# Joint optimisation of secret key capacity and sparse channel estimation based on pilot power allocation

Chenhao Qi✉, Arumugam Nallanathan and Lenan Wu

Pilot power allocation is investigated under the framework of physical layer secure communications in time-division duplex systems, where the secret keys are generated from the estimates of sparse wireless channels. The joint optimisation of secret key capacity and sparse channel estimation performance based on pilot power allocation is formulated as a convex optimisation problem. Considering the fairness between these two sides, a scaling factor is introduced. Then, a scheme is proposed to fast solve the problem by looking up a table and using existing optimisation solvers. Simulation results show that a proper scaling factor can make a trade-off between the secret key capacity and sparse channel estimation performance.

*Introduction:* The broadcast property of wireless communications makes it susceptible to various security threats, e.g. eavesdropping, modification and deception. To strengthen the security of wireless networks, traditional methods are based on the public key cryptography [1]. In contrast to this paradigm, physical layer security techniques generate secret keys by exploiting the inherent randomness of wireless channels, leading to much lower complexity than traditional methods [2]. The channel phase, channel magnitude and multipath delay spread are used to extract secret keys based on the uplink–downlink channel reciprocity of time-division duplex (TDD) systems. Recently, with the successful application of compressed sensing (CS) to channel estimation, it has been demonstrated that the sparse channel estimation can improve the channel estimation performance and reduce the pilot overhead compared with the traditional least squares methods [3]. Therefore, it is natural to adopt sparse channel estimation for secret key generation. In [4], ergodic capacity and secrecy outage are investigated with the secret key generated from a sparse wireless channel and it is shown that a higher ergodic secret key rate can be achieved in a sparser channel. However, to the authors' best knowledge, so far there has been no work studying the pilot power allocation for secret key generation using sparse channel estimation.

In this Letter, we jointly optimise the secret key capacity and sparse channel estimation performance. We first study the pilot power allocation under the framework of physical layer secure communications where the secret keys are generated from the estimates of sparse wireless channels. Then, we formulate the pilot power allocation with respect to both the secret key capacity and the sparse channel estimation performance as a convex optimisation problem. Considering the fairness between these two sides, a scaling factor is introduced. After that, a scheme is proposed to fast solve the problem by looking up a table and using existing optimisation solvers.

*System model:* As shown in Fig. 1, Alice and Bob can transmit and receive information over the wireless channels with the presence of an eavesdropper Eve. Eve listens to the transmission of Alice and Bob, but does not send signals to interfere with the legitimate transmission which means that Eve is passive. We denote the impulse response of wireless channels from Alice to Bob and from Bob to Alice as $\boldsymbol{h}_{\mathrm{AB}}$ and $\boldsymbol{h}_{\mathrm{BA}}$, respectively. Suppose both Alice and Bob are equipped with a single antenna and the communication between Alice and Bob works in TDD mode, which indicates that $\boldsymbol{h}_{\mathrm{AB}} = \boldsymbol{h}_{\mathrm{BA}}$. In this way, Alice and Bob can share a common stochastic randomness to extract secret keys after individual channel estimation. We denote the impulse response of wireless channels from Alice to Eve and from Bob to Eve as $\boldsymbol{h}_{\mathrm{AE}}$ and $\boldsymbol{h}_{\mathrm{BE}}$, respectively. It is shown that if the distance between Alice (Bob) and Eve is larger than $\lambda/2$, $\boldsymbol{h}_{\mathrm{AB}}(\boldsymbol{h}_{\mathrm{BA}})$ and $\boldsymbol{h}_{\mathrm{AE}}(\boldsymbol{h}_{\mathrm{BE}})$ will be statistically independent, where $\lambda$ is the wavelength used for communications [5]. For example, in a GSM band working at 1800 MHz, if the distance between Alice and Eve is larger than 16.7 cm, $\boldsymbol{h}_{\mathrm{AB}}$ and $\boldsymbol{h}_{\mathrm{AE}}$ will be independent, which implies that Eve cannot generate the same key as Alice and Bob.

*Pilot power allocation:* Suppose Alice and Bob communicate to each other using an OFDM system with $N$ subcarriers, where $K(K \leq N)$ subcarriers are used to transmit pilot symbols for frequency-domain pilot-assisted channel estimation. We denote the power of each pilot subcarrier as $c_1, c_2, \ldots, c_K$. Regarding the linear region between cutoff and saturation of the power amplifier, we have $C_L \leq c_i \leq C_H$, $i = 1, 2, \ldots, K$, which also indicates the minimum power requirement $C_L$ for pilot detection and the maximum power limitation $C_H$ considering the peak-to-average power ratio. According to Corollary 1 of [6], the secret key capacity in the high signal-to-noise ratio (SNR) regime is $I(\gamma) = \log_2(1+\gamma/2)$, where $\gamma \triangleq (1/K\sigma^2)\sum_{i=1}^{K} c_i$ is defined to be the average SNR of pilot subcarriers, with $\sigma^2$ representing the noise variance. To maximise $I(\gamma)$, which can be formulated as

$$\begin{aligned} \max_{\{c_1,c_2,\ldots,c_K\}} \quad & \log_2\left(1+\frac{1}{2K\sigma^2}\sum_{i=1}^{K} c_i\right) \\ \text{s.t.} \quad & C_L \leq c_i \leq C_H, \quad i = 1, 2, \ldots, K \end{aligned} \tag{1}$$

the pilot power tends to be $c_1 = c_2 = \ldots = c_K = C_H$. However, such a strategy of pilot power allocation cannot guarantee the optimal performance of sparse channel estimation.

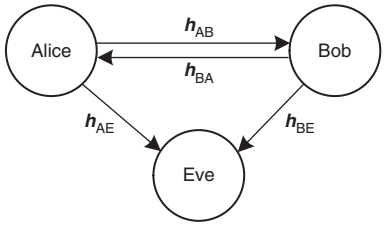


**Fig. 1** *Wireless communication system including two legitimate users Alice and Bob and eavesdropper Eve*

Since the design of the pilot pattern for sparse channel estimation has already been discussed in the existing literature [7, 8], in this Letter we focus on the pilot power allocation given a pilot pattern $\boldsymbol{p} \triangleq \{p_1, p_2, \ldots, p_K\}$. If we want to jointly optimise the pilot pattern and the pilot power, we may use a two-loop iterative algorithm. In the inner-loop iterations, given a pilot pattern, we obtain an optimal pilot power vector based on convex optimisation. Moreover, in the outer-loop iterations, we iteratively search for an optimal or near-optimal pilot pattern via discrete optimisation [9].

Without loss of generality, we assume $1 \leq p_1 < p_2 < \cdots < p_K \leq N$. The transmit pilot symbols and the receive pilot symbols are denoted as $\boldsymbol{x} \triangleq [x(p_1), x(p_2), \ldots, x(p_K)]^{\mathrm{T}}$ and $\boldsymbol{y} \triangleq [y(p_1), y(p_2), \ldots, y(p_K)]^{\mathrm{T}}$, respectively. Then, the relation between the transmit pilots and the receive pilots can be written in matrix notation as $\boldsymbol{y} = \boldsymbol{X}\boldsymbol{F}\boldsymbol{h} + \boldsymbol{\eta}$, where $\boldsymbol{X} \triangleq \mathrm{diag}\{x(p_1), x(p_2), \ldots, x(p_K)\}$ is a diagonal matrix with the diagonal entries to be the transmit pilot symbols, $\boldsymbol{\eta} \triangleq [\eta(1), \eta(2), \ldots, \eta(K)]^{\mathrm{T}} \sim \mathcal{CN}(\boldsymbol{0}, \sigma^2\boldsymbol{I}_K)$ is an additive white Gaussian noise term where $\boldsymbol{I}_K$ denotes the identity matrix with the dimension of $K$, $\boldsymbol{h} \triangleq [h(1), h(2), \ldots, h(L)]^{\mathrm{T}}$ is the channel impulse response with the channel length to be $L$ ($\boldsymbol{h}$ can be either $\boldsymbol{h}_{\mathrm{AB}}$ or $\boldsymbol{h}_{\mathrm{BA}}$), and $\boldsymbol{F}$ is a DFT submatrix with the entry at the $m$th row and $n$th column ($1 \leq m \leq K$, $1 \leq n \leq L$) given by $F_{m,n} = \omega^{p_m(n-1)}$, where $\omega = \mathrm{e}^{-\mathrm{j}2\pi/N}$. We further denote $\boldsymbol{A} \triangleq \boldsymbol{X}\boldsymbol{F}$, since $\boldsymbol{A}$ is usually referred to as the measurement matrix in the CS literature. Then, we have $\boldsymbol{y} = \boldsymbol{A}\boldsymbol{h} + \boldsymbol{\eta}$.

**Table 1:** Comparisons of coherence and secret key capacity

| $\alpha$ | Coherence | Secret key capacity (bits per subcarrier) |
|---|---|---|
| 0 | 46.3 | 2.6 |
| 0.3 | 42.2 | 2.5 |
| 0.5 | 41.7 | 2.4 |
| 0.7 | 41.4 | 2.3 |
| 1 | 41.3 | 1.8 |

It has been shown in many existing works that the wireless channel is typically sparse [3]. The number of non-zero entries in $\boldsymbol{h}$, denoted as $S$, is much smaller than the channel length $L(S \ll L)$. By exploring the sparse property of wireless channels, we introduce the sparse channel estimation to reduce the pilot overhead. Sparse recovery algorithms such as the orthogonal matching pursuit can be applied to estimate $\boldsymbol{h}$. To further improve the performance of sparse channel estimation, we have already proposed a tree-based backward pilot generation scheme

for sparse channel estimation with the objective to minimise the 'coherence' of $\boldsymbol{A}$ [7], since smaller coherence of $\boldsymbol{A}$ leads to better performance of sparse recovery [10]. In this Letter, we further consider the pilot power allocation.

Given a pilot pattern $\boldsymbol{p}$ and a pilot power vector $\boldsymbol{c} \triangleq \{c_1, c_2, \ldots, c_K\}$, we define the coherence of $\boldsymbol{A}$ as the maximum absolute correlation between any two different columns of $\boldsymbol{A}$, i.e. $g_p(\boldsymbol{c}) \triangleq \max_{0\le m<n\le L-1}|\langle A(m), A(n)\rangle|$, where $\langle A(m), A(n)\rangle$ denotes the inner product of $A(m)$ and $A(n)$, i.e. $\langle A(m), A(n)\rangle = A^{\mathrm{H}}(m)A(n)$. Let $d \triangleq n-m$ and $\Lambda \triangleq \{1, 2, \ldots, L-1\}$. Then we have $g_p(\boldsymbol{c}) = \max_{d\in\Lambda}|\sum_{i=1}^{K} c_i \omega^{p_i d}|$. According to [7], the objective for the pilot design is to minimise the coherence of $\boldsymbol{A}$, i.e.

$$\begin{aligned} \min_{\boldsymbol{c}} \quad & g_p(\boldsymbol{c}) \\ \text{s.t.} \quad & C_L \le c_i \le C_H, \quad i = 1, 2, \ldots, K \end{aligned} \tag{2}$$

However, (2) only concerns the performance of sparse channel estimation and the pilot power tends to be different.

*Joint optimisation:* Combining (1) and (2), the pilot power allocation with respect to both the sparse channel estimation performance and the secret key capacity can be formulated as

$$\begin{aligned} \min_{\boldsymbol{c}} \quad & \alpha g_p(\boldsymbol{c}) - (1-\alpha)\log_2\left(1 + \frac{1}{2K\sigma^2}\sum_{i=1}^{K} c_i\right) \\ \text{s.t.} \quad & C_L \le c_i \le C_H, \quad i = 1, 2, \ldots, K \end{aligned} \tag{3}$$

where $\alpha (0 \le \alpha \le 1)$ is a linear scaling factor that combines (1) and (2) in the simplest way. It is observed that (1) and (2) correspond to $\alpha = 0$ and $\alpha = 1$, respectively. If $\alpha > 0.5$, more weights are given on the coherence, which means that the performance of sparse channel estimation is more important than the secret key capacity. Otherwise, if $\alpha < 0.5$, the secret key capacity is more important.

We now propose a scheme to allocate power for pilot subcarriers. We first generate a table $\boldsymbol{M}$ as

$$\boldsymbol{M} = \begin{bmatrix} \omega & \omega^2 & \cdots & \omega^N \\ \omega^2 & \omega^4 & \cdots & \omega^{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{L-1} & \omega^{2(L-1)} & \cdots & \omega^{(L-1)N} \end{bmatrix} \tag{4}$$

where $\omega = \mathrm{e}^{-\mathrm{j}2\pi/N}$. Once $N$ and $L$ are given, $\boldsymbol{M}$ is determined. Given a pilot pattern $\boldsymbol{p}$, we look up $\boldsymbol{M}$ and select the corresponding $K$ columns indexed by $\boldsymbol{p}$ from $\boldsymbol{M}$, making up an $L-1$ by $K$ submatrix $\boldsymbol{M}(\boldsymbol{p})$. We have $g_p(\boldsymbol{c}) = ||\boldsymbol{M}(\boldsymbol{p})\boldsymbol{c}||_\infty$, where $||\boldsymbol{\mu}||_\infty$ denotes the infinity norm of $\boldsymbol{\mu}$. Then, (3) can be written as

$$\begin{aligned} \min_{\boldsymbol{c}} \quad & \alpha||\boldsymbol{M}(\boldsymbol{p})\boldsymbol{c}||_\infty - (1-\alpha)\log_2\left(1 + \frac{1}{2K\sigma^2}\sum_{i=1}^{K} c_i\right) \\ \text{s.t.} \quad & C_L \le c_i \le C_H, \quad i = 1, 2, \ldots, K \end{aligned} \tag{5}$$

which can be solved by an existing optimisation solver, e.g. CVX [11].

*Simulation results:* Alice and Bob transmit and receive information using an OFDM system with $N = 256$ subcarriers, where $K = 16$ subcarriers are used to transmit pilot symbols for channel estimation. A sparse multipath channel $\boldsymbol{h} = \boldsymbol{h}_{\mathrm{AB}} = \boldsymbol{h}_{\mathrm{BA}}$ is generated with $L = 50$ taps, where $S = 5$ dominant non-zero channel taps are randomly placed among $L$ taps. The channel gain of each path is modelled as an independent and identically distributed complex Gaussian variable with zero mean and unit variance, i.e. $\mathcal{CN}(0, 1)$. We set $C_L = 1$ and $C_H = 10$.

As shown in Table 1, we compare the coherence of the measurement matrix $\boldsymbol{A}$ and the secret key capacity for different $\alpha$. Although $\alpha = 0$ achieves larger capacity than the others, its coherence is also larger than the others, which implies that it achieves capacity at the cost of increased coherence. $\alpha = 1$ achieves the smallest coherence, but the capacity is also small. It is seen that $\alpha = 0.5$ can make an appropriate trade-off between the above two schemes by reducing the coherence without too much sacrifice of the secret key capacity.

Now, we further compare the performance of sparse channel estimation for different $\alpha$. It is shown in Fig. 2 that $\alpha = 0.5$ achieves similar mean square errors (MSE) as that of $\alpha = 0.7$ and $\alpha = 1$ and performs substantially better than that of $\alpha = 0.3$ and $\alpha = 0$. Note that secret key extraction is much easier with smaller MSE. Hence, it is better to choose $\alpha = 0.5$ which can make a proper trade-off between the secret key capacity and sparse channel estimation performance.

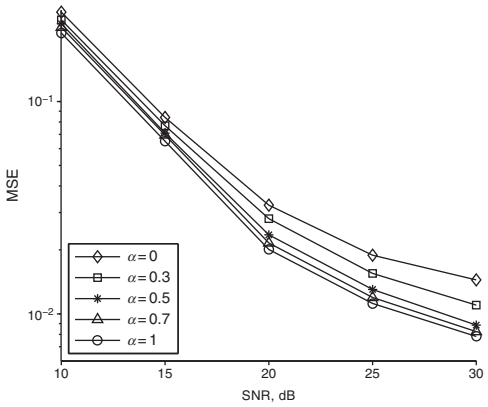


**Fig. 2** *Comparison of sparse channel estimation performance*

*Conclusion:* We have investigated pilot power allocation with respect to both sparse channel estimation performance and secret key capacity. We have formulated the pilot power allocation as a convex optimisation problem and propose a scheme that can solve the problem quickly by looking up a table and using existing optimisation solvers. Simulation results verify the effectiveness of the proposed approach.

*Acknowledgments:* This work was supported by the National Natural Science Foundation of China (NSFC) under grant 61302097 and the PhD Programs Foundation of the Ministry of Education of China under grant 20120092120014.


Submitted: *23 November 2014* E-first: *3 June 2015*
doi: 10.1049/el.2014.4078

Chenhao Qi and Lenan Wu (*School of Information Science and Engineering, Southeast University, Nanjing 210096, People's Republic of China*)

✉ E-mail: qch@seu.edu.cn

Arumugam Nallanathan (*Center for Telecommunications, King's College London, London WC2R 2LS, United Kingdom*)

## References

1 Schwenk, J., and Huber, K.: 'Public key encryption and digital signatures based on permutation polynomials', *Electron. Lett.*, 1998, **34**, (8), pp. 759–760
2 Ren, K., Su, H., and Wang, Q.: 'Secret key generation exploiting channel characteristics in wireless communications', *IEEE Wirel. Commun.*, 2011, **18**, (4), pp. 6–12
3 Berger, C.R., Wang, Z., Huang, J., and Zhou, S.: 'Application of compressive sensing to sparse channel estimation', *IEEE Commun. Mag.*, 2010, **48**, (11), pp. 164–174
4 Chou, T.H., Draper, S.C., and Sayeed, A.M.: 'Secret key generation from sparse wireless channels: ergodic capacity and secrecy outage', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (9), pp. 1751–1764
5 Sun, X., Xu, W., Jiang, M., and Zhao, C.: 'Improved generation efficiency for key extracting from wireless channels'. Proc. of IEEE Int. Conf. on Communications (ICC), Kyoto, Japan, June 2011, pp. 1–6
6 Chou, T.H., Sayeed, A.M., and Draper, S.C.: 'Minimum energy per bit for secret key acquisition over multipath wireless channels'. Proc. of IEEE Int. Symp. on Information Theory (ISIT), Seoul, Korea, June 2009, pp. 2296–2300
7 Qi, C., and Wu, L.: 'Tree-based backward pilot generation for sparse channel estimation', *Electron. Lett.*, 2012, **48**, (9), pp. 501–503
8 He, X., Song, R., and Zhu, W.-P.: 'Pilot allocation for sparse channel estimation in MIMO-OFDM systems', *IEEE Trans. Circuits Syst. II, Exp. Briefs*, 2013, **60**, (9), pp. 612–616
9 Qi, C., Wu, L., Huang, Y., and Nallanathan, A.: 'Joint design of pilot power and pilot pattern for sparse cognitive radio systems', *IEEE Trans. Veh. Technol.*, 2014, **PP**, (99), DOI:10.1109/TVT.2014.2374692
10 Ben-Haim, Z., Eldar, Y., and Elad, M.: 'Coherence-based performance guarantees for estimating a sparse vector under random noise', *IEEE Trans. Signal Process.*, 2010, **58**, (10), pp. 5030–5043
11 Boyd, S., and Vandenberghe, L.: 'Convex Optimization' (Cambridge University Press, 2004)