Adaptation de l'algorithme quantique de Grover à la détection multi-utilisateurs dans un système OCDMA

Muhammad Idham HABIBIE[1] Jihad HAMIE[1] Claire GOURSAUD[1]

[1] Université de Lyon, INSA Lyon, INRIA
CITI EA 3720
F-69621 Villeurbanne, France
muhammad-idham.habibie@insa-lyon.fr

Résumé – Pour prendre en charge les transmissions multiples dans une fibre optique, plusieurs techniques ont été étudiées, comme l'accès multiple par répartition en code (OCDMA). En particulier, les systèmes OCDMA incohérents sont appréciés pour leur simplicité. Cependant, ils souffrent de l'interférence d'accès multiple (MAI), qui dégrade les performances. Afin de faire face à cette MAI, plusieurs détecteurs ont été étudiés. Parmi eux, le Maximum Likelihood (ML) est le meilleur. Mais il est très coûteux, car il nécessite tester toutes les possibilités avant de prendre une décision. Cependant, grâce aux récentes avancées de l'informatique quantique, ce problème de complexité peut être contourné. En effet, les algorithmes quantiques, tels que Grover, exploitent les états de superposition dans le domaine quantique et permettent d'accélérer le calcul. Ainsi, dans cet article, nous proposons d'adapter l'algorithme quantique de Grover dans le contexte de la détection multi-utilisateurs, dans un système OCDMA utilisant des codes non-orthogonaux. Nous présentons un moyen d'adapter le signal bruité reçu aux contraintes définies par l'algorithme de Grover, et évaluons ensuite la probabilité de succès du récepteur quantique. Nous montrons les avantages de notre proposition par rapport au détecteur classique et au détecteur ML optimal.

Abstract – To support multiple transmissions in an optical fiber, several techniques have been studied such as Optical Code Division Multiple Access (OCDMA). In particular, the incoherent OCDMA systems are appreciated for their simplicity and reduced cost. However, they suffer from Multiple Access Interference (MAI), which degrades the performances. In order to cope with this MAI, several detectors have been studied. Among them, the Maximum Likelihood (ML) detector is the optimal one but it suffers from high complexity as all possibilities have to be tested prior to a decision. However, thanks to the recent quantum computing advances, the complexity problem can be circumvented. As a matter of fact, quantum algorithms, such as Grover, exploit the superposition states in the quantum domain to accelerate the computation. Thus, in this paper, we propose to adapt the quantum Grover's algorithm in the context of Multi-User Detection (MUD), in an OCDMA system using non-orthogonal codes. We propose a way to adapt the received noisy signal to the constraints defined by Grover's algorithm. We further evaluate the probability of success in detecting the active users for different noise levels. Aside from the complexity reduction, simulations show that our proposal has a high probability of detection when the received signal is not highly altered. We show the benefits of our proposal compared to the classical and optimal ML detector.

1 Introduction

La transmission par fibre optique est un élément clé des systèmes de communication actuels car cela une grande largeur de bande [1]. Néanmoins, le partage de cette ressource nécessite des techniques d'accès adaptées. Par rapport aux techniques historiques (Time Division Multiple Access (TDMA), Frequency DMA (FDMA), et Wavelength DMA (WDMA)), la plus récente Optical Code Division Multiple Access (OCDMA) a fait l'objet d'une attention particulière de la part de la communauté des chercheurs au cours des deux dernières décennies [2]. Les systèmes OCDMA peuvent être divisés en deux catégories : les systèmes cohérents et les systèmes incohérents. Dans la première catégorie, les codes sont bipolaires $c \in \{-1, 1\}$, et permettent la sélection de familles de codes parfaitement orthogonaux. Au contraire, les systèmes OCDMA incohérents considèrent des codes unipolaires $c \in \{0, 1\}$ [3]. Ce dernier permet l'utilisation d'un émetteur et d'un récepteur plus simples, mais au prix d'interférences entre les séquences transmises simultanément. Ces interférences sont appelées interférence d'accès multiple (MAI), et constituent l'une des principales limitations des performances et de la capacité de l'OCDMA. Des techniques de traitement ont été étudiées afin de réduire l'impact du MAI sur la performance finale. Les techniques de détection multi-utilisateurs (MUD), telles que Serial Interference Cancellation (SIC) et Parallel Interference Cancellation (PIC) avec Hard Limiter (HL) [4] [5], éliminent de manière itérative la contribution des utilisateurs brouilleurs. Les performances sont améliorées, mais elles n'atteignent jamais celles des détecteurs optimaux Maximum Likelihood (ML). La principale limite à l'utilisation de ce récepteur optimal est sa complexité.

Heureusement, l'informatique quantique est une solution prometteuse pour atténuer cette complexité. En effet, les algorithmes quantiques, tels que Grover, exploitent les états de superposition dans le domaine quantique pour accélérer le calcul. Dans [6], les auteurs ont étudié la détection quantique multi-utilisateurs (QMUD) pour les systèmes de communication sans fil. Cependant, à la connaissance des auteurs, l'approche consistant à utiliser des algorithmes quantiques pour l'OCDMA n'a pas encore été envisagée. Le présent document propose donc d'évaluer les avantages de l'utilisation d'un al-

gorithme quantique pour effectuer la MUD dans un système OCDMA utilisant des codes non orthogonaux. Nous évaluons également les performances de plusieurs ensembles de mots de code avec des bruits additifs ainsi que les attributs quantiques.

2 Vue d'ensemble de l'informatique quantique

2.1 Principe Quantique

L'approche quantique est basée sur un nouveau type de bits, à savoir les qubits. Les qubits sont dans l'état 0 et 1 simultanément (dans un état dit superposé) [7]. Un qubit est désigné par la notation de Dirac et s'écrit comme suit :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

où $\alpha, \beta \in \mathbb{C}$, et vérifient $|\alpha|^2 + |\beta|^2 = 1$. Mesurer $|\psi\rangle$ selon le base $\{|0\rangle, |1\rangle\}$ projettera aléatoirement le qubit sur $|0\rangle$ ou $|1\rangle$ en fonction de leur probabilité associée. Nous pouvons étendre ce principe en supposant que l'on dispose de N qubits. Dans ce cas, 2^N états peuvent être traités simultanément.

2.2 Algorithme de Grover

L'algorithme de Grover vise à résoudre $f(x) = \delta$, où δ est la valeur souhaitée, et $f(x)$ est la valeur de la fonction avec le qubit d'entrée $|x\rangle \in \mathbb{B}$. Tout d'abord, comme l'illustre la fig.1a, l'algorithme de Grover utilise Hadamard pour réaliser une superposition égale des états $|\psi\rangle$ [7]. L'équation de superposition complète s'écrit comme suit :

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle \tag{2}$$

L'algorithme de Grover se compose alors de deux parties : Oracle (U_w) et Diffuseur (U_s). L'Oracle (U_w) marque les états qui vérifient la contrainte ciblée $f(x) = \delta$ en fournissant une amplitude négative [7] et qui s'écrit comme suit :

$$U_w|\psi\rangle = (-1)^{f(x)}|q\rangle = \begin{cases} U_w|\psi\rangle & f(x) \neq \delta \\ -U_w|\psi\rangle & f(x) = \delta \end{cases} \tag{3}$$

Nous notons que la superposition des états $|\psi\rangle$ rend tous les états possibles égaux, alors que l'Oracle (U_w) ne marque que ceux qui satisfont $f(x) = \delta$. Les états marqués sont ensuite amplifiés par le diffuseur (U_s) qui agit comme une opération d'inversion par rapport à la moyenne.

$$\begin{aligned} U_s.U_w.|q\rangle &= H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}U_w|\psi\rangle \\ &= (2|s\rangle\langle s| - I).U_w.|\psi\rangle \end{aligned} \tag{4}$$

ou $H^{\otimes n}$ est le produit tensoriel de n copies de l'opérateur de Hadamard (H), et $|0^n\rangle$ représente l'état de base dans un système de n qubits. $|s\rangle$ est l'état initial equi-superposé. Pour trouver les solutions souhaitées, la séquence Oracle et Diffuseur est exécutée plusieurs fois $O(\sqrt{N})$ [7]. Après N_I étapes d'itération, la probabilité de succès (P_s) est donnée par [7] :

$$P_s(N_I) = \sin^2\left((2N_I + 1)\,\theta_s\right) \tag{5}$$

où $\theta_s = \arcsin^{-1}\sqrt{S/N}$. Dans ce contexte, [7] a défini le nombre optimal d'itérations pour trouver une solution spécifique qui dépend de la taille N de la base de données concernée et du nombre de solutions valides S comme :

$$L_{opt} = \lfloor \pi/4\sqrt{N/S} \rfloor \tag{6}$$

Le circuit de Grover se compose de nombreuses portes quantiques pour développer l'oracle et le diffuseur, comme illustré sur la Fig. 1b. Le circuit de Grover repose sur quatre registres différents : 1) *Registre d'index* 2) *Registre de valeur* 3) *Registre de référence* 4) *Registre de marque* [8]. Le registre des indices (taille N qubits) contient l'argument de la fonction x et fournira la solution livrée à la fin de l'algorithme. Le *registre de valeur* (taille Z qubits) contient la valeur de la fonction $f(x)$ appliquée au *registre d'index* de l'état, tandis que le *registre de référence* (taille Z qubits) correspond à la valeur souhaitée (δ). Le *registre de marquage* (taille 1 qubits) fournit le signe négatif au calcul, afin de marquer les états valides.

3 Système proposé

3.1 Modèle du système

Dans cet article, nous proposons d'adapter l'algorithme de Grover pour effectuer la détection multi-utilisateurs dans un système OCDMA, et nous évaluons ses performances. Dans un système OCDMA incohérent, nous considérons un réseau où chaque utilisateur k se voit attribuer un code unique $\underline{c_k} \in \{0,1\}^{SF}$ de facteur d'étalement (SF). Ce code est transmis uniquement si $b_k = 1$. Il faut noter que la transmission est classique (seul le décodage sera effectué dans le domaine quantique). Nous considérons un canal parfait $h = 1$, ainsi qu'un bruit blanc gaussien additif (AWGN) désigné par $\underline{n}$. Ainsi, le modèle complet du système peut être décrit de la façon suivante :

$$\underline{y} = \sum_{k=1}^{K} h b_k \underline{c_k} + \underline{n} \tag{7}$$

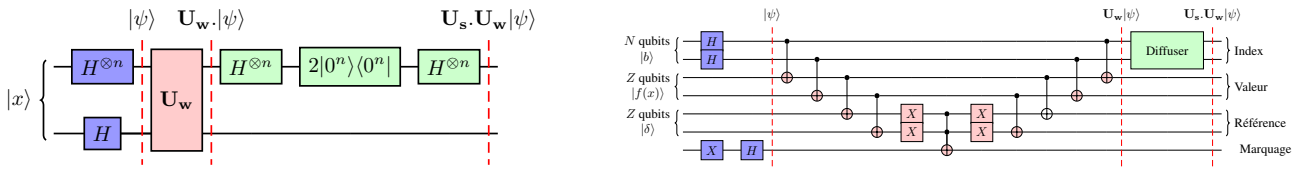
où $\underline{y} \in \mathbb{R}^{SF}$ est le signal reçu, K désigne le nombre d'utilisateurs, $b_k \in \{0,1\}$ est le bit transmis, c_k est le mot codé correspondant et $\underline{n}$ est le bruit gaussien dont chaque composante suit $\mathcal{N}(0,\sigma)$. L'objectif du récepteur est de déterminer les valeurs de tous les bits transmis $\hat{b} = \{\hat{b}_k | k \in \{1,...,K\}\}$.

3.2 Algorithme quantique proposé

L'algorithme de Grover ne prend en entrée que des nombres binaires et recherchera l'ensemble $\hat{b}$ le plus probable à l'origine du signal reçu. Mais, y dans eq.7 est une variable continue. Un moyen simple de surmonter ce problème est d'obtenir une approximation de $\underline{y}$ aux valeurs entières les plus proches. La partie entière conservée de $\underline{y}$ est limitée par $2^m - 1$, où m est le nombre de bits utilisés pour représenter chaque composant de $\underline{y}$. Ainsi, l'algorithme de Grover prend $\underline{\tilde{y}}$ comme entrée dans le *registre de référence* de la fig. 1b, comme par exemple :

$$\underline{\tilde{y}} = \min(\max(0, \text{round}(y)), 2^m - 1) \tag{8}$$

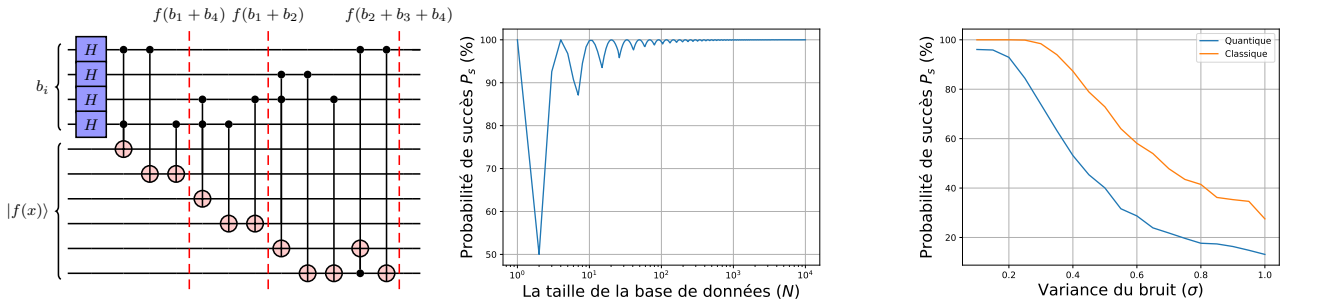
Le traitement dans le domaine quantique commence par l'application de l'algorithme de Grover approprié. L'algorithme est



(a) Le schéma de Grover

(b) Circuit de Grover 2 qubits

FIGURE 1 : Principe de Grover



(a) Oracle modifié $[\hat{y_1}, \hat{y_2}, \hat{y_3}]$

(b) Sans bruit : $P_s(\%)$ par rapport à N

(c) Canal bruité : $P_s(\%)$ par rapport à σ

FIGURE 2 : Oracle modifié et la mesure de P_s

exécuté avec le nombre optimal d'itérations et fournit en sortie l'ensemble des bits transmis estimés. L'algorithme proposé peut être résumé comme suit :

Algorithm 1 Algorithme proposé

1: Définir L_{opt} en connaissant le nombre de solutions (S) et la valeur désirée δ.
2: Observer le signal reçu avec un bruit additif (y)
3: Exécuter $\underline{\tilde{y}} = \min(\max(0, \text{round}(y)), 2^{m-1})$.
4: Convertir un nombre entier en nombre binaire $int(\underline{\tilde{y}}) \longrightarrow bin(\underline{\tilde{y}})$
5: Fournir $bin(\underline{\tilde{y}})$ dans *registre de référence*. Créer les circuits *registre de valeur* et *registre d'index* sur la base de la fig 2a.
6: Itérer Grover L_{opt} fois

Il est à noter que *registre de référence* contient les $\underline{\tilde{y}}$ tandis que *registre d'index* correspond à l'ensemble ciblé d'utilisateurs actifs $b_k \in \{0, 1\}$.

4 Configuration de la simulation et résultats

Pour valider notre approche, nous avons pris un exemple. Nous avons été contraints d'utiliser une configuration de réseau réduite, afin de pouvoir faire tourner la simulation sur un processeur classique. Nous nous sommes donc concentrés sur les codes ayant un petit facteur d'étalement (SF). Nous définissons pour chaque utilisateur i ($i \in \{1, 2, ..., K\}$, où K est le nombre total d'utilisateurs) un code $c_i = [c_i^1, c_i^2, ..., c_i^{SF}]$. Nous avons choisi une famille de codes qui permet de traiter le nombre maximal d'utilisateurs, sous la contrainte que 2 de sous-ensembles différents du code ne conduisent pas à la même signature superposée. Avec cette contrainte, nous nous assurons que la fonction qui relie l'ensemble d'activités b au signal reçu y est injective, et donc que, dans un cas sans bruit, la probabilité d'erreur est nulle. Nous supposons que nous avons un facteur d'étalement SF $= 3$ avec un nombre d'utilisateurs $K = 4$. Nous avons sélectionné des mots de codes de 4 utilisateurs comme suit : $c_1 = [1, 1, 0], c_2 = [0, 1, 1], c_3 = [0, 0, 1], c_4 = [1, 0, 1]$.

Sur la base de ces codes, la fonction oracle, qui évalue le signal reçu attendu en fonction des bits transmis, a été implémentée dans Qiskit, conduisant au circuit présenté sur la fig.2a. Nous pouvons noter que deux qubits sont utilisés pour représenter chaque composante $\hat{y}$. Ceci est dû au fait que pour le jeu de codes considéré, la valeur maximale qui peut être atteinte sur n'importe quel slot est de 3.

Avec les codes choisis, la séquence reçue $\hat{y}$ peut être dérivée $\underline{\tilde{y_1}} = b_1 + b_4 + \tilde{n_1}; \underline{\tilde{y_2}} = b_1 + b_2 + \tilde{n_2}; \underline{\tilde{y_3}} = b_2 + b_3 + b_4 + \tilde{n_3}$.

L'implémentation spécifique de ces équations est présentée, pour exemple, sur la fig.2a. Pour d'autres familles de codes, ou hypothèses, cette partie sera de nouveau modifée.Les autres parties telles que *registre de référence*, *registre de marque* et diffuseur sont toujours les mêmes, mais seulement ajustées en fonction de la dimension concernée.

Une fois le circuit réalisé, nous envoyons le composant $\hat{y}$ au *registre de référence*. Ensuite, nous exécutons le circuit avec L_{opt} itérations pour atteindre les performances optimales.

4.1 Performances dans le cas sans bruit

Pour évaluer les performances, nous considérons d'abord le cas idéal où aucun bruit n'affecte le signal reçu. Dans ce cas, pour l'algorithme ML classique, la probabilité de succès est $P_s = 1$ grâce au caractère injectif des codes choisis.

Avec l'algorithme quantique, nous pouvons voir sur la fig.2b qu'à mesure que la taille de la base de données augmente, avec $N_I = L_{opt}$ dans l'équation 5, la probabilité de réussite tend vers 1. Ainsi, l'efficacité de l'algorithme quantique augmente pour un plus grand nombre d'utilisateurs. En effet, selon l'équation (5), lorsque N est suffisamment grand, la

probabilité de succès devrait converger vers 1. En outre, nous pouvons noter que lorsque la taille de la base de données est faible, par exemple $N = 2$, probabilité de succès diminue à $\sim 50\%$ même pour le nombre d'itérations optimal. Cela est dû au fait que le nombre optimal d'itérations est arrondi à sa partie entière (eq.6), et pour une petite taille de base de données, le nombre entier obtenu est plus susceptible d'être éloigné du nombre réel.

4.2 Performances dans le cas bruité

Dans cette partie, nous prenons en compte le bruit. Nous supposons que le bruit suit une loi normale avec une moyenne $\mu = 0$ et un écart type noté σ. Nous pouvons rencontrer deux situations. Dans la première situation, le bruit ne conduit pas à une modification de la signature $\hat{y}$ introduite dans l'algorithme de Grover. En effet, si la contribution du bruit est suffisamment faible, elle est supprimée par la fonction d'arrondi appliquée au signal reçu y. Ainsi, le calcul quantique a une forte probabilité de succès pour identifier correctement les utilisateurs, et présente les mêmes performances que dans le cas sans bruit. C'est souvent le cas lorsque l'écart-type du bruit est faible.

Dans la seconde situation, avec un écart de bruit plus important, la signature $\hat{y}$ est modifiée ; soit en tant qu'autre signature valide (conduisant à une probabilité de réussite presque nulle), soit en tant que signature non valide (conduisant à des statistiques équiprobables parmi toutes les (N) solutions possibles dans la base de données).

Dans la pratique, le système est confronté à ces deux situations, avec un équilibre différent, en fonction de l'écart de bruit réel. La probabilité de réussite est donc obtenue par une combinaison linéaire des 2 situations. Le détecteur ML optimal et les algorithmes que nous proposons sont comparés dans la fig.2c, otenue pour une famille avec $N = 5$ utilisateurs. Cette figure montre la variation de la probabilité moyenne de succès dans la détection des utilisateurs actifs, en fonction de l'écart-type du bruit σ. Pour chaque variance de bruit, 4000 réalisations indépendantes de processus de bruit sont testées et moyennées. Nous pouvons tout d'abord constater que les performances se dégradent lorsque la variance du bruit augmente. La probabilité de succès passe du maximum dans le cas sans bruit (96%), à une sélection aléatoire avec des variables équiprobables ($6.25\% = 100/16$). En outre, comme on s'y attendait, le ML fournit la meilleure précision puisqu'il s'agit de l'algorithme optimal, mais on peut noter que notre proposition donne des résultats comparables à ceux du détecteur ML, en particulier lorsque le niveau de bruit est relativement faible. De plus, grâce à la Fig. 2b, nous pouvons nous attendre à ce que la différence de performance diminue pour une taille de réseau plus importante, car l'algorithme de Grover devient plus précis. En outre, notre proposition quantique surpasse le détecteur ML en termes de complexité, car le détecteur ML classique nécessite $2^K = 16$ évaluations, tandis que celui de Grover a besoin de $\sqrt{2^K}$. Comme indiqué dans l'équation (5), le bénéfice quantique augmente avec le nombre d'utilisateurs. Nous pouvons donc observer que la solution que nous proposons permet de réduire considérablement le délai de calcul au prix d'un impact raisonnable sur les performances. Ainsi, notre proposition peut être un détecteur prometteur d'utilisateurs actifs dans un réseau de communication massif.

5 Conclusion

Dans cet article, nous avons adapté l'algorithme quantique de Grover à des fins de MUD dans un système de communication OCDMA. L'algorithme de Grover adapté est alimenté par des signaux reçus bruités, qui sont préalablement traités afin d'être conformes aux contraintes de l'algorithme de Grover. La probabilité de détection des utilisateurs actifs a été évaluée en fonction du rapport signal sur bruit (RSB) ou de la variance du bruit. Les résultats obtenus sur un réseau de petite taille ont montré que notre proposition a une bonne performance de détection, même si elle n'est pas aussi bonne que le détecteur ML optimal, mais avec une complexité beaucoup plus faible. Il est intéressant de noter que les résultats ont prouvé qu'à mesure que la taille de la base de données augmente, la probabilité de succès peut tendre vers 100%.

Références

[1] Alaan GHAZI, S. ALJUNID, Alaa FAREED, Syed Zulkarnain SYED IDRUS, Syed IDRUS[1], C.B.M. RASHIDI, Marwa ALBAYATY, Aras AL-DAWOODI et Ahmed FAKHRUDEEN : Performance analysis of zcc-optical-cdma over smf for fiber-to- the-home access network. *Journal of Physics Conference Series*, page 22013, 06 2020.

[2] Hichem MRABET, Abdelhamid CHERIFI, Thiago RADDO, Iyad DAYOUB et Shyqyri HAXHA : A comparative study of asynchronous and synchronous ocdma systems. *IEEE Systems Journal*, 15(3):3642–3653, 2021.

[3] Chih-Ta YEN et Chih-Ming CHEN : A study of three-dimensional optical code-division multiple-access for optical fiber sensor networks. *Computers and Electrical Engineering*, 49:136–145, 2016.

[4] B MANATSAVEE, Kazi AHMED et Anil FERNANDO : Performance of pic, sic and decorrelating detectors for mud technique in wcdma system. *In Fourth International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint*, volume 2, pages 892–896. IEEE, 2003.

[5] Muhammad Idham HABIBIE, Jihad HAMIE et Claire GOURSAUD : Adaptation of grover's quantum algorithm to multiuser detection in an ocdma system. *In 2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT)*, pages 88–93, 2021.

[6] Panagiotis BOTSINIS, Soon Xin NG et Lajos HANZO : Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design. *IEEE Access*, 1:94–122, 2013.

[7] Michael A. NIELSEN et Isaac L. CHUANG : *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[8] Panagiotis BOTSINIS, Zunaira BABAR, Dimitrios ALANIS, Daryus CHANDRA, Hung NGUYEN, Soon NG et L. HANZO : Quantum error correction protects quantum search algorithms against decoherence. *Scientific Reports*, 6, 12 2016.