Robust Secrecy Rate Optimizations for Healthy Monitoring System MISO Channel with D2D Communications

Xuemeng Jia¹, Mingjun Pei¹, Rong Fu¹ and Zhanwei Jiao²,*

¹ State Grid Henan Electric Power Company Xinan Power Supply Company
² Zhengzhou University

*Email: 11892646@qq.com

Abstract. In this paper, we study the robust secrecy rate optimization of multiple-input-single-output (MISO) security channels with multiple device-to-device (D2D) communication in an electronic physical system for health monitoring applications. We focus on the problems of robust power minimization and maximizing robust secrecy with transmit power in this system. Both of these robust optimizations are subject to probability-based secrecy and D2D transmission rates. The design of robust beamforming can consider combining statistical channel uncertainty model (CUM), but the problem of construction is a non-convexity problem that is not easy to solve, so we propose two methods to solve this problem: based on Bernstein-type inequality and a conservative approximation of S-Procedure. The simulation results demonstrate that the performance of the S-Procedure method on the reachable confidentiality rate is not as good as the method based on the Bernstein-type inequality.

1. Introduction
With the gradual improvement of the fifth generation (5G) wireless communication network architecture, people have begun to integrate modern medical and information technology [1]. Establishing a medical and health supervision system with the help of wireless communication networks can effectively control the damage caused by sudden illness to some patients. In a complete medical and health supervision system, patients do not have to exchange information with remote network medical platforms, but can use device-to-device (D2D) communication to achieve health supervision at anytime and anywhere [2]. Some pharmacies and clinics can place comprehensive diagnostic equipment that can communicate to receive and process distress signals from patients with sudden illnesses nearby who wear them.

The advantage of D2D communication is that it can effectively improve spectrum utilization [3]. This is mainly because the user (UE) in the communication network can be regarded as a low-power micro base station. D2D communication can directly exchange signals without using cellular resources. Base station. However, due to the interference between different links in the communication process, the realization of D2D communication is also subject to certain constraints [4]. For the communication between cellular and D2D, some interference cancellation schemes have been proposed [5]-[7].

In the development of wireless communication information theory, some people have carried out research on physical layer security [8]-[10]. Thanks to multiple antennas, more secure communications with diversity gain and eavesdropping channels have become a research hotspot [11]. The perfect channel state information (CSI) cannot always be obtained at the transmitter and receiver...
because of the channel estimation and quantization errors. If the eavesdropper's CSI cannot be obtained at the transmitter, the optimization of the privacy rate is more difficult to solve. Because the use of robust technology can introduce channel uncertainty into the system, this effectively avoids the problem of imperfect CSI [12]-[14]. In this paper, for the issue of MISO confidential channel, we consider that under the premise of eavesdroppers and D2D nodes, the sender can still establish good communication with legitimate users. D2D nodes can interfere with eavesdroppers on the one hand, and can also reach the reachable rate. The main contributions of this article can be summarized as follows.

1) We first construct a robust power minimization problem constrained by the secrecy rate and the D2D transmission rate, where both of them are probability constraints; the second problem is robust secrecy rate maximization problem which is constrained by transmit power and the above two probability constraints;

2) To get the form of an easy-to-solve optimization problems, then we introduce two approximation methods which are based on Bernstein-type inequality and S-Procedure to release the constraints;

3) By using binary search on $R_i$, to get the solution to the problem of maximizing the confidentiality rate, this can be determined by solving the power minimization problem.

The rest of the paper is organized as follows. Section II describes the system model. Section III proposes the secrecy rate optimization problems which can be solved by the conservative. Section V summarizes this work.

2. SYSTEM MODEL

In healthy monitoring system of this paper, a MISO eavesdropping channel with $K$ eavesdroppers is considered, in which legitimate senders and users can establish secure communication transmission under this condition, and only the information of legitimate users will be intercepted by eavesdroppers.

The system also includes legal transmitters and eavesdroppers equipped with $N_f$ transmitting antenna legal transmitters and only a single receiving antenna. The legal user's reachable privacy rate and D2D node rate can be donated as:

\[
R_{u,i} = \max_{\beta, \alpha} \left\{ \log(1 + \frac{|h_i^u w|^2}{\sum_{j=1}^{M} p_j \beta_{ij} + \sigma_u^2}), \right. i \in \{1,\ldots,M\} \right\},
\]

\[
R_j = \log(1 + \frac{p_j h_j |w_j|^2}{|h_j w|^2 + \sigma_j^2}), \right. j \in \{1,\ldots,J\} \right\},
\]

where $h_i \in \mathbb{C}^{N_r \times 1}$, $h_j \in \mathbb{C}^{N_r \times 1}$ and $h_j \in \mathbb{C}^{N_r \times 1}$ are the channel coefficients between the legitimate transmitter and the legitimate receiver, the $k$ -th eavesdropper, $i$ -th D2D receiver, respectively, and $w$ is the beamforming vector of the legitimate transmitter. The $\beta_{ij}$, $\beta_{ij}$ and $\beta_{ij}$ donate the channel gains between the $i$ -th D2D transmitter and the legitimate receiver, $k$ -th eavesdropper, the corresponding D2D receive. $\sigma_j^2$ are the noise variance of receivers. The robust privacy rate optimization problems with probabilistic which is based on secrecy rate constraint can be expressed as

\[
\min \|w\|^2
\]

s.t. \( \Pr\{R_{u,i} \geq R_i\} \geq 1 - \alpha, i \in \{1,\ldots,M\} \), \( \Pr\{\log(1 + \frac{p_j h_j |w_j|^2}{|h_j w|^2 + 1}) \geq R_j\} \geq 1 - \beta, i \in \{1,\ldots,M\} \).

\[1518\ (2020) 012079\] doi:10.1088/1742-6596/1518/1/012079
\[
\max_w R_u \quad \text{s.t.} \quad \Pr\{R_u \geq R_j \geq 1-\alpha, i \in \{1,\ldots,M\}\}, \quad \Pr\{\log(1 + \frac{p_j h_j}{|\mathbf{h}, w|^2 + 1}) \geq R_j \geq 1-\beta, i \in \{1,\ldots,M\}\}, \quad \|w\|^2 \leq P, \tag{4}
\]

where \(\alpha, \beta \in (0,1)\) is the interruption probability of the rate constraint of the legitimate user and D2D nodes. (3) and (4) are difficult to be easily solved due to their nonconvexity. In (3), if \(R_j\) is to be achieved, the transmitter needs a lot of power to achieve this goal, but its maximum transmission power is controlled to a certain extent, which cannot be infinitely large. At the same time, the channel between transmitters cannot guarantee to achieve this goal. Therefore, this power minimization problem cannot be solved smoothly. In order to overcome the above problems, we consider (4) to maximize the rate of interrupt secrecy. We can get the optimal solution of the problem in (4) by solving different \(u_R\) in (3) and based on the bisection search on \(R_j\). In this section, we only consider the case of fixed parameters, but not to combine with channel uncertainty model (CUM). Next, we will focus on this aspect.

### 3. Robust Secrecy Rate Optimization Based on Statistical CUM

Then we introduce channel uncertainty models to solve the problem of power minimization and security rate maximization by combining these models.

It is essentially a partial channel uncertainty model, where eavesdroppers on legitimate transmitters have imperfect CSI. The causes of imperfect CSI may be estimation errors, quantization errors, and so on. The channel combined with CUM can be expressed as:

\[
\mathbf{h}_{ei} = \hat{\mathbf{h}}_{ei} + \mathbf{e}_{ei}, \quad i = \{1,\ldots,M\}, \quad \mathbf{h}_{ej} = \hat{\mathbf{h}}_{ej} + \mathbf{e}_{ej}, \quad j = \{1,\ldots,J\}, \tag{5}
\]

where \(\hat{\mathbf{h}}_{ei} \in \mathbb{C}^{N_r \times 1}\) and \(\hat{\mathbf{h}}_{ej} \in \mathbb{C}^{N_r \times 1}\) are the estimated CSI of \(k\)-th eavesdropper and \(m\)-th D2D nodes, and \(\mathbf{e}_{ei}\) and \(\mathbf{e}_{ej}\) are the corresponding statistical errors with zero mean and the corresponding error covariance matrices and \(\mathbf{e}_{ei} = \mathbb{E}[\mathbf{Z}_{ei}^H], \text{where } \mathbf{Z}_{ei} \sim \mathcal{CN}(0, I)\).

If we let \(\mathbf{G}_{ei} = \mathbb{E}[\mathbf{w}_R^H]\), the outage secrecy rate constraint in (1) can be expressed as

\[
\Pr\{\mathbf{Z}_u^H \mathbf{G}_{ei}^H \mathbf{E}_{ei}^2 \mathbf{Z}_u + 2R(\mathbf{Z}_u^H \mathbf{G}_{ei}^H \mathbf{G}_u \mathbf{h}_e) + \mathbf{h}_e^H \mathbf{G}_u \mathbf{h}_e - 2^{-R} \vartheta^*(\vartheta^* \mathbf{h}_u^H \mathbf{G}_u \mathbf{h}_u + 1) - \vartheta^* \leq 0\} \geq 1 - \alpha. \tag{6}
\]

where \(\vartheta = \sum_{j=1}^{J} p_j \vartheta_{w,j} + \vartheta_u^2\) and \(\vartheta^* = \sum_{j=1}^{J} p_j \vartheta_{g,j} + \vartheta_e^2\). By employing Lemma in [15-17], (6) can be reformulated as

\[
\begin{align*}
\left\| \begin{bmatrix} \mathbf{E}_{ei}^H \mathbf{G}_u \mathbf{E}_{ei}^2 & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{bmatrix} \right\|^2_2 &\leq u_i, \quad s_1 - \mathbf{E}_{ei}^H \mathbf{G}_u \mathbf{E}_{ei}^2 \mathbf{g}_i \geq 0, \quad s_i \geq 0, \quad i = \{1,\ldots,M\}, \tag{7}
\end{align*}
\]

\[
\begin{align*}
&\text{Tr}(\mathbf{E}_{ei}^H \mathbf{G}_u \mathbf{E}_{ei}^2) + [2 \ln(\eta)]^{\mathbf{1}} u_i - \ln(\eta) s_i - \vartheta^* \vartheta^{-1} 2^{-R} \mathbf{h}_u^H \mathbf{G}_u \mathbf{h}_u - \vartheta^* (2^{-R} - 1) + \hat{\mathbf{h}}_e^H \mathbf{G}_u \mathbf{h}_e \leq 0, \\
\end{align*}
\]

and the transmission rate constraint can be donated as
\[
\begin{align*}
\left\| \vec{(E_j^2 G_u E_j^2)} \right\|_2 & \leq u_i, \quad s \in E_j G_u E_j^2 \geq 0, s \geq 0, j = \{1, \ldots, J\}, \\
\sqrt{2E_j^2 G_u h_j} & \end{align*}
\]

\[
\text{Tr}(E_j^2 G_u E_j^2) + [-2 \ln(\beta)]^\frac{1}{2} u_j - \ln(\beta) s_j - [p_j h_j (2^R - 1)^{-1} - \hat{h}_j H G_u \hat{h}_j] \leq 0.
\]

So the power minimization problem can be formulated as
\[
\min_{a_u} \text{Tr}(G_u), \quad \text{s.t.} (7), (8), \text{rank}(G_u) = 1.
\]

The non-convex rank 1 constraint keeps the above problem non-convex. But rank relaxation can help us solve two problems, and rank-1 solutions can be obtained by random techniques. We can also use S-Procedure in [18] to rewrite the secrecy rate constraint as
\[
v_i^H X_i v_i + 2\Re\{v_i^H W_i\} + q_i \geq 0,
\]

where \( X_i = -E_i^2 G_u E_i^2 \), \( W_i = -E_i^2 G_u \hat{h}_i \), \( q_i = 2^{-R} g^* g^{-1} h_i^H G_u h_i - h_i^H G_u \hat{h}_i + g'(2^R - 1) \)
\[\Omega = \{v_i : \Pr(v_i^H v_i \leq \chi^2_{\alpha_i}) \geq 1 - \alpha\} \quad \chi^2_{\alpha_i} \]

The covariance matrix of \( \Omega \) is \( I_{N_r} \), and the degree of freedom of \( \|v_i\|^2 \) is \( 2N_f \) which is a Chi-square random variable. If we let \( P^{-1}(x) \) donate the inverse cumulative distribution function of Chi-square random variable, then we have \( \chi^2_{\alpha_i} = (2P)^{-1}(1 - \alpha) \), and (10) can be reformulated as
\[
v_i^H X_i v_i + 2\Re\{v_i^H W_i\} + q_i \geq 0, \quad v_i^H v_i \leq \chi^2_{\alpha_i}.
\]

We can eliminated \( v_i \) by S-Procedure, and this constraint can be re-formulated as
\[
\begin{bmatrix}
X_i + \frac{\lambda_i}{2} I & W_i \\
W_i^H & q_i - \frac{\lambda_i}{2} \chi^2_{\alpha_i}
\end{bmatrix} \succeq 0, \lambda_i \geq 0.
\]

where \( X_i = X_i^H \in \mathbb{F}^{m \times m} \). Similar to the expression above, it can be further written as
\[
\Pr(v_i^H X_i v_i + 2\Re\{v_i^H W_i\} + q_i \geq 0) \geq 1 - \beta
\]

where \( X_i = -E_i^2 G_u E_i^2 \), \( q_i = p_i h_i (2^R - 1)^{-1} - \hat{h}_i^H G_u \hat{h}_i \), \( \Phi = \{v_i : \Pr(v_i^H v_i \leq \chi^2_{\alpha_i}) \geq 1 - \beta\} \), \( W_i = -E_i^2 G_u \hat{h}_i \), and both \( \|v_i\|^2 \) and \( \|v_i\|^2 \) have the same properties. So the transmission rate constraint can be translated into the linear matrix inequality as
\[
\begin{bmatrix}
X_j + \frac{\zeta_j}{2} I & W_j \\
W_j^H & q_j - \frac{\zeta_j}{2} \chi^2_{\alpha_j}
\end{bmatrix} \succeq 0, \zeta_j \geq 0.
\]

so the power minimization problem can be formulated as
\[
\min_{a_u} \text{Tr}(G_u), \quad \text{s.t.} \quad \text{rank}(G_u) = 1, \begin{bmatrix}
X_j + \frac{\lambda_j}{2} I & W_j \\
W_j^H & q_j - \frac{\lambda_j}{2} \chi^2_{\alpha_j}
\end{bmatrix} \succeq 0, \lambda_j \geq 0.
\]

The above optimization problem is easy to solve, and the final solution is obtained by the interior point method. But due to the influence of rank relaxation, the solution cannot be rank-1. When \( G_u \) is a...
rank-1 matrix, the method of eigenvalue decomposition can be used to obtain the final solution. If $G_a$ is not a rank-1 matrix, it needs to use randomization technology to solve it.

4. Simulation Results
In this simulation, we assume that there is a legitimate user, $N_1=3$ eavesdroppers and $N_2=5$ D2D nodes in secrecy network of healthy monitoring system. Legal transmitters are equipped with $N_T=5$ antennas, while all other nodes are composed of one antenna. The outage probability of secrecy rate is $\alpha = 0.05$ and the target D2D transmission rate is $R = 5$.

When the CUM is considered, the perfect CSI of the transmitter only can be obtained by the legitimate user, neither the eavesdropper nor the D2D nodes can obtain the perfect CSI. If $\zeta_i$ and $\zeta_j$ denote the error variance of the $i$-th eavesdropper and the $j$-th D2D receiver, respectively, then $E_i = \zeta_i I$ and $E_j = \zeta_j I$ can represent the error covariance matrix of the channels which are assumed Rayleigh fading channels. Considering that the channel error variances of the eavesdropper and the D2D pairs are 0.01 and 0.04, respectively. Figure 1 shows the transmission power required in the power minimization problem under this condition and different target secrecy rates. It can be seen from the results that with the increase of the target secrecy rate, the transmission power increases obviously. Compared with Bernstein-type inequality and S-Procedure program, the difference between them increases with the increase of target speed, and the former consumes less power. Figure 2 shows the secret rate of different transmit power of the two methods, and the method based on S-Procedure program is not as good as that based on Bernstein-type inequality.

![Figure 1. Transmit power with different target secrecy rates.](image1)

![Figure 2. Secrecy rates with different transmit powers.](image2)

5. Conclusion
In this paper, security rate optimization problems are studied for the MISO secure channel of multiple D2D communication in healthy monitoring system. By combining statistical CUMs, the problem of robust power minimization based on probability and D2D transmission rate constraints, and the problem of robust security rate maximization based on transmission power, probability and D2D transmission rate constraints are solved. Two approximate methods based on Bernstein-type inequality and S-Procedure program are introduced to transform the constraints from probability to certainty, and to transform robust beamforming design into a convex optimization problem which is easy to solve. Compared with the simulation results of Bernstein-type inequality and S-Procedure program, the former is better than the latter.
References

[1] G. Loubet, A. Takacs and D. Dragomirescu, “Implementation of a Battery-Free Wireless Sensor for Cyber-Physical Systems Dedicated to Structural Health Monitoring Applications,” in IEEE Access, vol. 7, pp. 24679-24690, 2019.

[2] W. H. Chin, Z. Fan, and R. J. Haines, “Emerging technologies and research challenges for 5G wireless networks,” arXiv preprint arXiv:1402.6474, 2014.

[3] L. Song, Z. Han, and C. Xu, Resource Management for Device-To-Device Underlay Communication. Springerbriefs in Computer Science, Springer-Verlag New York Incorporated, 2013.

[4] L. Wang, T. Peng, Y. Yang, and W. Wang, “Interference constrained D2D communication with relay underlaying cellular networks,” in Proc. IEEE VTC, Fall, pp. 1–5, Sept. 2013.

[5] H. Min, W. Seo, J. Lee, S. Park, and D. Hong, “Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks,” IEEE Trans. Wireless Commun., vol. 10, pp. 413–418, Feb. 2011.

[6] H. Min, J. Lee, S. Park, and D. Hong, “Capacity enhancement using an interference limited area for device-to-device uplink cellular networks,” IEEE Trans. Wireless Commun., vol. 10, pp. 3995–4000, Dec. 2011.

[7] H. Wang and X. Chu, “Distance-constrained resource-sharing criteria for device-to-device communications underlaying cellular networks,” Electronics Lett., vol. 48, pp. 528–530, Apr. 2012.

[8] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, “Interference assisted secret communication,” IEEE Trans. Inf. Theory, vol. 57, no. 5.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[10] Y. Liang, H. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[11] L. Zhang, R. Zhang, Y. C. Liang, Y. Xin, and S. Cui, “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.

[12] K. Cumanan, R. Krishna, V. Sharma, and S. Lambotharan, “Robust interference control techniques for multi-user cognitive radios using worst-case performance optimization,” in Proc. Asilomar Conf. Sign., Syst. and Comp., Pacific Grove, CA, pp. 378–382, Oct. 2008.

[13] K. Cumanan, R. Krishna, V. Sharma, and S. Lambotharan, “A robust beamforming based interference control technique and its performance for cognitive radios,” in Proc. Int. Symp. Commun. and Inform. Techno. (ISCIT) 2008, pp. 9–13, Oct. 2008.

[14] K. Cumanan, R. Krishna, V. Sharma, and S. Lambotharan, “Robust interference control techniques for cognitive radios using worst-case performance optimization,” in Proc. ISITA 2008, Auckland, New Zealand, pp. 1–5, Dec. 2008.

[15] I. Bechar, “A Bernstein-type inequality for stochastic processes of quadratic forms of Gaussian variables,” Available[online]: http://arxiv.org/abs/0909.3595., 2009.

[16] K.Y. Wang, A. M.C. 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,” arXiv preprint arXiv:1108.0982, 2011.

[17] Q. Li, W.-K. Ma, and A.-C. So, “A safe approximation approach to secrecy outage design for MIMO wiretap channels,” IEEE, Signal Processing Lett., vol. 21, pp. 118–121, Jan 2014.

[18] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, Linear Matrix Inequalities in System and Control Theory. Philadelphia PA: SIAM Studies in Applied Mathematics, 1994.