HAL
open science

Consensus de moyenne dans un réseau de capteurs sans fil sécurisé

Alain Kibangou

To cite this version:

Alain Kibangou. Consensus de moyenne dans un réseau de capteurs sans fil sécurisé. CIFA 2012 - 7ème Conférence Internationale Francophone d'Automatique, Jul 2012, Grenoble, France. Paper ThAM2T8.5. hal-00735066

HAL Id: hal-00735066

https://hal.science/hal-00735066v1

Submitted on 25 Sep 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Consensus de moyenne dans un réseau de capteurs sans fil sécurisé

Alain Y. Kibangou *

* *GIPSA-LAB,*
UMR 5216 – Université Joseph Fourier, CNRS
11, rue des mathématiques. Grenoble Campus, BP 46,
F-38402 Saint Martin d'Hères Cedex, France.
Alain.Kibangou@ujf-grenoble.fr

Résumé : Dans cet article, notre étude est relative au problème du consensus de moyenne dans un réseau de capteurs. Contrairement à différents algorithmes, proposés dans la littérature, qui ne garantissent qu'une convergence asymptotique, nous proposons deux nouvelles approches de synthèse des matrices de consensus permettant d'atteindre le consensus de moyenne en un nombre fini d'itérations. Dans des travaux récents, nous avons montré que ce nombre n'est autre que celui des valeurs propres distinctes et non nulles de la matrice Laplacienne du graphe. Dans le présent article, nous montrons comment faire la synthèse des matrices de consensus dans le cas d'un réseau sécurisé. En particulier, nous montrons que dans le cas d'un graphe de Hamming ou plus généralement d'un graphe distance-régulier le consensus de moyenne peut être réalisé en un nombre d'itérations égal au diamètre du graphe associé.

Mots-clés: Consensus ; Réseaux de capteurs ; Algorithmes distribués ; Réseaux sécurisés ; Théorie des graphes.

1. INTRODUCTION

Ces dernières années de nombreuses contributions ont été apportées, tant dans la communauté de l'automatique que de celle du traitement du signal, en termes d'algorithmes d'estimation distribuée à l'aide de capteurs sans fil aussi bien statiques que mobiles, Blondel et al. (2005); Olfati-Saber et Murray (2004). Un tel effort est motivé par le grand potentiel qu'ont les réseaux de capteurs en termes d'applications.

La plupart des algorithmes d'estimation distribuée sont basés sur le concept du consensus. L'objectif principal d'un algorithme de consensus étant de faire converger tous les nœuds du réseau vers une valeur commune après négociations. Par exemple, le consensus de moyenne, consistant à faire converger tous les nœuds vers la moyenne de leurs valeurs initiales, peut être obtenu en mettant à jour de manière itérative les valeurs locales des différents nœuds comme étant une somme pondérée des valeurs issues des voisins.

Une caractéristique importante d'un réseau de capteurs sans fil concerne la topologie du réseau. Les différents nœuds du réseau sont généralement représentés comme étant les sommets d'un graphe dont les arêtes représentent l'existence d'une communication entre les nœuds associés. En raison de ses ressources limitées, un nœud-capteur ne peut communiquer qu'avec d'autres nœuds se trouvant dans son rayon de communication. Ainsi, la couche physique du réseau donne lieu généralement à un graphe géométrique aléatoire.

Cependant, les réseaux de capteurs sans fil ont plusieurs caractéristiques qui ne garantissent ni l'intégrité physique des capteurs ni la confidentialité des messages échangés. Tout d'abord, un canal sans fil est ouvert à tous. Avec une interface radio configurée sur la même bande de fréquences, n'importe qui peut avoir accès aux messages échangés et même s'inviter à la conversation. Ensuite, les ressources limitées en calcul et en mémoire ne permettent pas d'implémenter des algorithmes de sécurité robustes. Un réseau de capteurs sans fil peut donc être sujet à différentes attaques extérieures. En conséquence, il est nécessaire de rajouter, via la couche réseau, des algorithmes de cryptage de complexité calculatoire faible mais d'efficacité maximale. Ainsi, la couche réseau peut induire un graphe différent de celui engendré par la couche physique. Pour être voisins, il ne suffit plus que deux capteurs soient dans un même rayon de communication mais il faut en plus qu'ils soient à même de partager une même clé cryptographique. Dans ce cas, la structure du graphe est imposée par la technique de cryptage utilisée.

La plupart des travaux dédiés à l'estimation distribuée basée sur des algorithmes de consensus de moyenne ne considèrent que le graphe lié à la couche physique. Dans cet article, nous nous intéressons au problème du consensus dans des réseaux sécurisés utilisant des techniques de pré-distribution de clés. En particulier, nous montrons qu'en absence de bruit, le consensus de moyenne peut être atteint en un nombre fini d'itérations.

Le problème du consensus de moyenne en un nombre fini d'itérations a été étudié par un certain nombre d'auteurs. Dans Kingston et Beard (2006), la méthode proposée requiert un graphe complet durant au moins une itération.

Un algorithme d'agrégation de données est proposé par Lechevin et al. (2009), approche nécessitant davantage de ressources en mémoire qu'une approche itérative. Une autre approche plus compatible aux ressources des capteurs est celle proposée par Sundaram et Hadjicostis (2008). L'idée principale exploitée par les auteurs est qu'au bout d'un certain temps, les capteurs ont suffisamment d'observations leur permettant de reconstruire l'état initial du système et d'en déduire toute fonction de celui-ci, la moyenne par exemple. Dans Sundaram et Hadjicostis (2007), les mêmes auteurs montrent que chaque capteur peut calculer la valeur du consensus comme une combinaison linéaire de ses valeurs antérieurs après D itérations, D étant le degré du polynôme caractéristique de la matrice de consensus associée. Cependant, cette approche nécessite le calcul du rang d'une matrice et de son noyau ; ce qui a un coût de calcul élevé. Dans Ko (2010), le consensus en temps fini est formulé comme un problème de factorisation de matrices. Cependant, la méthode requiert une topologie variable dans le temps, les variations étant guidées par un nœud central. Récemment, nous avons reformulé le problème comme étant un problème de diagonalisation conjointe de matrices permettant de conserver la topologie du réseau constante. La solution proposée requiert toutefois l'utilisation du spectre de la matrice Laplacienne du graphe, Kibangou (2011, 2012).

2. POSITION DU PROBLÈME

Considérons un réseau représenté à l'aide d'un graphe non-orienté et connecté $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ où $\mathcal{N} = \{1, \cdots, N\}$ désigne l'ensemble des sommets et $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ l'ensemble d'arêtes. Nous notons par $\mathcal{N}_i$ l'ensemble des nœuds pouvant communiquer avec le nœud n_i (pour l'instant nous ne distinguons pas la couche physique de la couche réseau). Son cardinal est noté N_i. La matrice Laplacienne $\mathbf{L}$ du graphe $\mathcal{G}$, est définie par ses éléments l_{ij} donnés par :

$$l_{ij} = \begin{cases} N_i & \text{si } i = j \\ -1 & \text{si } j \in \mathcal{N}_i \\ 0 & \text{partout} \quad \text{ailleurs} \end{cases}$$

Le graphe étant non-orienté, la matrice Laplacienne est symétrique ($\mathbf{L} = \mathbf{L}^T$). Ses valeurs propres, $\lambda_0 < \lambda_1 \leq \cdots \leq \lambda_{N-1}$, permettent d'appréhender de nombreuses propriétés associées à la topologie du graphe $\mathcal{G}$. En particulier, $\lambda_0 = 0$ avec $\mathbf{1}$, le vecteur ayant tous ses éléments égaux à 1, comme vecteur propre.

A présent, supposons que chaque nœud n dispose initialement d'une valeur scalaire $x_n(0) \in \Re$ et définissons par $\mathbf{x}(0) = (\, x_1(0) \cdots x_N(0) \,)^T$ le vecteur des valeurs initiales du réseau. Nous nous intéressons à calculer la valeur moyenne des valeurs initiales au moyen d'un algorithme distribué, chaque nœud ne pouvant communiquer qu'avec ses voisins. Ainsi, à chaque itération, le nœud n met à jour sa valeur $x_n(t)$ comme une combinaison linéaire des apports de ses voisins et de sa valeur antérieure :

$$x_n(t+1) = w_{nn} x_n(t) + \sum_{m \in \mathcal{N}_n} w_{nm} x_m(t) \qquad (1)$$

De manière équivalente, sous forme matricielle on obtient :

$$\mathbf{x}(t+1) = \mathbf{W}\mathbf{x}(t) \qquad (2)$$

où les valeurs hors diagonales $w_{i,j}$ de la matrice $\mathbf{W}$ sont non-nulles si et seulement si $j \in \mathcal{N}_i$. Le consensus de moyenne est atteint si

$$\lim_{t \to \infty} \mathbf{x}(t) = \frac{1}{N} \mathbf{1}\mathbf{1}^T \mathbf{x}(0),$$

ce qui signifie que

$$\lim_{t \to \infty} \mathbf{W}^t = \frac{1}{N} \mathbf{1}\mathbf{1}^T.$$

La condition nécessaire et suffisante permettant d'atteindre le consensus est : $\mathbf{W}$ doit admettre 1 comme valeur propre simple, les autres valeurs propres étant de valeur absolue strictement inférieure à 1. Les vecteurs propres à gauche et à droite associés à la valeur propre 1 étant donnés par $\frac{1}{N}\mathbf{1}$ et $\mathbf{1}$, Xiao et Boyd (2004). Grâce à cette condition, la convergence asymptotique est assurée.

Plusieurs matrices de pondération $\mathbf{W}$ permettent d'assurer une convergence asymptotique. L'une d'elles, couramment utilisée, est reliée à la matrice laplacienne du graphe de la manière suivante : $\mathbf{W} = \mathbf{I} - \gamma \mathbf{L}$, avec $0 < \gamma < 1/N_{max}$, $N_{max} = \max\{N_1, \cdots, N_N\}$, Olfati-Saber et al. (2007).

La vitesse de convergence de l'algorithme du consensus est directement liée à la seconde plus grande valeur propre de la matrice de pondération $\mathbf{W}$. Par conséquent, différents auteurs ont proposé différentes techniques pour accélérer la convergence en modifiant adéquatement le spectre de la matrice de pondération, Xiao et Boyd (2004); Kokiopoulou et Frossard (2009); Montijano et al. (2011). Bien que les algorithmes de consensus rapide soient suffisant dans de nombreux cas, la détermination de l'arrêt de l'algorithme n'est cependant pas claire. Il est donc parfois plus judicieux de recourir à des algorithmes garantissant une valeur exacte en un nombre fini d'itérations. Par ailleurs de tels algorithmes peuvent permettre de mieux évaluer la durée de vie du réseau. Dans la suite de cet article, nous allons développer de nouvelles techniques de calcul de consensus en temps fini en considérant des connexions sécurisées via un schéma de prédistribution de clés cryptographiques.

3. SÉCURISATION DES COMMUNICATIONS À L'AIDE DE CLÉS CRYPTOGRAPHIQUES

La plupart des protocoles de sécurité sont basés sur des opérations cryptographiques nécessitant des clés. Pour assurer la confidentialité, une opération de cryptage nécessite une clé embarquée dans un algorithme permettant de transformer un message en un cryptogramme. Deux types de clés sont utilisées dans les systèmes cryptographiques.

La première est la clé symétrique dont les propriétés théoriques ont été établies dans Shannon (1949). Dans ce type d'approche, la source et le destinataire partagent une clé secrète inconnue des autres nœuds du réseau. La source code son message M avec la clé K à l'aide d'un algorithme de cryptage E générant ainsi un cryptogramme $C = E(M, K)$. Après réception du message crypté, le destinataire recouvre le message original à l'aide d'un algorithme de décryptage D et de la clé secrète : $M = D(C, K)$, Zhou et al. (2008).

La seconde approche considère une clé asymétrique. Chaque nœud dispose d'une paire de clés $\{K_s, K_p\}$. La clé privée K_s est gardée secrète par son détenteur qui

diffuse sa clé publique K_p. Ainsi chaque source désirant envoyer un message M vers le source de clé publique K_p code le message de la manière suivante : $C = E(M, K_p)$. A la réception le message est décrypté en faisant $M = D(C, K_s)$. Il est à noter que la mise en place d'une approche de sécurisation asymétrique est plus complexe que l'approche asymétrique. Par conséquent, la plupart des protocoles de sécurité dans les réseaux de capteurs sans fil utilisent des clés symétriques.

La procédure de sécurisation d'un réseau de capteurs sans fil inclut deux étapes. Avant d'être déployés, les nœuds sont configurés avec un certain nombre de clés. Une fois déployés, les nœuds choisissent les clés à utiliser après plusieurs échanges de messages. Ce choix peut être fait via un serveur de clés, Perrig et al. (2002). Bien évidemment l'existence d'un tel serveur central en fait un point névralgique dont toute défaillance ruinerait les efforts de sécurisation entrepris. Par conséquent, la plupart des solutions récemment proposées sont distribuées, Zhou et al. (2008). Dans l'une d'elles, chaque nœud est associé à un identifiant unique $(n_1, n_2, \cdots, n_k)$ de sorte que tous les nœuds forment une grille de dimension k. Chaque nœud, lors de sa configuration, est équipé d'un certain nombre de clés qu'il peut partager avec d'autres nœuds avec qui il partage la même dimension. Ainsi, deux nœuds ne peuvent partager une secrète que si la distance de Hamming de leurs identifiants est égale à 1. En d'autres termes, tous les éléments de l'identifiant sont égaux sauf un, Zhou et Fang (2007). En appliquant un tel protocole, le graphe résultant de la couche réseau est donc un graphe de Hamming dont nous allons exploiter différentes propriétés.

3.1 Algèbre de Bose-Mesner

Rappelons tout d'abord quelques définitions :
- Deux sommets sont adjacents s'il existe une arête entre eux. On définit alors la matrice d'adjacence $\mathbf{A}$ d'entrées $A_{ij} = 1$ s'il existe une arête entre les sommets i et j et $A_{ij} = 0$ dans le cas contraire.
- Un chemin est une liste de sommets telle qu'il existe une arête entre chaque paire de sommets. Ce chemin est dit simple si chaque arête est empruntée une seule fois.
- La longueur du chemin correspond au nombre d'arêtes parcourues.
- La distance entre deux sommets est la longueur du plus court chemin contenant ces deux sommets.
- Le diamètre d'un graphe est la distance maximale quelque soit la paire de sommets.
- Un graphe est dit régulier de degré (ou valence) k si tous les sommets ont exactement le même nombre de voisins.
- Un graphe est dit distance-régulier si pour tous sommets n_i et n_j le nombre de sommets voisins de n_i à distance d et le nombre de sommets voisins de n_j à distance δ ne dépendent que de d, δ et de la distance entre n_i et n_j.

Soit $\mathcal{G}(\mathcal{N}, \mathcal{E})$ un graphe distance-régulier de valence k. Notons $R_m \subset \mathcal{E}$ le sous-ensemble d'éléments (n_i, n_j) tels que n_i et n_j sont à une distance m. Soit $\mathbf{A}_m$ la matrice d'adjacence du graphe $\mathcal{X}_m = (\mathcal{N}, R_m)$. Evidemment $\mathbf{A}_0 = \mathbf{I}$, la matrice identité et $\mathbf{A}_1 = \mathbf{A}$, la matrice d'adjacence du graphe $\mathcal{G}$. Les matrices $\mathbf{A}_m$, $m = 0, \cdots, D$, engendrent une algèbre de dimension $(D+1)$ de matrices symétriques ayant une diagonale constante. Cette algèbre est celle de Bose-Mesner (voir Bose et Mesner (1959)). Il en découle les propriétés suivantes :

$$\sum_{m=0}^{D} \mathbf{A}_m = \mathbf{1}\mathbf{1}^T \tag{3}$$

et

$$\mathbf{A}\mathbf{A}_m = b_{m-1}\mathbf{A}_{m-1} + a_m\mathbf{A}_m + c_{m+1}\mathbf{A}_{m+1}, \quad m = 1, \cdots, D \tag{4}$$

où

$$a_m + b_m + c_m = k,$$
$$a_0 = 0,\ b_0 = k,\ b_D = 0,\ c_0 = 1,\ \text{et}\ c_1 = 1.$$

3.2 Graphe de Hamming

Le graphe de Hamming $H(D, q)$ de dimension D sur un alphabet S de taille q est le graphe dont les sommets sont l'ensemble des mots de longueur D sur un alphabet S. Deux sommets sont adjacents dans $H(D, q)$ s'ils sont à une distance de Hamming de 1. Ce graphe admet les propriétés suivantes Brouwer et al. (1989) :
- Chaque sommet est connecté à exactement $D(q-1)$ voisins ;
- Le diamètre du graphe est égal à D ;
- Le graphe est $D(q-1)$-régulier ;
- Le graphe est distance régulier avec comme paramètres $c_i = i$ et $b_i = (q-1)(D-i)$.
- Sa matrice d'adjacence admet comme valeurs propres $(q-1)D - qi$ de multiplicité $\binom{D}{i}(q-1)^i$, $i = 0, 1, \cdots, D$.

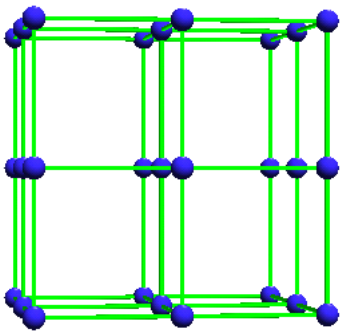

FIG. 1. Graphe cubique en treillis ou graphe de Hamming $H(3, q)$, avec $q = 3$

4. CONSENSUS EN TEMPS FINI DANS UN RÉSEAU SÉCURISÉ REPRÉSENTÉ À L'AIDE D'UN GRAPHE DE HAMMING

Nous allons à présent considérer le problème du consensus en un nombre fini d'itérations dans un réseau représenté à l'aide d'un graphe de Hamming. Il s'agit de faire la synthèse d'un ensemble de matrices $\{\mathbf{W}_i\}_{i=1,\cdots,d}$, compatibles avec le réseau, telles que

$$\prod_{i=1}^{d} \mathbf{W}_i = \frac{1}{N}\mathbf{1}\mathbf{1}^T. \tag{5}$$

Notons qu'une matrice $\mathbf{W}_i$ est dite compatible avec le réseau s'il existe une matrice $\mathbf{Q}_i$ telle que $\mathbf{W} = \mathbf{Q}_i \circ \mathbf{A}$ où $\circ$ représente le produit de Hadamard et $\mathbf{A}$ la matrice d'adjacence du graphe représentant le réseau.

A cet effet, nous allons centrer notre étude sur des matrices de consensus dépendant de la matrice Laplacienne du graphe et paramétrées par des constantes α_i :

$$\mathbf{W}_i = \mathbf{I} - \alpha_i \mathbf{L}.$$

On peut aisément vérifier que ces matrices sont compatibles avec le réseau.

4.1 Synthèse basée sur une diagonalisation conjointe de matrices

La matrice Laplacienne du graphe étant sysmétrique, sa diagonalisation est donnée par :

$$\mathbf{L} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^T, \ \ \mathbf{U}^T\mathbf{U} = \mathbf{I}, \ \ \mathbf{U}\mathbf{U}^T = \mathbf{I}$$

où $\mathbf{\Lambda} = diag(\lambda_0, \lambda_1, \cdots, \lambda_{N-1})$ et $\mathbf{U} = \left(\frac{1}{\sqrt{N}}\mathbf{1} \ \tilde{\mathbf{U}} \right)$ avec $\tilde{\mathbf{U}}^T\tilde{\mathbf{U}} = \mathbf{I}_{N-1}$ et $\tilde{\mathbf{U}}^T\mathbf{1} = \mathbf{0}$.

Par suite, les matrices de pondération $\mathbf{W}_i$ peuvent être exprimées en fonction des valeurs propres et des vecteurs propres de la matrice Laplacienne :

$$\mathbf{W}_i = \mathbf{U}\left(\mathbf{I} - \alpha_i \mathbf{\Lambda}\right)\mathbf{U}^T.$$

Par conséquent, l'équation (5) peut être récrite comme :

$$\mathbf{U}\left(\prod_{i=1}^{d}(\mathbf{I} - \alpha_i\mathbf{\Lambda})\right)\mathbf{U}^T = \frac{1}{N}\mathbf{1}\mathbf{1}^T \tag{6}$$

ou de manière équivalente :

$$\mathbf{U}\left(\prod_{i=1}^{d}(\mathbf{I} - \alpha_i\mathbf{\Lambda})\right)\mathbf{U}^T = \mathbf{U}diag(1 \quad 0 \cdots 0)\mathbf{U}^T. \tag{7}$$

Nous pouvons alors formuler le théorème suivant :

Théorème 1. Soient $\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_D \neq 0$ les D valeurs propres distinctes non-nulles de la matrice Laplacienne $\mathbf{L}$ du graphe représentant le réseau. Les matrices de pondérations $\mathbf{W}_i = \mathbf{I} - \frac{1}{\lambda_i}\mathbf{L}$, $i = 1, \cdots, D$, permettent d'atteindre la valeur exacte du consensus de moyenne en D itérations.

Preuve : A partir de l'équation (7), nous obtenons :

$$\prod_{i=1}^{d}(1 - \alpha_i\lambda_j) = \begin{cases} 1 \text{ si } j = 0 \\ 0 \text{ sinon} \end{cases}$$

Puisque $\lambda_0 = 0$, nous avons donc à résoudre

$$\prod_{i=1}^{d}(1 - \alpha_i\lambda_j) = 0, \ \ j = 2, 3, \cdots, N.$$

En prenant en compte les multiplicités des valeurs propres, il n'y a que D équations distinctes. Une solution de ce système d'équation est alors obtenue en prenant α_i égal à l'inverse d'une des valeurs propres λ_i de la matrice Laplacienne. ■

Nous en déduisons le corollaire qui suit :

Corollaire 1. Les matrices de pondérations

$$\mathbf{W}_i = \mathbf{I} - \frac{1}{qi}\mathbf{L}, \ \ i = 1, \cdots, D$$

permettent d'atteindre la valeur exacte du consensus de moyenne dans un graphe de Hamming $H(D, q)$.

Preuve : On sait que $\mathbf{L} = \mathbf{D} - \mathbf{A}$ où $\mathbf{D}$ est la matrice diagonale contenant les degrés de chaque sommets. Pour un graphe k-régulier, $\mathbf{D} = k\mathbf{I}$. Sachant que les valeurs propres distinctes de la matrice d'adjacence d'un graphe de Hamming $H(D, q)$ sont données par $(q-1)D - qi$, $i = 0, 1, \cdots, D$ et sachant que la valence de ce graphe de Hamming est $D(q-1)$, nous déduisons que :

$$\lambda_i = qi, \quad i = 0, 1, \cdots, D.$$

Par application du théorème 1, nous déduisons les valeurs des constantes α_i. ■

Nous pouvons noter que dans le cas d'un graphe de Hamming et plus généralement dans le cas des graphes distance-régulier, le nombre d'itérations de l'algorithme de consensus proposé est exactement égal au diamètre du graphe. Rappelons que celui-ci représente la distance entre les deux points les plus distants du réseau.

Exemple 1. Considérons un graphe de Hamming $H(3, 2)$. D'après le corollaire du théorème 1, les matrices de consensus sont données par : $\mathbf{W}_1 = \mathbf{I} - \frac{1}{2}\mathbf{L}$, $\mathbf{W}_2 = \mathbf{I} - \frac{1}{4}\mathbf{L}$ et $\mathbf{W}_3 = \mathbf{I} - \frac{1}{6}\mathbf{L}$. Le tableau 1 décrit les trois itérations de l'algorithme de consensus permettant de calculer la moyenne des valeurs initiales.

TAB. 1. Consensus de moyenne dans un graphe $H(3, 2)$

$\mathbf{x}(0)$	$\mathbf{x}(1)$	$\mathbf{x}(2)$	$\mathbf{x}(3)$
4.1000	2.6000	2.9100	3.1950
3.1000	2.4150	3.4800	3.1950
2.9100	3.5350	3.4800	3.1950
2.1700	4.2300	2.9100	3.1950
3.2900	3.0900	3.4800	3.1950
1.6600	4.6750	2.9100	3.1950
3.7100	3.5550	2.9100	3.1950
4.6200	1.4600	3.4800	3.1950

Exemple 2. Considérons un graphe de Hamming $H(4, 2)$. D'après le corollaire du théorème 1, les matrices de consensus sont données par : $\mathbf{W}_1 = \mathbf{I} - \frac{1}{2}\mathbf{L}$, $\mathbf{W}_2 = \mathbf{I} - \frac{1}{4}\mathbf{L}$, $\mathbf{W}_3 = \mathbf{I} - \frac{1}{6}\mathbf{L}$, et $\mathbf{W}_4 = \mathbf{I} - \frac{1}{8}\mathbf{L}$. Le tableau 2 décrit les quatre itérations de l'algorithme de consensus permettant de calculer la moyenne des valeurs initiales.

TAB. 2. Consensus de moyenne dans un graphe $H(4, 2)$

$\mathbf{x}(0)$	$\mathbf{x}(1)$	$\mathbf{x}(2)$	$\mathbf{x}(3)$	$\mathbf{x}(4)$
2.3100	4.4550	2.7375	3.2337	3.1800
3.8600	1.6800	3.9175	3.1262	3.1800
4.2500	1.1000	4.3550	3.1262	3.1800
1.5000	6.2350	1.7100	3.2337	3.1800
1.6000	4.7400	2.7800	3.1262	3.1800
3.5700	2.0050	3.2850	3.2337	3.1800
2.6000	3.6600	2.8475	3.2337	3.1800
3.6900	1.5650	3.8075	3.1262	3.1800
3.8200	3.4300	2.8750	3.1262	3.1800
3.7000	2.9750	3.1900	3.2337	3.1800
4.2900	3.0700	2.7525	3.2337	3.1800
3.6700	2.4950	3.9025	3.1262	3.1800
4.2000	1.0000	4.3275	3.2337	3.1800
2.0000	5.1550	2.3275	3.1262	3.1800
2.9800	3.9850	2.7650	3.1262	3.1800
2.8400	3.3300	3.3000	3.2337	3.1800

4.2 Synthèse basée sur l'algèbre de Bose-Mesner

En utilisant différentes propriétés issues de l'algèbre de Bose-Mesner, nous allons à présent montrer comment faire la synthèse des matrices de pondération $\mathbf{W}_i = \mathbf{I} - \alpha_i \mathbf{L}$. Pour ce faire, nous énonçons tout d'abord le lemme suivant :

Lemme 1. Etant donnée la matrice Laplacienne $\mathbf{L} = k\mathbf{I} - \mathbf{A}$ d'un graphe distance-régulier de valence k et de paramètres b_i et c_i, les matrices $\mathbf{L}^m$ sont à diagonale principale constante et peuvent être développées sur la base des matrices d'adjacence associées à l'algèbre de Bose-Mesner :

$$\mathbf{L}^m = \sum_{i=0}^{m} \beta_{i,m} \mathbf{A}_i \tag{8}$$

où les coefficients de développement s'écrivent de manière recursive comme suit, pour $i = 1, \cdots, m+1$:

$$\begin{aligned} \beta_{i,m} &= -c_i \beta_{i-1,m-1} + (b_i + c_i)\beta_{i,m-1} - b_i \beta_{i+1,m-1}, \\ &\qquad i = 1, \cdots, m \\ \beta_{i,m} &= 0, \quad i > m \\ \beta_{0,0} &= 1. \end{aligned} \tag{9}$$

Preuve : Nous pouvons vérifier que cette proposition est vraie pour L^0 et pour L. Supposons qu'elle est vraie pour L^{m-1} et montrons qu'elle l'est aussi au rang supérieur :

$$\begin{aligned} \mathbf{L}^m = \mathbf{L}\mathbf{L}^{m-1} &= (k\mathbf{I} - A) \sum_{i=0}^{m-1} \beta_{i,m-1} \mathbf{A}_i \\ &= \sum_{i=0}^{m-1} k\beta_{i,m-1} \mathbf{A}_i - \sum_{i=0}^{m-1} \beta_{i,m-1} \mathbf{A}\mathbf{A}_i \end{aligned}$$

Tenant compte de la propriété (4), nous obtenons :

$$\begin{aligned} \mathbf{L}^m = &\sum_{i=0}^{m-1} (k - a_i)\beta_{i,m-1} \mathbf{A}_i - \sum_{i=0}^{m-1} b_{i-1}\beta_{i,m-1} \mathbf{A}_{i-1} \\ &- \sum_{i=0}^{m-1} c_{i+1}\beta_{i,m-1} \mathbf{A}_{i+1} \end{aligned}$$

Sachant que $c_0 = 0$, nous pouvons récrire l'expression précédente de la manière suivante :

$$\begin{aligned} \mathbf{L}^m = &\sum_{i=0}^{m-1} (k - a_i)\beta_{i,m-1} \mathbf{A}_i - \sum_{i=0}^{m-2} b_i \beta_{i+1,m-1} \mathbf{A}_i \\ &- \sum_{i=0}^{m} c_i \beta_{i-1,m-1} \mathbf{A}_i \end{aligned}$$

Les termes $\beta_{i,m-1}$ étant nuls pour $i > m-1$ et sachant que $k - a_i = b_i + c_i$ nous obtenons :

$$\mathbf{L}^m = \sum_{i=0}^{m-1} \left((b_i + c_i)\beta_{i,m-1} - b_i \beta_{i+1,m-1} - c_i \beta_{i-1,m-1} \right) \mathbf{A}_i$$

d'où l'expression de $\beta_{i,m}$ donnée en (9). ■

Une conséquence intéressante de ce Lemme est que réciproquement nous pouvons écrire les matrices $\mathbf{A}_i$ comme des combinaisons linéaires de puissances de la matrice Laplacienne :

$$\mathbf{A}_m = \sum_{i=0}^{m} \gamma_{i,m} \mathbf{L}^i, \tag{10}$$

les coefficients $\gamma_{i,m}$ étant les éléments de la matrice triangulaire inférieure $\mathbf{\Gamma} = \mathbf{B}^{-1}$ avec :

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \beta_{0,1} & \beta_{1,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{0,m} & \beta_{1,m} & \cdots & \beta_{m,m} \end{pmatrix} \tag{11}$$

Par suite, tenant compte des équations (3) et (10) nous pouvons conclure que :

$$\sum_{m=0}^{D} \sum_{i=0}^{m} \frac{\gamma_{i,m}}{N} \mathbf{L}^i = \frac{1}{N} \mathbf{1}\mathbf{1}^T. \tag{12}$$

Nous pouvons alors formuler le théorème suivant :

Théorème 2. L'ensemble des matrices de pondération $\mathbf{W}_i = \mathbf{I} - \frac{1}{\epsilon_i}\mathbf{L}$, $i = 1, \cdots, D$, permet d'atteindre le consensus de moyenne en D itérations si les pas ϵ_i sont les racines du polynôme $p(t) = \sum_{m=0}^{D} \sum_{i=0}^{m} \gamma_{i,m} t^i$.

On peut montrer que les racines du polynôme $p(t)$ correspondent aux valeurs propres non nulles de la matrice Laplacienne. Ce qui permet de conclure que les deux approches de synthèse des matrices de consensus sont strictement équivalentes.

On peut par ailleurs noter que grâce aux symétries présentes dans le réseau. Le nombre d'itérations ne dépend pas du nombre de nœuds dans le réseau. Pour un graphe de Hamming $H(D, q)$ contenant q^D sommets, le nombre d'itérations ne dépend que de D. Ainsi, pour un réseau de N nœuds tel que $N = q_1^{D_1} = q_2^{D_2}$ avec $D_1 > D_2$, il vaut mieux structurer la sécurisation du réseau en utilisant des identifiants les plus courts possibles. En d'autres termes, il vaut mieux choisir des identifiants de longueur D_2 plutôt que D_1. On peut notamment se restreindre à l'utilisation d'identifiant de longueur $D = 3$. Dans ce cas, le graphe correspondant est aussi appelé graphe cubique en treillis Laskar (1969).

Exemple 3. Considérons de nouveau un graphe de Hamming H(3,2). On peut aisément vérifier que la matrice $\mathbf{B}$, définie par (11), est donnée par :

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & -1 & 0 & 0 \\ 12 & -6 & 2 & 0 \\ 54 & -34 & 18 & -6 \end{pmatrix}.$$

Par suite, on en déduit :

$$\mathbf{\Gamma} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & -1 & 0 & 0 \\ 3 & -3 & 1/2 & 0 \\ 1 & -10/3 & 3/2 & -1/6 \end{pmatrix}$$

D'après le théorème 2, les pas ϵ_i, $i = 1, 2, 3$ sont les racines du polynôme $p(t) = \frac{-1}{6}t^3 + 2t^2 - \frac{22}{3}t + 8$. On obtient $\epsilon_i \in \{2, 4, 6\}$, qui sont les valeurs propres non-nulles de la matrice Laplacienne du graphe.

Exemple 4. Dans cet exemple, nous considérons un graphe de Hamming H(5,3). C'est un graphe de valence 10 contenant 243 nœuds. Ces paramètres sont $c_i = i$ et $b_i = 2(5-i)$,

$i = 0, 1, \cdots, D$. En utilisant les formules récursives donnant les paramètres $\beta_{i,m}$, on obtient la matrice $\mathbf{B}$ suivante.

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 10 & -1 & 0 & 0 & 0 & 0 \\ 110 & -19 & 2 & 0 & 0 & 0 \\ 1290 & -297 & 54 & -6 & 0 & 0 \\ 15870 & -4395 & 1062 & -204 & 24 & 0 \\ 202650 & -63921 & 18510 & -4710 & 960 & -120 \end{pmatrix}.$$

Après avoir déduit les paramètres $\gamma_{i,m}$, on peut conclure que les pas ϵ_i, $i = 1, 2, 3$ sont les racines du polynôme $p(t) = 243 - 184.95t + 50.625t^2 - 6.375t^3 + 0.375t^4 - 0.0083t^5$. On obtient $\epsilon_i \in \{3, 6, 9, 12, 15\}$, qui sont les valeurs propres non-nulles de la matrice Laplacienne du graphe.

5. CONCLUSION

De nombreuses contributions récentes parues dans la littérature montrent l'intérêt d'utiliser l'algorithme de consensus en vue de distribuer une tâche d'estimation, de commande ou plus généralement d'optimisation. La plupart de ces algorithmes ont des propriétés de convergence asymptotique dont la rapidité est liée au spectre des matrices de consensus. Dans cet article, nous avons développé un nouveau résultat permettant d'atteindre le consensus de moyenne en un nombre fini d'itérations. Cette performance est réalisée en utilisant des matrices de consensus variant dans le temps, la loi de variation étant fixée par l'ensemble des valeurs propres non-nulles de la matrice Laplacienne du graphe. Bien souvent, l'étude du problème du consensus est menée en ne considérant que le graphe induit par la couche physique ; graphe dans lequel l'existence d'une arête est liée à la présence de capteurs dans le rayon de communication de la source. En y ajoutant les contraintes de sécurité, le graphe engendré par la couche réseau peut avoir des propriétés pouvant être exploitées pour améliorer les algorithmes d'estimation. Lorsque le schéma de sécurisation des données d'un réseau engendre un graphe distance-régulier, nous avons développé une nouvelle approche de synthèse des matrices de consensus permettant d'achever celui-ci en un temps fini correspondant au diamètre du graphe. Dans les travaux futurs nous nous intéresserons à l'impact du bruit et de la perte des paquets dans les communications entre capteurs. Il est à noter que dans le cas d'une communication via un canal additif blanc gaussien, nous avons montrer dans Kibangou (2011) que l'algorithme du consensus en temps fini pouvait être utilisé comme étant le noyau d'une approche de type monte-carlo.

RÉFÉRENCES

Blondel, V., Hendrickx, J., Olshevsky, A., et Tsitsiklis, J. (2005). Convergence in multiagent coordination, consensus, and flocking. In *Proc. of the joint 44th IEEE Conf. on Decision and Control (CDC) and European Control Conf (ECC)*, 2996–3000. Seville, Spain.

Bose, R. et Mesner, D. (1959). On linear associative algebras corresponding to association schemes of partially balanced designs. *The Annals of Mathematical Statistics*, 30, 21–38.

Brouwer, A., Cohen, A., et Neumaier, A. (1989). *Distance-regular graphs.* Springer.

Kibangou, A. (2011). Finite-time average consensus based protocol for distributed estimation over awgn channels. In *Proc. of the 50th IEEE Conference on Decision and Control (CDC).* Orlando, Fl, USA.

Kibangou, A. (2012). Graph laplacian based matrix design for finite-time distributed average consensus. In *Proc. of the American Conference on Control(ACC).* Montréal, Canada.

Kingston, D. et Beard, R. (2006). Discrete-time average consensus under switching network topologies. In *Proc. of American Control Conference (ACC).* Minneapolis, Minenesota, USA.

Ko, C.K. (2010). *On matrix factorization and scheduling for finite-time average consensus.* Thèse de doctorat, California Institue of Technology, Pasadena, California, USA.

Kokiopoulou, E. et Frossard, P. (2009). Polynomial filtering for fast convergence in distributed consensus. *IEEE Trans. on Signal Processing*, 57, 342–354.

Laskar, R. (1969). Eigenvalues of the adjacency matrix of cubic lattice graphs. *Pacific Journal of Mathematics*, 29(3), 623–629.

Lechevin, N., Rabbath, C., et Zhang, Y. (2009). Information broadcasting algorithm for finite-time reaching-at-risk consensus with application to weapon-target assignment. In *Proc. of American Control Conference (ACC)*, 3286–3291. St. Louis, MO, USA.

Montijano, E., Montijano, J., et Sagues, C. (2011). Fast distributed consensus with Chebyshev polynomials. In *2011 American Control Conference*, 5450–5455. San Francisco, CA, USA.

Olfati-Saber, R., Fax, A., et Murray, R. (2007). Consensus and cooperation in networked multi-agent systems. *Proc. of the IEEE*, 95(1), 215–233.

Olfati-Saber, R. et Murray, R. (2004). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Trans. on Automatic Control*, 49, 1520–1533.

Perrig, A., Szewczyk, R., Tygar, J., Wen, V., et Culler, D. (2002). SPINS : Security protocols for sensor networks. *Wireless Networks*, 8, 521–534.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28, 656–715.

Sundaram, S. et Hadjicostis, C. (2007). Finite-time distributed consensus in graphs with time-invariant topologies. In *Proc. of American Control Conference (ACC).* New York City, USA.

Sundaram, S. et Hadjicostis, C. (2008). Distributed function calculation and consensus using linear iterative strategies. *IEEE Journal on Selected Areas in Communications*, 26(4), 650–660.

Xiao, L. et Boyd, S. (2004). Fast linear iterations for distributed averaging. *Systems Control Lett.*, 53, 65–78.

Zhou, Y. et Fang, Y. (2007). Scalable and deterministic key agreement scheme for large scale networks. *IEEE Trans. Wireless Communications*, 6(11).

Zhou, Y., Fang, Y., et Zhang, Y. (2008). Securing wireless sensor networks : a survey. *IEEE Communications Surveys*, 10(3), 6–28.