Détection des faux avis dans un cadre évidentiel Fake reviews detection in an evidential framework

Malika Ben Khalifa, Zied Elouedi, Eric Lefevre

Détection des faux avis dans un cadre évidentiel

Fake reviews detection in an evidential framework

M. Ben Khalifa[1] Z. Elouedi[1] E. Lefèvre[2]
[1] Université de Tunis, Institut Supérieur de Gestion de Tunis, LARODEC, Tunisia
[2] Univ. Artois, EA 3926, Laboratoire de Génie Informatique et d'Automatique de l'Artois (LGI2A), Béthune, F-62400, France

malikabenkhalifa2@gmail.com, zied.elouedi@gmx.fr
eric.lefevre@univ-artois.fr

Résumé :
De nos jours, les opinions partagées sur les sites web sont devenues l'une des principales sources d'information lors de la prise de décision pour les acheteurs (qu'ils soient des particuliers ou des entreprises). Malheureusement, l'importance de la publicité et l'attrait du profit ont provoqué l'apparition de fausses opinions afin de troubler les consommateurs. Puisque les avis donnés sont généralement imprécis et incertains, il est assez difficile de distinguer les faux avis des vrais. Dans cet article, nous proposons une nouvelle méthode de détection de faux avis, capable de traiter l'incertitude en se fondant sur la théorie des fonctions de croyance. Cette approche permet de prendre en compte la compatibilité entre l'avis donné et tous les autres. Nous proposons de valider le comportement de notre méthode à travers des exemples numériques et de l'évaluer à travers des bases artificielles. Ces expérimentations prouvent que cette méthode, prenant en compte l'incertitude, constitue une première démarche intéressante pour la détection de fausses opinions.

Mots-clés :
Faux avis, Incertitude, Théorie des fonctions de croyance.

Abstract:
Nowadays, opinions sharing websites are used as one of the main sources of information for both customers and companies and influence potential purchases to make or reserve decisions. Due to the reviews' dominance power, spammers create fake reviews to confuse the consumers. So, it is crucial to detect fake reviews from the genuine ones. Since the reviews provide imperfections, the spam reviews detection became one of the most challenging problems. In this paper, we elucidate a new method to detect fake reviews using the belief function theory. This method handles the uncertainty in the vote reviews and takes into consideration the compatibility between the given rating opinions and all other ones. We propose to validate our method behavior through numerical examples and to evaluate it via artificial ones. Experimentation proves that the proposed method is promising solution for the fake reviews detection.

Keywords:
Fake reviews, Uncertainty, Belief function theory.

1 Introduction

Au cours des dernières années, on note l'émergence des avis publiés en ligne que ce soit sur les forums, les plateformes ou les sites d'opinions tels que Amazon.com, Tripadvisor.com, Yelp.com, PriceGrabber.com, Shopzilla.com et Resellerratings.com, qui permettent aux clients de partager leurs expériences, ainsi que leurs attitudes à l'égard de différents produits et services. Ces avis influencent implicitement la prise de décision des clients potentiels, d'où l'apparition de faux avis. Ils peuvent être positifs afin d'enjoliver l'attractivité de certains services et produits, ou bien négatifs afin de discréditer la concurrence et ainsi détruire leur réputation. Cela rend indispensable la détection des avis malveillants pour gagner la confiance des clients et maintenir une concurrence équitable entre les entreprises.
Ce problème a attiré l'attention de beaucoup de chercheurs qui ont proposé différentes techniques visant à détecter les faux avis. La plupart de ces travaux ont eu recours aux aspects linguistiques et sentimentaux [3], au style d'écriture [2, 8], à la lisibilité et à la subjectivité [13] pour détecter les commentaires frauduleux. Certains chercheurs essaient de détecter les groupes de spammeurs qui ont un grand pouvoir de manipulation sur l'opinion public à l'égard des produits et des services. Dans [12], les auteurs ont étudié ce problème en définissant un ensemble de huit indicateurs qui utilisent le comportement des membres du groupe tels

que la date des publications, la similarité des avis fournis, etc. D'autres études [11] ont proposé des scores de groupes de candidats tenant en compte les différentes relations entre les individus ainsi que les produits. D'autres techniques se sont concentrées sur la détection des spammeurs en se fondant sur des graphes [1, 6, 19] composés essentiellement par trois types de nœuds : les revues, les évaluateurs et les magasins. L'écart par rapport à l'évaluation globale a été utilisé comme une caractéristique importante dans [14, 16, 20]. Toutes ces études ont apporté des résultats significatifs. En outre, un algorithme pour détecter les "burst patterns" dans les opinions a été proposé dans [7]. Il a généré cinq nouvelles caractéristiques de comportement des évaluateurs afin de les utiliser comme indicateurs dans la détection des spammeurs.

À notre connaissance, aucun travail n'a pris en compte l'incertitude dans les opinions. Toutefois, la détection des faux avis est un problème nécessitant la gestion des imperfections car il implique des avis qui sont imprécis et incertains. Dans ce contexte, nous proposons une nouvelle méthode permettant la détection des faux avis en se fondant sur la théorie des fonctions de croyance. En effet, cette théorie est capable de gérer l'incertitude et permet de faire face à l'ignorance partielle et totale. En outre, notre méthode nécessite en entrée des opinions peu informatives comme des évaluations données sous forme de notations globales ainsi chaque évaluateur donne une seule opinion. L'objectif est de déterminer si cette opinion est vraie ou fausse.

Cet article est structuré de la façon suivante. Dans la section 2, nous présentons les concepts de base de la théorie des fonctions de croyance. Ensuite, dans la section 3, nous détaillons notre méthode. L'expérimentation, validant le comportement de notre méthode à travers des exemples numériques et l'évaluant en utilisant des bases de données artificielles, sera décrite dans la section 4. Enfin, une conclusion et des travaux futurs sont proposés dans la section 5.

2 La théorie des fonctions de croyance

2.1 Les concepts de base

La théorie des fonctions de croyance, connue également sous le nom de la théorie de l'évidence [4, 15], permet de modéliser et de gérer les données incertaines.

Le cadre de discernement Ω est un ensemble fini et exhaustif des différents événements associés à un problème donné. L'ensemble puissance de Ω, noté 2^Ω, contient l'union des événements possibles et l'ensemble vide (qui représente le conflit). Il est défini par : $2^\Omega = \{A : A \subseteq \Omega\}$.

Une fonction de masse de croyance bba est définie comme une fonction m^Ω de 2^Ω à $[0, 1]$ telle que : $\sum_{A\subseteq\Omega} m^\Omega(A) = 1$. Les sous-ensembles A de Ω, ayant une masse strictement positive, $m^\Omega(A) > 0$, sont appelés éléments focaux. Les différents types d'imperfection sont représentés par des fonctions de masse spéciales :

- Une bba certaine est définie comme suit : $m^\Omega(\{\omega_i\}) = 1$ et $\omega_i \in \Omega$.
- Une bba vide est définie comme suit : $m^\Omega(\Omega) = 1\ m^\Omega(A) = 0\ \forall A \neq \Omega$. Cette fonction modélise l'état de l'ignorance totale.
- Une bba catégorique est définie comme suit : $m^\Omega(A) = 1$ avec $A \subset \Omega$ et $m^\Omega(B) = 0\ \forall B \subseteq \Omega$ et $B \neq A$. Cette bba a un élément focal unique A.
- Une fonction à support simple est définie comme suit :

$$m^\Omega(X) = \begin{cases} \omega & \text{si} \quad X = \Omega \\ 1-\omega & \text{si} \quad X = A \\ 0 & \forall X \in 2^\Omega \backslash \{\Omega, A\} \end{cases} \tag{1}$$

où A est l'élément focal et $\omega \in [0, 1]$.

2.2 Affaiblissement

Les différentes sources d'information ne sont pas généralement fiables, c'est pourquoi on associe une mesure de confiance à chaque

source d'information indiquant sa fiabilité. Cette opération permet d'affaiblir les masses à travers le taux d'affaiblissement $\alpha \in [0,1]$ tel que $(1-\alpha)$ est le degré de fiabilité de la source. Par conséquent, la bba affaiblie ${}^{\alpha}m^{\Omega}$ est définie comme suit [15] :

$$\begin{cases} {}^{\alpha}m^{\Omega}(A) = (1-\alpha)m^{\Omega}(A) & \forall A \subset \Omega, \\ {}^{\alpha}m^{\Omega}(\Omega) = \alpha + (1-\alpha)m^{\Omega}(\Omega). \end{cases} \tag{2}$$

2.3 Combinaison

Soient m_1^{Ω} et m_2^{Ω} deux bbas différentes définies sur le même cadre de discernement Ω issues de deux sources distinctes.
Plusieurs règles de combinaison ont été proposées dans le cadre de la théorie des fonctions de croyance. Chaque règle a ses spécificités et ses caractéristiques. Nous présenterons dans ce qui suit certaines des plus utilisées.

Règle de combinaison conjonctive : Introduite par Smets [18], elle permet de combiner deux bbas issues de sources d'informations distinctes et fiables. Elle est notée $\textcircled{\cap}$ et est définie par :

$$m_1^{\Omega}\textcircled{\cap}m_2^{\Omega}(A) = \sum_{B \cup C = A} m_1^{\Omega}(B) m_2^{\Omega}(C) \tag{3}$$

La masse affectée à l'ensemble vide, $m(\emptyset)$, quantifie le degré de conflit entre les deux bbas.
Règle de combinaison de Dempster : C'est la version normalisée de la règle conjonctive qui redistribue de manière proportionnelle la masse sur l'ensemble vide [4]. Elle est notée par $\oplus$ et définie par :

$$m_1^{\Omega} \oplus m_2^{\Omega}(A) = \begin{cases} \frac{m_1^{\Omega}\textcircled{\cap}m_2^{\Omega}(A)}{1-m_1^{\Omega}\textcircled{\cap}m_2^{\Omega}(\emptyset)} & \text{si} A \neq \emptyset, \forall A \subseteq \Omega, \\ 0 & sinon. \end{cases} \tag{4}$$

Règle de combinaison avec un conflit adapté CWAC : Cette combinaison [5] agit comme la règle conjonctive quand les bbas sont antonymes (en conflit) et comme la règle de Dempster quand les bbas sont similaires.
Pour assurer l'adaptation entre toutes les sources, cette combinaison prend en compte la notion de dissimilarité à travers la distance de Jousselme [10] qui est définie comme suit :

$$d(m_1^{\Omega}, m_2^{\Omega}) = \sqrt{\frac{1}{2}(m_1^{\Omega} - m_2^{\Omega})^T D (m_1^{\Omega} - m_2^{\Omega})}, \tag{5}$$

avec T la transposée et D est l'indice de Jaccard défini par :

$$D(E,F) = \begin{cases} 1 & \text{si} \quad E = F = \emptyset, \\ \frac{|E \cap F|}{|E \cup F|} & \forall E, F \in 2^{\Omega} \backslash \emptyset \end{cases} \tag{6}$$

L'objectif de cette règle est d'identifier si au moins une des sources est opposée aux autres. Cette synthèse peut être obtenue en prenant, par exemple, la valeur maximale de toutes les distances. Par conséquent, la valeur de D_{max} peut être définie comme suit :

$$D_{max} = max[d(m_i^{\Omega}, m_j^{\Omega})], \tag{7}$$

avec $i \in [1, M]$, $j \in [1, M]$, M est le nombre total de fonctions de masse. La règle de combinaison CWAC est alors :

$$\begin{aligned} m^{\Omega}_{\textcircled{\leftrightarrow}}(A) = (\textcircled{\leftrightarrow} m_i^{\Omega})(A) = D_{max} m^{\Omega}_{\textcircled{\cap}}(A) \\ + (1 - D_{max}) m^{\Omega}_{\oplus}(A) \end{aligned} \tag{8}$$

2.4 Décision

Dans cette étape, on choisit l'hypothèse la plus appropriée pour un problème donné. Le modèle des croyances transférables (TBM en anglais pour Transferable Belief Model), proposé dans [17], est composé à la fois d'un niveau crédal où les croyances sont manipulées (modélisées, affaiblies, combinées, etc) et d'un niveau pignistique où les bbas sont transformées en probabilités pignistiques. Cette information notée $BetP$ est définie comme suit :

$$BetP(B) = \sum_{A \subseteq \Omega} \frac{|A \cap B|}{|A|} \frac{m^{\Omega}(A)}{(1 - m^{\Omega}(\emptyset))} \quad \forall\, B \in \Omega \tag{9}$$

3 Détection des faux avis dans un cadre évidentiel

Dans cet article, nous proposons une méthode de Détection de Faux Avis dans un cadre Évidentiel (DFAE) dont l'objectif principal est de distinguer les avis frauduleux des avis authentiques tout en gérant l'incertitude. Notre méthode utilise uniquement une opinion globale comme entrée. Étant donnée une base de données de N opinions qui ont des valeurs différentes comprises entre 1 et 5 étoiles (respectivement très mauvais, mauvais, moyen, bon et excellent), chaque opinion V_i (également appelée vote par la suite) est fournie par un évaluateur E_i avec i son identifiant. Notre méthode est composée de quatre étapes principales détaillées comme suit.

3.1 Modélisation des opinions par des fonctions de masses

Nous adoptons la théorie des fonctions de croyance afin de modéliser les imperfections des opinions, chaque opinion V_i sera transformée en une fonction de masse $m^{\Omega}_{ik}(\{k\})$ définie sur $\Omega = \{1, 2, 3, 4, 5\}$ où chaque élément de Ω représente le nombre d'étoiles donné par un évaluateur E_i et modélisé par k.
Nous pensons que l'évaluateur qu'il soit un spammeur ou un véritable client peut donner une opinion imprécise et qu'il est incertain à une valeur près. Ainsi, nous proposons de modéliser le vote global donné par le vote, vote+1 et vote-1 représenté par k et modélisé comme suit : $m^{\Omega}_{ik}(\{k\}) = 1$ avec $k \in \{V_i, V_{i+1}, V_{i-1}\}$. Dans le cas extrême supérieur ($V_i = 5$), nous modélisons le vote et le vote-1 c-à-d $k \in \{V_i, V_{i-1}\}$ et dans le cas extrême inférieur ($V_i = 1$) nous modélisons le vote et le vote+1 c-à-d $k \in \{V_i, V_{i+1}\}$.
Exemple 1. Prenons l'exemple de 5 évaluateurs qui donnent une note globale pour juger un hôtel, détaillé dans le tableau 1.
Dans cet exemple, on souhaite étudier la véracité de l'avis donné par E_1. Ainsi pour la phase de modélisation des connaissances,

Tableau 1 – Évaluation de l'hôtel

Évaluateurs	Votes
E_1	4 *
E_2	4 *
E_3	5 *
E_4	3 *
E_5	1 *

nous obtenons pour E_1 : $m^{\Omega}_{14}(\{4\}) = 1$; $m^{\Omega}_{15}(\{5\}) = 1$; $m^{\Omega}_{13}(\{3\}) = 1$.

Par la suite, nous proposons de modéliser le degré de fiabilité de l'évaluateur E_i par $(1 - \alpha_i)$ avec α_i son taux d'affaiblissement. Sa valeur est entre $[0, 1]$. Lorsque l'évaluateur est totalement fiable $\alpha_i = 0$ et dans le cas contraire lorsque $\alpha_i = 1$, l'évaluateur n'est pas fiable et il ne sera pas pris en considération. Nous calculons α_i comme suit :

$$\alpha_i = \frac{\text{Nombre de votes différents du vote courant}}{\text{Nombre de votes total}} \tag{10}$$

Le processus traite les votes un à un donc le vote courant est celui qui est en cours de traitement.
Ainsi, chaque vote transformé en fonction de masse est affaibli par son degré de fiabilité relative $1 - \alpha_i$ en utilisant l'opération d'affaiblissement et par conséquent son avis sera représenté par une fonction à support simple.
Exemple 2. Nous continuons avec l' Exemple 1, nous calculons le degré de fiabilité de l'évaluateur E_1 : $\alpha_1 = \frac{3}{5} = 0.6$.
Après l'opération d'affaiblissement, les bbas seront représentées par des fonctions à support simple comme suit : ${}^{\alpha_1}m^{\Omega}_{14}(\{4\}) = (1 - 0.6) * 1 = 0.4$; ${}^{\alpha_1}m^{\Omega}_{14}(\{\Omega\}) = 0.6 + (1 - 0.6) * 0 = 0.6$.
${}^{\alpha_1}m^{\Omega}_{15}(\{5\}) = 0.4$; ${}^{\alpha_1}m^{\Omega}_{15}(\{\Omega\}) = 0.6$.
${}^{\alpha_1}m^{\Omega}_{13}(\{3\}) = 0.4$; ${}^{\alpha_1}m^{\Omega}_{13}(\{\Omega\}) = 0.6$.

En outre, nous proposons de prendre en compte

la distance entre la valeur d'un vote donné, noté V_i, et les valeurs qui le modélisent (vote, vote+1 et vote-1) notées k et représentées par m_{ik}. Cette distance est modélisée par β_{ik} qui sera considéré comme un facteur d'affaiblissement. La valeur de β_{ik} est comprise entre $[0, 1]$, si $\beta_{ik} = 0$ alors le vote modélisé correspond à celui fourni et si $\beta_{ik} = 1$ cela signifie que le vote modélisé est très éloigné de celui donné. Le facteur d'affaiblissement β_{ik} est calculé comme suit :

$$\beta_{ik} = \frac{|V_i - k|}{\text{La valeur du vote maximale}} \qquad (11)$$

Ensuite, chaque fonction de croyance à support simple associée à chaque vote donné est affaiblie par $(1 - \beta_{ik})$ en utilisant l'opération d'affaiblissement.

Exemple 3. Considérons le même Exemple 1, nous calculons le facteur d'affaiblissement β de l'évaluateur E_1 : $\beta_{14} = \frac{|4-4|}{5} = 0$; $\beta_{15} = \frac{|4-5|}{5} = 0.2$; $\beta_{13} = \frac{|4-3|}{5} = 0.2$.
En appliquant la deuxième opération d'affaiblissement, les bbas se transforment comme suit :
${}^{\alpha_1\beta_{14}}m^{\Omega}_{14}(\{4\}) = 0.4$; ${}^{\alpha_1\beta_{14}}m^{\Omega}_{14}(\{\Omega\}) = 0.6$.
${}^{\alpha_1\beta_{15}}m^{\Omega}_{15}(\{5\}) = 0.32$; ${}^{\alpha_1\beta_{15}}m^{\Omega}_{15}(\{\Omega\}) = 0.68$.
${}^{\alpha_1\beta_{13}}m^{\Omega}_{13}(\{3\}) = 0.32$; ${}^{\alpha_1\beta_{13}}m^{\Omega}_{13}(\{\Omega\}) = 0.68$.

Enfin, nous combinons les trois bbas affaiblies (deux dans les cas extrêmes) qui modélisent chaque vote donné en utilisant la règle de Dempster (Eq. 4) afin de représenter chaque vote donné par une bba, notée m^{Ω}_i, contenant quatre éléments focaux (trois dans les cas extrêmes).

Exemple 4. Après avoir agrégé les votes actualisés correspondant à E_1 (calculé dans l'Exemple 3) en utilisant la règle de Dempster, nous trouvons : $m^{\Omega}_1 = {}^{\alpha_1\beta_{14}}m^{\Omega}_{14} \oplus {}^{\alpha_1\beta_{13}}m^{\Omega}_{13} \oplus {}^{\alpha_1\beta_{15}}m^{\Omega}_{15}$
$m^{\Omega}_1(\{4\}) = 0.255$; $m^{\Omega}_1(\{5\}) = 0.180$; $m^{\Omega}_1(\{3\}) = 0.180$; $m^{\Omega}_1(\Omega) = 0.385$.
Cette bba représente le vote (4 *) donné par E_1.

3.2 Distance entre le vote de l'évaluateur actuel et la combinaison de tous les autres votes

Afin d'évaluer le vote fourni par chaque évaluateur, nous l'avons comparé à tous les autres votes comme suit :
Pour chaque évaluateur, nous combinons tous les autres votes représentés par m^{Ω}_i en utilisant la règle de combinaison CWAC (Eq. 8), choisie pour sa capacité à gérer le conflit dans les différents votes. Le résultat de cette opération est une fonction de masse, notée m^{Ω}_{ci} qui représente la combinaison de tous les autres votes donnés par les évaluateurs sauf celui de l'évaluateur courant i. Cette masse est représentée comme suit :
$m^{\Omega}_{ci} = m^{\Omega}_1 \circledleftrightarrow m^{\Omega}_2 \circledleftrightarrow \ldots \circledleftrightarrow m^{\Omega}_{i-1} \circledleftrightarrow m^{\Omega}_{i+1} \circledleftrightarrow \ldots \circledleftrightarrow m^{\Omega}_N$.
Ensuite, nous calculons la distance $d(m^{\Omega}_i, m^{\Omega}_{ci})$ en utilisant la distance de Jousselme (Eq. 5), afin de mesurer la similarité entre le vote courant et tous les autres.

Exemple 5. Nous continuons avec l'Exemple 4 où nous combinons en utilisant la règle CWAC tous les votes des différents évaluateurs, sauf le premier : $m^{\Omega}_{c1} = m^{\Omega}_2 \circledleftrightarrow m^{\Omega}_3 \circledleftrightarrow m^{\Omega}_4 \circledleftrightarrow m^{\Omega}_5$.
$m^{\Omega}_{c1}(\emptyset) = 0.16$; $m^{\Omega}_{c1}(\{1\}) = 0.04$; $m^{\Omega}_{c1}(\{2\}) = 0.25$; $m^{\Omega}_{c1}(\{3\}) = 0.15$; $m^{\Omega}_{c1}(\{4\}) = 0.25$; $m^{\Omega}_{c1}(\{5\}) = 0.15$.
Ensuite, nous appliquons la distance de Jousselme entre le vote du premier évaluateur et tous les autres : $d(m^{\Omega}_1, m^{\Omega}_{c1}) = 0.155$.

3.3 Construction d'une nouvelle fonction de masse identifiant les vrais des faux avis

La distance mesurée à l'étape précédente représente le degré de compatibilité entre le vote et tous les autres, ce qui signifie que plus la valeur de la distance diminue plus le vote est consensuel. Donc, nous proposons de transformer chaque distance en une nouvelle bba, définie sur $\Theta = \{f, \bar{f}\}$ avec f = faux et $\bar{f}$ =

vrai, à travers l'équation suivante :

$$\begin{cases} m^{\Theta}(\{f\}) = \gamma * \frac{1}{1+e^{-a.ds+\frac{a}{2}}} \\ m^{\Theta}(\{\bar{f}\}) = \gamma * (1 - \frac{1}{1+e^{-a.ds+\frac{a}{2}}}) \\ m^{\Theta}(\Theta) = 1 - \gamma \end{cases} \quad (12)$$

avec $ds = d(m_i^{\Omega}, m_{ci}^{\Omega})$, $\gamma = \frac{\text{L'écart-type qui représente tous les votes}}{\text{La valeur maximale de l'écart-type}}$ et $a = 10$ où a correspond à la pente au point d'inflexion. En prenant l'équation $-ax + a/2 = 0$ cela permet que le point d'inflexion se trouve à $x = 0.5$.

Exemple 6. Nous transformons la distance de Jousselme $d(m_1^{\Omega}, m_{c1}^{\Omega})$ calculée dans l'Exemple 5 en une nouvelle bba avec $\Theta = \{f, \bar{f}\}$, nous obtenons : $m^{\Theta}(\{f\}) = 0.018$; $m^{\Theta}(\{\bar{f}\}) = 0.562$; $m^{\Theta}(\Omega) = 0.42$.

3.4 La prise de décision

Le processus de décision effectué dans cette dernière étape est assuré par la probabilité pignistique $BetP$ (Eq. 9). La $BetP$ avec la plus grande valeur est considérée comme la décision finale.

Exemple 7. Après avoir calculé la probabilité pignistique de la bba calculé dans l'Exemple 6, nous trouvons : $BetP(\{f\}) = 0.227$; $BetP(\{\bar{f}\}) = 0.773$.

Ainsi, nous concluons que le vote donné par le premier évaluateur est un vote authentique.

4 Expérimentation

Dans la détection de fausses opinions, l'évaluation est l'un des problèmes les plus difficiles en raison de l'indisponibilité des bases de données étiquetées puisqu'il n'est pas évident de distinguer les faux avis des vrais. Ainsi, les chercheurs ont utilisé l'évaluation humaine dans la plupart des travaux antérieurs. Cependant, l'évaluation humaine reste subjective puisque les différents évaluateurs ont souvent des niveaux de tolérance différents. Dans cet article, nous proposons d'étudier le comportement de notre méthode en utilisant les exemples numériques et de l'évaluer à l'aide de quatre bases de données artificielles.

4.1 Comportement de la méthode DFAE

Nous proposons de valider le comportement de notre méthode DFAE à travers quelques exemples numériques.

La figure 1 représente les résultats obtenus en utilisant quatre exemples différents qui sont détaillés dans le tableau 2, où les examinateurs évaluent un hôtel en donnant une note globale à travers les étoiles (notées * dans le tableau 2). Nous proposons deux cas standards (Exemple 3 et 4) et deux cas particuliers (Exemple 1 et 2) dans lesquels la majorité des votes est répartie sur 5 classes pour l'un et sur 2 classes pour l'autre. Nous constatons que notre méthode donne des résultats logiques dans les différents cas.

Tableau 2 – Descriptions et résultats des exemples numériques

Les exemples numériques	Opinions		Faux avis	Vrais avis
	Les étoiles	Le nombre d'évaluateurs		
Exemple 1	5* 4* 3* 2* 1*	5 5 5 5 5	-	5*, 4*, 3*, 2* et 1*
Exemple 2	5* 4*	5 5	-	5* et 4*
Exemple 3	4* 5* 3* 2* 1*	4 2 2 1 1	2* et 1*	4*, 5* et 3*.
Exemple 4	5* 4* 3* 2* 1*	4 0 1 4 7	5* et 3*	1* et 2*

4.2 Évaluation de la méthode DFAE

Pour évaluer notre approche, nous proposons de créer quatre bases de données artificielles dans lesquelles les évaluateurs donnent un vote

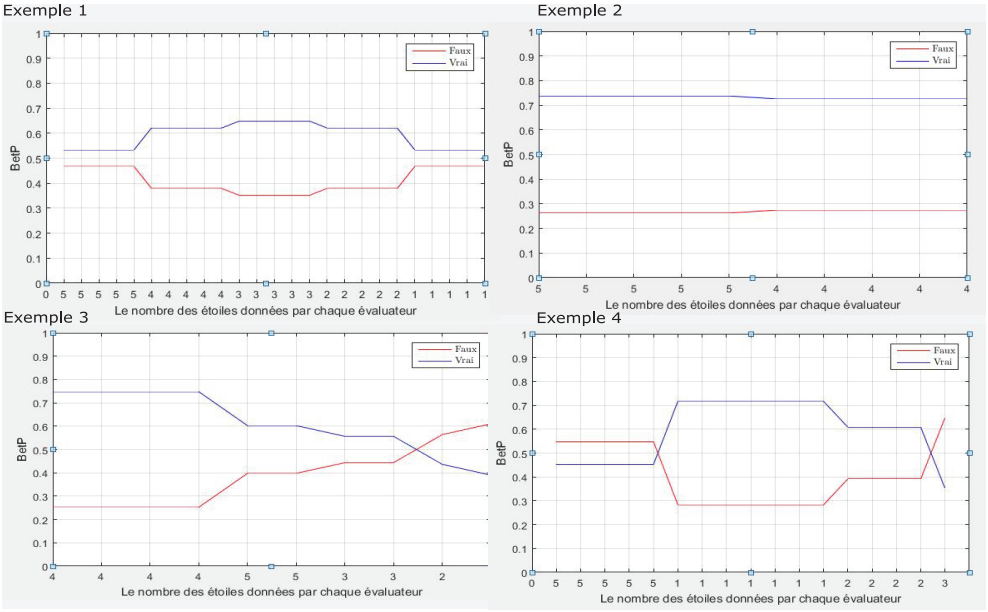

Figure 1 – Les résultats des exemples numériques

global pour évaluer quatre hôtels différents. Dans ces bases, des étiquettes ”vraies” seront données pour les avis majoritaires et des étiquettes ”fausses” seront associées aux avis minoritaires. Le tableau 3 présente la description et l'étiquetage de ces différentes bases de données.

Afin d'évaluer les performances de notre approche, nous avons utilisé le taux de bonne classification ”Correct Classification Rate (CCR)” qui est défini comme le rapport entre le nombre d'instances bien classées et le nombre total d'instances :

$$\text{CCR} = \frac{\text{Le nombre d'instances bien classées}}{\text{Le nombre total d'instances classées}} \quad (13)$$

Nous nous comparons avec la méthode du vote majoritaire qui est une méthode de décision binaire qui sélectionne des alternatives majoritaires. Le tableau 4 présente les résultats obtenus, en terme de CCR, sur les quatre bases de données avec la méthode du vote majoritaire et notre méthode de détection de faux avis DFAE.

Tableau 3 – Description des bases de données artificielles

Bases	Opinion		étiqueté faux	étiqueté vrai
	Les étoiles	Le nombre d'évaluateurs		
Base1 : 220 instances	5* 4* 3* 2* 1*	60 90 50 10 10	1*, 2* : 20 instances	5*, 4*, 3* : 200 instances
Base2 : 430 instances	5* 4* 3* 2* 1*	105 140 105 40 40	1*, 2* : 80 instances	5*, 4*, 3* : 350 instances
Base3 : 270 instances	5* 4* 3* 2* 1*	100 10 10 0 150	4*, 3*, 2* : 20 instances	5*, 1* : 250 instances
Base4 : 265 instances	5* 4* 3* 2* 1*	15 10 0 100 140	5*, 4*, 3* : 25 instances	1*, 2* : 240 instances

Tableau 4 – CCR (MV vs. DFAE)

Les bases	CCR MV	CCR DFAE
Base1	0.49	0.90
Base2	0.51	0.81
Base3	0.59	0.91
Base4	0.59	0.95

Nous remarquons que notre méthode obtient,

sur les différentes bases qui illustrent divers cas, des taux de classification élevés compris entre 81% et 95% alors que ceux du vote majoritaire sont compris entre 49% et 59%.
Cela démontre que notre méthode donne de meilleurs résultats en comparaison de ceux obtenus avec le vote majoritaire avec un écart qui peut atteindre 41%.

5 Conclusion

Dans cet article, nous avons abordé le problème de la détection de fausses opinions dans un contexte incertain en utilisant la théorie des fonctions de croyance. Nous avons proposé une méthode capable de gérer l'incertitude au niveau des votes globaux et de les évaluer en les comparant à tous les autres. Ainsi, notre méthode montre son efficacité pour distinguer les vrais avis des faux. De plus, cette approche peut être appliquée dans plusieurs domaines tels que le *e*-commerce et le *e*-business. Pour les travaux futurs, nous pouvons étendre notre méthode avec l'intégration d'autres notions comme la fiabilité du magasin à travers l'utilisation d'autres métadonnées. Nous pouvons également prendre en considération les différents indicateurs de spam ainsi que les aspects sémantiques à travers l'analyse du contenu des revues. Par ailleurs, nous pourrons comparer notre approche avec le rejet d'un avis selon son écart à la moyenne.

Références

[1] L. Akoglu, R. Chandy, C. Faloutsos, C. Opinion fraud detection in online reviews by network effects. *Proceedings of the Seventh International Conference on Weblogs and Social Media (ICWSM), 2013*, 13, pp. 2-11.

[2] S. Banerjee, A. Y. K. Chua. Applauses in hotel reviews : Genuine or deceptive ? *Proceedings of science and information conference (SAI), 2014*, pp. 938-942.

[3] X. Deng, R. Chen. Sentiment analysis based online restaurants fake reviews hype detection. *Web Technologies and Applications, 2014*, pp. 1-10.

[4] A. P. Dempster. Upper and lower probabilities induced by a multivalued mapping. *The annals of mathematical statistics, 1967*, pp. 325-339.

[5] E. Lefèvre, Z. Elouedi. How to preserve the confict as an alarm in the combination of belief functions ? *Decision Support System*, 56 : 326-333, 2013.

[6] S. Fayazbakhsh, J. Sinha. Review spam detection : A network-based approach. *Final Project Report* CSE 590, Data Mining and Networks, 2012.

[7] G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, R. Ghosh. Exploiting burstiness in reviews for review spammer detection. *Proceedings of the Seventh international AAAI conference on weblogs and social media, 2013*, 13, pp. 175-184.

[8] D. H. Fusilier, M. M. Montes-y-Gómez, P. Rosso, R. G. Cabrera. Detection of opinion spam with character n-grams. *Computational linguistics and intelligent text processing, 2015*, pp. 285-294.

[9] A. Heydari, M. Tavakoli, Z. Ismail, N. Salim. Leveraging quality metrics in voting model based thread retrieval. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 10 (1) : 117-123, 2016.

[10] A.-L. Jousselme, D. Grenier, É. Bossé. A new distance between two bodies of evidence. *Inf. Fusion* 2(2) : 91-101, 2001.

[11] N. M. Kolhe, M. M. Joshi,A. B. Jadhav, P. D. Abhang. Fake reviewer groups detection system. *Journal of Computer Engineering (IOSR-JCE)*, 16(1) : 06-09, 2014.

[12] A. Mukherjee, A. Kumar, B. Liu, J. Wang, M. Hsu, M. Castellanos. Spotting opinion spammers using behavioral footprints. *Proceedings of the ACM international conference on knowledge discovery and data mining, 2013*, pp. 632-640.

[13] T. Ong, M. Mannino, D. Gregg. Linguistic characteristics of shill reviews. *Electronic Commerce Research and Applications*, 13 (2) : 69-78, 2014.

[14] D. Savage, X. Zhang, X. Yu, P. Chou, Q. Wang. Detection of opinion spam based on anomalous rating deviation. *Expert Systems with Applications*, 42 (22) : 8650-8657, 2015.

[15] G. Shafer. A mathematical theory of evidence.*Vol. 1. Princeton : Princeton university press*, 1976.

[16] K. Sharma, K. I. Lin. Review spam detector with rating consistency check. *Proceedings of the 51st ACM southeast conference, 2013*.

[17] P. Smets. The transferable belief model for quantified belief representation. *Proceedings of the Quantified Representation of Uncertainty and Imprecision, 1998*, pp. 267-301.

[18] P. Smets. The combination of evidence in the transferable belief model. *Proceedings of IEEE Transactions on pattern analysis and machine intelligence, 1990*, pp. 447-458.

[19] G. Wang, S. Xie, B. Liu, P. S. Yu. Review graph based online store review spammer detection. *Proceedings of 11th international conference on data mining (ICDM), 2011*, pp. 1242-1247.

[20] H. Xue, F. Li, H. Seo, R. Pluretti. Trust-aware review spam detection. *Proceedings of IEEE Trustcom/BigDataSE/ISPA, 2015*, pp. 726-733.