} \ln |\mathbf{K}|. \quad (11)$$

Thus, the original inequality-constrained max-min problem in (4) is transformed to

$$\max_{\mathbf{R}} \min_{\mathbf{K}} f_t(\mathbf{R}, \mathbf{K}) \quad (12)$$

without any explicit constraints, so that its KKT conditions are simply the stationarity conditions:

$$\nabla_{\mathbf{R}} f_t = \mathbf{0}, \ \nabla_{\mathbf{K}} f_t = \mathbf{0} \quad (13)$$

for a fixed t, which are also sufficient for global optimality since $f_t(\mathbf{R}, \mathbf{K})$ is convex-concave in the right way. Following Proposition 3 in [13], the optimality gap of the barrier method in (12) applied to the minimax problem in (4) can be bounded as follows

$$|f(\mathbf{R}^*(t), \mathbf{K}^*(t)) - C| \leq \max(m, n_1 + n_2)/t \quad (14)$$

where $\{\mathbf{R}^*(t), \mathbf{K}^*(t)\}$ is the optimal point for the modified problem in (12). Hence, the gap can be made as small as desired by selecting sufficiently large t. It is this inequality that makes the barrier method so powerful for inequality-constrained problems.

In the proposed algorithm, we use the residual-form Newton method to compute the optimal point $\{\mathbf{R}^*(t), \mathbf{K}^*(t)\}$ for a fixed t in an iterative way with any desired accuracy. To reduce the number of variables and improve the efficiency, we use $\mathbf{x} = vech(\mathbf{R})$ and $\mathbf{y} = vec(\mathbf{N})$ as independent variables to represent $\mathbf{R}$ and $\mathbf{K}$ (exploiting their symmetry). The corresponding KKT conditions in (13) become

$$\mathbf{r}(\mathbf{z}) = \nabla_{\mathbf{z}} f_t = \mathbf{0} \quad (15)$$

where $\mathbf{z} = [\mathbf{x}', \mathbf{y}']'$ is the aggregate vector of the variables and $\mathbf{r}(\mathbf{z})$ is the residual. In the residual-form Newton method, the optimality condition $\mathbf{r}(\mathbf{z}) = 0$ is iteratively solved using 1st-order approximation of $\mathbf{r}(\mathbf{z})$ at each step (which corresponds to the 2nd order approximation of the objective):

$$\mathbf{r}(\mathbf{z}_k + \Delta\mathbf{z}) = \mathbf{r}(\mathbf{z}_k) + D\mathbf{r}\Delta\mathbf{z} + o(\Delta\mathbf{z}) = 0. \quad (16)$$

where $\mathbf{z}_k$ and $\Delta\mathbf{z}$ are the current variables and their updates respectively at iteration k, and where $D\mathbf{r}$ is the derivative of $\mathbf{r}(\mathbf{z})$, i.e. the Hessian of $f_t(\mathbf{x}, \mathbf{y})$:

$$D\mathbf{r} = \begin{bmatrix} \nabla^2_{\mathbf{xx}} f_t & \nabla^2_{\mathbf{xy}} f_t \\ \nabla^2_{\mathbf{yx}} f_t & \nabla^2_{\mathbf{yy}} f_t \end{bmatrix} = \mathbf{T}. \quad (17)$$

where $\mathbf{T}$ is also the KKT matrix (since there are no explicit constraints). After evaluating the gradients and Hessians, the update $\Delta\mathbf{z}$ can be computed via (16) by ignoring $o(\Delta\mathbf{z})$:

$$\Delta\mathbf{z} : \mathbf{T}\Delta\mathbf{z} = -\mathbf{r}(\mathbf{z}_k). \quad (18)$$

which is a system of linear equations in $\Delta\mathbf{z}$. Note that when KKT matrix $\mathbf{T}$ is non-singular, (18) has a unique solution. In our setting, the non-singularity of $\mathbf{T}$ at each step can be rigorously established following similar steps as in [13] with proper modifications to account for the interference constraint and the fact that the TPC can be inactive (the proof is omitted due to the page limit). Thus, the updates can be expressed as

$$\mathbf{z}_{k+1} = \mathbf{z}_k + s\Delta\mathbf{z} \quad (19)$$

where $s > 0$ is the step size. It is found via the backtracking line search method. The Newton method in combination with the backtracking line search is guaranteed to reduce the residual norm $|\mathbf{r}(\mathbf{z})|$ at each step, which follows from the following norm-reduction property [17]:

$$\frac{d}{ds}|\mathbf{r}(\mathbf{z}_k + s\Delta\mathbf{z})| = -|\mathbf{r}(\mathbf{z}_k)| < 0 \quad (20)$$

so that, for sufficiently small s, the residual norm indeed shrinks at each iteration approaching $\mathbf{r} = 0$ as k increases. After several iterations, the convergence becomes quadratic (see [17] for related definitions and analysis) and hence very fast, so that the optimal point $(\mathbf{R}^*(t), \mathbf{K}^*(t))$ of the problem (12) can be approach with any desired accuracy in a small to moderate number of steps. Following the barrier method, the problem in (12) is solved for sequentially increasing t, where the optimal point of the previous t serves as an initial point for the new, increased t, thus minimizing the total number of Newton iterations required [17]. It follows from (14) that $f(\mathbf{R}^*(t), \mathbf{K}^*(t)) \rightarrow C$ as $t \rightarrow \infty$ so that any desired accuracy can be reached. Convergence to a global optimum can also be rigorously proved (the proof is omitted due to the page limit).

The proposed algorithm can be summarized as shown below, where α is the percentage of the linear decrease in the residual norm one is willing to accept at each step; β and μ are the parameters controlling reduction in step size s and increase in barrier parameter t at each iteration of the algorithm, ϵ is the target residual accuracy, t_0 and t_{max} are initial and maximum values of the barrier parameter; t varies from t_0 to t_{max}; $\mathbf{z}_0 = [\mathbf{x}_0', \mathbf{y}_0']'$ is the initial point defined as follows

$$\mathbf{x}_0 = \mathit{vech}(P_T\mathbf{I}/a), \ \ \mathbf{y}_0 = \mathbf{0} \tag{21}$$

where $a = 2\max(m, \mathit{tr}(\mathbf{W}_3)P_T/P_I)$ so that $\mathbf{R}_0$, $\mathbf{K}_0$ are strictly inside of $S_{\mathbf{R}}$ and $S_{\mathbf{K}}$, as required by the barrier method.

Algorithm 1 (for global maximization of secrecy rates)

```
Require $\mathbf{z}_0$, $0 < \alpha < 0.5$, $0 < \beta < 1$, $t_0 > 0$, $t_{max} > t_0$, $\mu > 1$, $\epsilon > 0$.
1. Set $t = t_0$.
repeat (barrier method)
    2. Set $k = 0$.
    repeat (residual-form Newton method)
        3. Compute $\mathbf{r}(\mathbf{z}_k)$ via (15) for current $k$.
        4. Compute update $\Delta\mathbf{z}$ via (18).
        5. Set $s = 1$.
        repeat (backtracking line search)
            6. $s := \beta s$.
            7. Update $\mathbf{z}_{k+1} = \mathbf{z}_k + s\Delta\mathbf{z}$;
        until $|\mathbf{r}(\mathbf{z}_{k+1})| \leqslant (1-\alpha s)|\mathbf{r}(\mathbf{z}_k)|$ and $\mathbf{R}_{k+1} \in S_{\mathbf{R}}, \mathbf{K}_{k+1} \in S_{\mathbf{K}}$
        8. $k := k + 1$.
    until $|\mathbf{r}(\mathbf{z}_k)| \leqslant \epsilon$
    9. Evaluate $f(\mathbf{R}_k, \mathbf{K}_k)$, $C(\mathbf{R}_k)$.
    10. Set $\mathbf{z}_0 := \mathbf{z}_k$ as a new starting point.
    11. Update $t := \mu t$.
until $t > \mu t_{max}$
```

V. Numerical examples

In this section, we present some numerical examples to illustrate the performance of the proposed algorithm. Channel matrices $\mathbf{H}_1$, $\mathbf{H}_2$ and $\mathbf{H}_3$ are selected as follows:

$$\begin{bmatrix} 0.17 & -0.81 \\ -1.01 & -0.50 \end{bmatrix}, \begin{bmatrix} -0.71 & -1.16 \\ 0.79 & 0.41 \end{bmatrix}, \begin{bmatrix} 1.16 & -0.15 \\ 0.47 & -0.27 \end{bmatrix} \tag{22}$$

so that the corresponding eigenvalues of $\mathbf{W}_1 - \mathbf{W}_2$ are $(0.48, -1.15)$, i.e. the channel is non-degraded and ”hard” for optimization (since the negative eigenmode is dominant).

Fig. 1 illustrates the convergence of the proposed algorithm for the channel in (22), i.e. the residual's Euclidian norm $|\mathbf{r}|$ versus the number of Newton steps for several values of fixed t. Note that, for all considered values of t, it takes only about 10 to 20 Newton steps to reach the machine precision level. Also note the presence of two convergence phases: linear and quadratic. After the quadratic (”water-fall”) phase is reached, the convergence is very fast.

Fig. 2 shows the achieved secrecy rate $C(\mathbf{R})$ and the upper bound $f(\mathbf{R}, \mathbf{K})$. Note that, while they converge as the algorithm converges, the behaviour of $C(\mathbf{R})$ is significantly non-monotonic and sensitive to $\mathbf{R}$, while the upper bound is less sensitive and converges faster. While $t = 10^3$ is sufficient to evaluate accurately the capacity via the upper bound, it takes $t = 10^5$ to get the same accuracy via $C(\mathbf{R})$ so we conclude that, in addition to being convex-concave in the right way, $f(\mathbf{R}, \mathbf{K})$ is more robust (less sensitive) than $C(\mathbf{R})$. For properly selected t, it takes 10 to 15 Newton steps for the algorithm to converge in terms of achieved secrecy rates.

To further validate the algorithm, its results were compared to those of Monte-Carlo (MC) search, where a large number (10^5) of covariance matrices $\mathbf{R}$ are randomly generated within the feasible set and the best one is selected. No significant difference between these 2 methods was observed while comparing the best achieved secrecy rates.

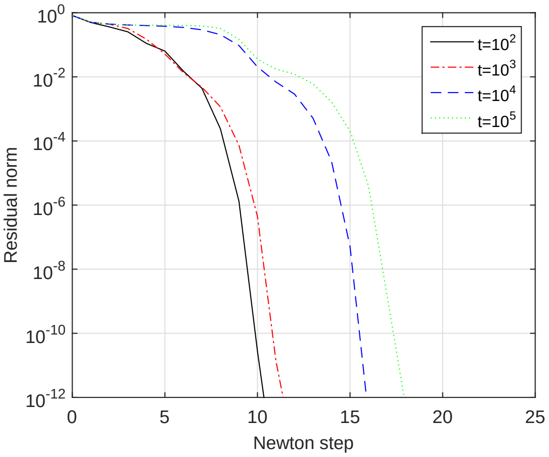

Fig. 1. Convergence of the Newton method for different values of t; $P_T = 5$ dB, $P_I = 2$ dB, $\alpha = 0.3, \beta = 0.5$, $\mathbf{H}_1 - \mathbf{H}_3$ as in (22).

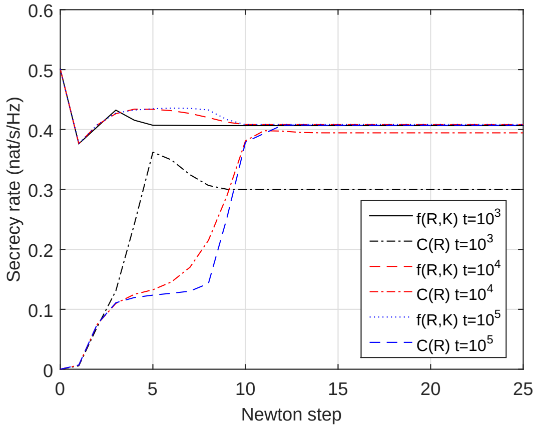

Fig. 2. Secrecy rates and upper bound for the same setting as in Fig. 1.

REFERENCES

[1] S. Haykin *et al* (Eds.), Cognitive Radio, Part 1: Practical Perspectives, and Part 2: Fundamental Issues, Proceedings of the IEEE, v. 97, n. 4 and 5, Apr. and May 2009.

[2] G. Scutari, D. P. Palomar, and S. Barbarossa, "*Cognitive MIMO Radio,*" IEEE Signal Processing Mag., vol. 25, no. 6, pp. 46-59, Nov. 2008.

[3] R. Zhang and Y.-C. Liang, "*Exploiting Multi-Antennas for Opportunistic Spectrum Sharing in Cognitive Radio Networks,*" IEEE J. Select. Topics Signal Processing, vol. 2, no. 1, pp. 88-102, Feb. 2008.

[4] M. Bloch and J. Barros, "*Physical-Layer Security: From Information Theory to Security Engineering,*" Cambridge University Press, 2011.

[5] P. A. Regalia et al (Eds.), Secure Communications via Physical-Layer and Information-Theoretic Techniques, Proceedings of the IEEE, vol.103, no.10, Oct. 2015.

[6] A. Khisti and G. W. Wornell, "*Secure Transmission With Multiple Antennas−Part II: The MIMOME Wiretap Channel,*" IEEE Trans. Info. Theory., vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[7] F. Oggier, B. Hassibi, The Secrecy Capacity of the MIMO Wiretap Channel, IEEE Trans. Info. Theory, v. 57, no. 8, Aug. 2011.

[8] S. Loyka, C.D. Charalambous, "*Rank-Deficient Solutions for Optimal Signaling over Wiretap MIMO Channels,*" IEEE Trans. Comm., vol. 64, no. 6, pp. 2400-2411, June 2016.

[9] S. Loyka, C.D. Charalambous, "*Optimal Signaling for Secure Communications Over Gaussian MIMO Wiretap Channels,*" IEEE Trans. Info. Theory, vol. 62, no. 12, pp. 7207-7215, Dec. 2016.

[10] Q. Li et al, Transmit Solutions for MIMO Wiretap Channels Using Alternating Optimization, IEEE JSAC, v. 31, no. 9, pp. 1714–1727, Sep. 2013.

[11] J. Steinwandt et al, Secrecy Rate Maximization for MIMO Gaussian Wiretap Channels With Multiple Eavesdroppers via Alternating Matrix POTDC, IEEE ICASSP, May 4-9, 2014, Florence, Italy, pp. 5686-5690.

[12] K. Cumanan *et al.*, "*Secrecy Rate Optimizations for a MIMO Secrecy Channel with a Multiple-Antenna Eavesdropper,*" IEEE Trans. Veh. Technol., vol. 63, no. 4, pp. 1678-1690, May. 2014.

[13] S. Loyka, C. D. Charalambous, "*An Algorithm for Global Maximization of Secrecy Rates in Gaussian MIMO Wiretap Channels,*" IEEE Trans. Commun., vol. 63, no. 6, pp. 2288-2299, June. 2015.

[14] L. Zhang *et al.*, "*On The Relationship Between The Multi-Antenna Secrecy Communications and Cognitive Radio Communications,*" IEEE Trans. Commun., vol. 58, no. 6, pp. 1877-1886, Jun. 2010.

[15] Y. Pei *et al.*, Y.-C. Liang, L. Zhang, K. C. Teh, "*Secure Communication Over MISO Cognitive Radio Channels,*" IEEE Trans. Wireless Commun., vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[16] L. Dong, S. Loyka and Y. Li, "*The Operational Secrecy Capacity of Cognitive Radio MIMO Channel,*" 15th Canadian Workshop on Information Theory, Quebec City, Canada, June 2017.

[17] S. Boyd and L. Vandenberghe, "*Convex Optimization,*" Cambridge University Press, 2004.