Spammers detection based on reviewers' behaviors under belief function theory

Malika Ben Khalifa, Zied Elouedi, Eric Lefevre

Spammers detection based on reviewers' behaviors under belief function theory

Malika Ben Khalifa[1,2], Zied Elouedi[1], and Eric Lefèvre[2]

[1] Université de Tunis, Institut Supérieur de Gestion de Tunis, LARODEC, Tunisia
malikabenkhalifa2@gmail.com, zied.elouedi@gmx.fr
[2] Univ. Artois, EA 3926, Laboratoire de Génie Informatique et d'Automatique de l'Artois (LGI2A), Béthune, F-62400, France
eric.lefevre@univ-artois.fr

Abstract. Nowadays, we note the dominance of the online reviews which become an essential factor in customers' decision to purchase a product or service. Driven by the immense financial profits from reviews, some corrupt individuals or organizations deliberately post fake reviews to promote their products or to demote their competitors' products, trying to mislead or influence customers. Therefore, it is crucial to spot these spammers in order to detect the deceptive reviews, to protect companies from this harmful action and to ensure the readers confidence. In this way, we propose a novel approach able to detect spammers and to accord a spamicity degree to each reviewer relying on some spammers indicators while handling the uncertainty in the different inputs through the strength of the belief function theory. Tests are conducted on a real database from Tripadvisor to evaluate our method performance.

Keywords: Online reviews, Spammers, Fake reviews, Uncertainty, Belief function theory.

1 Introduction

Online reviews are becoming more prevalent nowadays due to the huge use of social media, opinion-sharing websites, blogs, forms and merchant websites. Consumers rely heavily up on reviews posted on these websites when making decisions about which products or services to purchase online. However, reviews are more than just a way for customers to gather information, but also a powerful source information for companies since positive opinions bring significant financial gains for business and individuals. Moreover, negative reviews not only cause financial loss, but also damage the companies e-reputation. Unfortunately, all this gives an important incentive for fake reviews.
So driven by the desire of profit, spammers create fake reviews and posted them everywhere in order to mislead readers, to influence their decisions and to manipulate their opinion mining. Opinions spam may be positive to promote some companies or negative, to their competitive companies, in order to demote them. These review spamming activities make the products and the services identification confusing and complicated. We believe also that more online reviews are

used, more spammers will increase and will post more and more deceptive reviews. The spammer detection becomes an essential task since it allows us to stop the appearance of fake opinions. Several methods addressed this problem [5, 9], most of them are graph based approaches. The first study [16] proposes a heterogeneous graph model with three types of nodes to define relations between reviewers, reviews, and store. This method used the interrelationship between three based concepts namely; the trustworthiness of reviewers, the honesty of reviews, and the reliability of stores to generate a ranking list of suspicious reviews and reviewers. However, its level of precision amounts to 49% in the fake reviews detection. A similar approach elaborated by authors in [3] which also used a review graph. This method calculated a suspicion score for each node in the review graph and then used an iterative algorithm in order to update these scores based on the graph connectivity. This method has higher precision with respect of the conformity along the human judgments. The third graph based approach was elaborated by Akoglu et al. [1], introduced through a bipartite network. The authors proposed a signed inference algorithm for extending loopy belief propagation (LBP). The output of this algorithm is a list of users ranked by score to get clusters with k reviewers and products. This method was compared to two iterative classifiers, where it succeeded in detecting fraudulent users and spot their fake product ratings. Lim et al. [6] were the first use behavioral indicators of deceptive reviews to spot spammers. Their proposed method is based on the behavior scoring technique for ranking reviewers by measuring the spamming behaviors. The human judgment is used for the evaluation. As a result, the rating of the target products alternated adequately by removing the most suspicious reviews. Since then, behavioral indicators have become an important basis for spammer detection task. In this way, researchers in [8] proposed a method to exploit observed reviewing behaviors in order to detect opinion spammers using a Bayesian inference framework. Moreover, authors in [4] developed an algorithm in order to detect burst patterns in reviews for a specific product. It generated five new spammer behavior features as indicators to used them in review spammer detection. Two types of evaluation are performed: supervised classification and human evaluation. These techniques achieve significant results thanks to the spammers behavior features. Most of these approaches rely on different human evaluators and experts to annotate their data evaluation. Moreover, each method is based on various inputs and aspects. All this won't allow for a safe comparison in this field. In addition, these techniques exhibit some weaknesses fundamentally related to their inability to manage the uncertainty of different reviewers and in reviews information which are often imperfect and imprecise. Ignoring such uncertainty may deeply affect the detection. That is why, treating the uncertainty when dealing with the fake reviewers detection task becomes a widespread interest.

In this paper, we propose a novel method that aims to detect spammers based on the reviewer behavior characteristics under the belief function framework. It is known as a rich tool able to manage several pieces of imperfect information, to combine them, besides taking into account the reliability in the different sources

providing them, and making decision under uncertainty. Hence, our approach involves imperfections in the different inputs to spot the spammers and offers also an uncertain output. This latter represents the spamicity degree according to each reviewer in order to identify its reliability.
The remainder of the paper is structured as follows: We firstly present the belief function theory basic fundamentals in Section 2. Then, Section 3 elucidates our proposed approach. After that, we discuss the experimental results in Section 4. Finally, a conclusion and some future works are described in Section 5.

2 Belief Function Theory

The belief function theory is one of the useful theories that handles uncertain knowledge. It was introduced by Shafer [11] as a model to represent beliefs. It is considered as a powerful tool able to deal with uncertainty in different levels and to manage various types of imperfection.

2.1 Basic concepts

The frame of discernment Ω is a finite and exhaustive set of different events associated with a given problem, such set Ω is also called the universe of discourse, defined by:

$$\Omega = \{\omega_1, \omega_2 ..., \omega_n\} \tag{1}$$

The power set 2^Ω contains all possible hypotheses that formed the union of events, and the empty set $\emptyset$ which represents the conflict, defined by:

$$2^\Omega = \{A : A \subseteq \Omega\} \tag{2}$$

A basic belief assignment (*bba*) or a belief mass defined as a function from 2^Ω to $[0, 1]$ that represents the degree of belief given to an element A such that:

$$\sum_{A \subseteq \Omega} m^\Omega(A) = 1 \tag{3}$$

A focal element A is a set of hypotheses with positive mass value $m^\Omega(A) > 0$.
Several kinds of *bba*'s have been proposed [14] in order to express special situations of uncertainty. Here, we underline some special cases of *bba*'s:

- The certain *bba* represents the state of total certainty and it is defined as follows: $m^\Omega(\{\omega_i\}) = 1$ and $\omega_i \in \Omega$.
- The categorical *bba* has a unique focal element A different from the frame of discernment defined by: $m^\Omega(A) = 1$, $\forall A \subset \Omega$ and $m^\Omega(B) = 0$, $\forall B \subseteq \Omega$ $B \neq A$.
- Simple support function: In this case, the *bba* focal elements are $\{A, \Omega\}$. A simple support function is defined as the following equation:

$$m^\Omega(X) = \begin{cases} w & \text{if } X = \Omega \\ 1 - w & \text{if } X = A \text{ for some } A \subset \Omega \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

  Where A is the focus and $w \in$ [0,1].

2.2 Discounting

The discounting operation [7] allows us to update experts beliefs by taking into consideration their reliability through the degree of trust $(1-\alpha)$ given to each expert with $\alpha \in [0,1]$ is the discount rate.
When, the *bba* is defined on the set $\{reliable,\ not\ reliable\}$ such that [13]:

$$m(reliable) = 1-\alpha \quad and \quad m(not\ reliable) = \alpha \tag{5}$$

Accordingly, the discounted *bba*, noted ${}^{\alpha}m^{\Omega}$, m^{Ω} becomes:

$$\begin{cases} {}^{\alpha}m^{\Omega}(A) = (1-\alpha)m^{\Omega}(A) & \forall A \subset \Omega, \\ {}^{\alpha}m^{\Omega}(\Omega) = \alpha + (1-\alpha)m^{\Omega}(\Omega). \end{cases} \tag{6}$$

2.3 Combination Rules

Let m_1^{Ω} and m_2^{Ω} two *bba*'s representing two distinct sources of information defined on the same frame of discernment Ω. Various numbers of combination rules have been proposed in the framework of belief function. They were intended to aggregate a set of *bba*'s in order to get the fused information represented by one *bba*. In what follows, we elucidate those related to our approach.

1. *Conjunctive rule*
   It was settled in [15], denoted by $\textcircled{\cap}$ and defined as:
   $$m_1^{\Omega}\textcircled{\cap}m_2^{\Omega}(A) = \sum_{B\cap C=A} m_1^{\Omega}(B)m_2^{\Omega}(C) \tag{7}$$
2. *Dempster's rule of combination*
   This combination rule is a normalized version of the conjunctive rule [2]. This rule is characterized by a normalization factor denoted by K and it is defined as:
   $$(m_1^{\Omega} \oplus m_2^{\Omega})(A) = K.(m_1\textcircled{\cap}m_2^{\Omega}(A)) \tag{8}$$
   Where
   $$K^{-1} = 1 - (m_1^{\Omega}.\textcircled{\cap}m_2^{\Omega}(\emptyset)) \text{ and } (m_1^{\Omega} \oplus m_2^{\Omega})(\emptyset) = 0 \tag{9}$$

2.4 Decision process

Various solutions have been proposed to choose the most suitable decision for a given problem under the belief function framework. In this work, we adopt the pignistic probability proposed by the Transferable Belief Model [15]. Therefore, it is composed by two level models:

- The credal level where beliefs are defined by *bba*'s then combined.
- The pignistic level where *bba*'s are transformed into pignistic probabilities denoted by $BetP$ and defined as follows:

$$BetP(B) = \sum_{A\subseteq\Omega} \frac{|A\cap B|}{|A|} \frac{m^{\Omega}(A)}{(1-m^{\Omega}(\emptyset))} \quad \forall\ B \in \Omega \tag{10}$$

3 Spammers detection based on reviewers' behaviors under belief function theory

In this section, we elucidate our novel proposed method which deals with different important spammer indicators in an uncertain context through the belief function theory in order to distinguish between fake reviewers and genuine ones. Our method relies on the four most important spammer behaviors indicators namely; the reviewers average proliferation, the brust spamicity degree, the reviews helpfulness and the extreme rating providing by each reviewer.
Besides, we adopt the belief function theory to model uncertainty within those indicators. Each reviewer R_i will be represented by two mass functions (*bba*'s), the first one is to model the reviewer reputation $m^{\Omega}_{RR_i}$ and the second one is to represent the reviewer helpfulness m_{RH_i} with $\Omega = \{S, \overline{S}\}$ where S is spammer and $\overline{S}$ is non spammer. Our method follows four main steps detailed in-depth.

3.1 Step 1: Reviewer reputation

In the spammer review detection field, it has been proved that ordinary reviewers usually write their comments on several products in almost consistent patterns during different periods [5]. Generally, the genuine reviewers post their opinion when they have actually bought new products or used new services. It means that their reviews depend on the number of tested products or services and are also steadily given over time interval. However, spammers are excepted to post a huge number of reviews to limited intended products or services in short time span, say in two or three days. Consequently, these two indicators can construct the reviewer reputation.
In this way, we propose to examine the reviewing history for each reviewer $Hist_{R_i}$ defined as the set of all past reviews written by the reviewer R_i for n discrete products.
The average number of reviews per product is measured through the sum of different reviews given by each reviewer R_i and divided by the total number of reviewed products n. The reviewers average proliferation is calculated through the following equation:

$$AvgP(R_i) = \frac{Hist_{R_i}}{n} \tag{11}$$

If the $AvgP(R_i) > 3$, we can assume that the reviewer is suspicious to be a potential spammer since generally ordinary reviewers do not give more than three reviews per product. The reviewer reputation is then represented by a certain *bba* as follows:

$$m^{\Omega}_{RR_i}(\{S\}) = 1 \tag{12}$$

Else

$$m^{\Omega}_{RR_i}(\{\overline{S}\}) = 1 \tag{13}$$

Example 1. Let us consider the case of five reviewers, for which we have some information about their reviewing history, given an overall rating review for a hotel detailed in the Table 1.
We deal with the $Reviewer_{id} = 1$
So, we calculate the reviewers average proliferation:
$AvgP(R_1) = \frac{Hist_{R_1}}{n} = \frac{258}{30} = 8.6$
Then, we generate the corresponding *bba*:
$AvgP(R_1) > 3 \Rightarrow m^{\Omega}_{RR_1}(\{S\}) = 1$

Table 1. Hotel reviews and reviewers information

Review	Reviewer_id	Total number of reviews	Total number of product or services	Number of Extreme rating	Number of helpful votes	Number of reviews given in less than 3 days.
5*	1	258	30	208	100	200
4*	2	30	10	8	25	4
3*	3	20	12	0	18	2
5*	4	30	16	22	0	15
4*	8	100	92	10	88	10

Moreover, we propose to verify if the reviews are given in a short time of interval or are scattered during the reviewing history.
In our method, we fix the time interval to three days and we measure the brust spamicity degree α_i through the sum of the reviews' number given in less than three days divided by the total number of reviews by each reviewer denoted by TNR_i as follows:

$$\alpha_i = \frac{Number\ of\ reviews\ given\ by\ R_i\ in\ less\ than\ 3\ days}{TNR_i}. \tag{14}$$

Then, we weaken the reviewer reputation *bba* by each corresponding reliability degree (i.e., $(1 - \alpha_i)$ or α_i) using the discounting operation (Eq.6) in order to take into consideration the brust spamicity degree.
This discounted *bba* ${}^{\alpha}m^{\Omega}_{RR_i}$ represented the reviewer reputation using the reviewers average proliferation and the brust spamicity which are two important spammer indicators.

Example 2. We continue with the previous Example 1, we calculate the brust spamicity degree:
$\alpha_1 = \frac{200}{258} = 0.775$
α_1 is the reliability degree for S, hence we apply the discounting operation as

follows:
${}^{\alpha}m^{\Omega}_{RR_1}(\{S\}) = 1 * \alpha_1 = 1 * 0.775 = 0.775$
${}^{\alpha}m^{\Omega}_{RR_1}(\Omega) = (1 - \alpha_1) + \alpha_1 * 0 = 0.225$

3.2 Step 2: Reviewer helpfulness

The reviewer helpfulness is an important indicator to spot spammers. For this reason, we propose to verify if the reviewer post helpful reviews or unhelpful ones in order to mislead readers. Accordingly, we propose to use the Number of Helpful Reviews (NHR) to indicate the helpful ones associated to each reviewer. Therefore, if ($NHR_i = 0$), the reviewer is suspicious to be spammer, thus we model the reviewer helpfulness by a certain *bba*:

$$m^{\Omega}_{RH_i}(\{S\}) = 1 \tag{15}$$

Else

$$m^{\Omega}_{RH_i}(\{\overline{S}\}) = 1 \tag{16}$$

We propose to penalize the reviewer helpfulness mass by considering the non helpfulness degree for each reviewer R_i denoted by β_i.
So, we propose this discounting factor as follows:

$$\beta_i = \frac{TNR_i - NHR_i}{TNR_i} \tag{17}$$

Then, we use the discounting operation in order to update the *bba* into a simple support function ${}^{\beta}m^{\Omega}_{RH_i}$. Thus, we take into consideration the helpfulness degree.
Generally, customers are not totally satisfied by their consumed products or tested services. Therefore, the innocent reviewer will not usually post extreme rating. However, most spammers perpetually resort to extreme ratings [8], either highest (5*) or lowest (1*), in order to achieve their goal of rapidly raising or bringing down, respectively, the mean score of a product.
When the reviewer had a lot of helpful reviews but they are full of extreme rating, his chances of being genuine reviewer certainly decrease.
In order to take this fact into account, we calculate the extreme rating degree denoted γ_i, corresponding to each reviewer R_i, which is considered as the discounting factor calculated by the number of the extreme rating divided by the total number of reviews given by each reviewer TNR_i as the following equation:

$$\gamma_i = \frac{NER_i}{TNR_i} \tag{18}$$

Where, NER_i is the extreme reviews' number (i.e., $NER_i \in \{1, 5\}$) given by each reviewer R_i.
Then, each simple support function represented the reviewer helpfulness ${}^{\beta}m^{\Omega}_{RH_i}$ is weakened again by its relative reliability degree (i.e., $(1-\gamma_i)$ or γ_i) through the discounting operation.
Thus, this discounted ${}^{\beta\gamma}m^{\Omega}_{RH_i}$ modeled the reviewer helpfulness based on both the reviewer helpfulness degree and extreme ranting.

Example 3. Let us consider the same Example 1:

- The reviewer helpfulness *bba* corresponding to R_1 is generated as follows:
  Number of helpful reviews$= 100 > 0 \Rightarrow m^{\Omega}_{RH_1}(\{\overline{S}\}) = 1$

- Then, we calculate the corresponding helpfulness degree:
  $\beta_1 = \frac{258-100}{258} = 0.612$

- β_1 is the discounting factor $\overline{S}$ and its reliability degree is $(1-\beta_1)$. So, we apply the discounting operation as follows:
  ${}^{\beta}m^{\Omega}_{RH_1}(\{\overline{S}\}) = 1 * (1-\beta_1) = 0.388$
  ${}^{\beta}m^{\Omega}_{RH_1}(\Omega) = \beta_1 + (1-\beta_1) * 0 = 0.612$

- After that, we calculate the extreme rating degree for R_1:
  $\gamma_1 = \frac{208}{258} = 0.806$

- γ_1 is the discounting factor $\overline{S}$ and its reliability degree is $(1-\gamma_1)$. So, we reapply the discounting operation as follows:
  ${}^{\gamma\beta}m^{\Omega}_{RH_1}(\{\overline{S}\}) = 0.388 * (1-\gamma_1) = 0.388 * (1-0.806) = 0.075.$
  ${}^{\gamma\beta}m^{\Omega}_{RH_1}(\Omega) = \gamma_1 + (1-\gamma_1) * 0.612 = 0.925.$

3.3 Step 3: Modeling the whole reviewer trustworthiness

In the interest of representing the whole trustworthiness for each reviewer, we aggregate the reviewer *bba*'s reputation ${}^{\alpha}m^{\Omega}_{RR_i}$ with his helpfulness *bba* ${}^{\beta\gamma}m^{\Omega}_{RH_i}$ using the Dempster combination rule (i.e, $m^{\Omega}_{RT_i} = {}^{\alpha} m^{\Omega}_{RR_i} \oplus {}^{\beta\ \gamma}m^{\Omega}_{RH_i}$).

The output of this aggregation is a combined *bba* $m^{\Omega}_{RT_i}$ that represents the whole trustworthiness for each reviewer.

Example 4. Once the *bba*'s representing both the R_1 reputation and helpfulness, calculated in the previous example, are combined we obtain the following *bba*:
$m^{\Omega}_{RT_1}(\{S\}) = 0.761$
$m^{\Omega}_{RT_1}(\{\overline{S}\}) = 0.018$
$m^{\Omega}_{RT_1}(\Omega) = 0.221$

3.4 Step 4: According Spamicity degree and Making decision

In order to accord a spamicity degree to each reviewer, we resort the pignistic probability $BetP$. Then, the decision is made either the author is a spammer or innocent as we select the $BetP$ with the greater value as the final decision.

Example 5. After applying the pignistic probability on the *bba* calculated in the previous Example 4 and, we found:
$BetP(\{S\}) = 0.872$
$BetP(\{\overline{S}\}) = 0.128$
The reviewer R_1 is a spammer with a spamicity degree equal to 0.872.

4 Experimentation and Results

The evaluation in spam reviews detection problem has been always a significant barrier, due to the absence of true real world growth data. A common alternative, used by various previous works, is using human evaluators and experts in order to label the dataset. However, the human judgement may provide varying verdicts due to the variability in perception and tolerance without forgetting the human subjectivity.
In this paper, we conducted experiments on real dataset then we propose to validate our method behavior by analyzing some results.

4.1 Evaluation protocol

Dataset description
In order to evaluate our method, we used a real world dataset extracted from Tripadvisor which is composed by 6200 reviews given by 1420 reviewers. The dataset contains; the reviews, the reviewed restaurants or hotels and the reviewing historic corresponding to each reviewer which is detailed in the Table 2. We

Table 2. Example of reviewer history

The reviewer_id
Total number of reviewed restaurants and hotels
Total number of reviews
The review rating
The review time
Number of helpful ratings

propose to label our database through one of the most used clustering method K-means where $K = 2$ in order to divide it into two classes; spammer and non spammer, relying on some important features used in the literature [4] such as:

- Duplicate/Near Duplicate Reviews
- Extreme Rating
- Reviewing Burstiness
- The helpfulness degree
- The average mean rating given by each reviewer

Evaluation Criteria
We evaluate our method according to the three following criteria: Accuracy, precision and recall and they can be defined as Eqs.19, 20, 21 respectively where TP, TN, FP, FN denote True Positive, True Negative, False Positive and False Negative respectively.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{19}$$

$$Precision = \frac{TP}{(TP + FN)} \tag{20}$$

$$Recall = \frac{TP}{(TP + FN)} \tag{21}$$

Experimental results
Our method distinguishes between 229 spammers and 1266 genuine reviewers. We propose to compare it with state-of-art baselines classifier; the Support Vector Machine SVM and the Naive Bayes NB [5, 8, 16]. The results are reported in the table 3.

Table 3. Comparative results

Methods	Accuracy	Precision	Recall
SVM	0.72	0.71	0.70
NB	0.67	0.64	0.59
Our Method	**0.98**	**0.96**	**0.94**

Our approach accomplishes the best performance according to accuracy, precision and recall over-passing state-of-art methods. It records at best an accuracy improvement over 30% compared to NB and over 26% compared to SVM.

4.2 Method behavior validation

In order to analyze our results, we randomly pick a set of ten reviewers from our Tripadvisor dataset. Table 4 details the reviewers information and presents the results generated by our approach. Our method classifies each reviewer as spammer or innocent by according a spamicity degree to each one.
The $reviewer_{id} = 21012Z$ is detected as a spammer with a high spamicity degree

(i.e.,0.91) since he gives various non helpful reviews to some target products in short time interval including a lot of extreme rating in order to over-qualify or to damage them. However, the $reviewer_{id} = 10001E$ is classified as innocent with a very low spamicity degree as his reviews contain various helpful ones and few extreme rating. Moreover, they are spread along the reviewing time interval and each one is given to only one product. Taking also the $reviewer_{id} = 10012B$, almost this one is judged as innocent, he has a high spamicity degree (i.e., 0.47) because most of his reviews are given in less than three days including also some extreme rating, however we can not classified as spammer since he also has several helpful vote and he gives average less than two reviews per product.
Our method can be used in several fields by different reviews websites. In fact, these websites must block the detected spammers in order to stop the appearance of the fake reviews. Moreover and thanks to our uncertain output, they can control the behavior of the innocent ones with a high spamicity degree to prevent their tendency to turn into spammers.

Table 4. Reviewers information and results

Reviewer_id	Total number of reviews	Total number of product or services	Number of Extreme rating	Number of helpful vote	Number of reviews given in less than 3 days.	**Decision**	**Spamicity Degree**
10012D	258	30	208	100	100	Spammer	0.87
10013D	30	10	8	25	4	Innocent	0.02
10021D	20	12	0	18	2	Innocent	0.11
10010A	30	16	22	0	15	Spammer	0.68
10012B	16	12	6	10	9	Innocent	0.47
20012D	40	30	5	32	5	Innocent	0.02
18012B	30	3	25	0	28	Spammer	0.99
21012Z	60	5	20	2	50	Spammer	0.91
10412E	100	92	10	88	10	Innocent	0.01
10001E	150	150	10	120	15	Innocent	0.01

5 Conclusion

In this work, we addressed the spammer review detection problem and proposed a novel approach that manages the uncertainty while using the spammer behavior indicators. Our method shows its ability in distinguishing between fake and innocent reviewers while tuning a spamicity degree for each one. As future work, we aim to improve even more our detection by taking into account the semantic aspects through the analysis of the reviews contents.

References

1. Akoglu, L., Chandy, R., Faloutsos, C.: Opinion fraud detection in online reviews by network effects. Proceedings of the Seventh International Conference on Weblogs and Social Media, ICWSM, 13, 2-11 (2013)
2. Dempster, A.P.: Upper and lower probabilities induced by a multivalued map- ping. Ann. Math. Stat.38, 325-339 (1967)
3. Fayazbakhsh, S., Sinha, J.: Review spam detection: A network-based approach. Final Project Report: CSE 590 (Data Mining and Networks) (2012)
4. Fei, G., Mukherjee, A., Liu, B., Hsu, M., Castellanos, M., Ghosh, R.: Exploiting burstiness in reviews for review spammer detection. In Seventh international AAAI conference on weblogs and social media, 13, 175-184 (2013)
5. Heydari, A., Tavakoli, M., Ismail, Z., Salim, N.: 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)
6. Lim, P., Nguyen, V., Jindal, N., Liu, B., Lauw, H. : Detecting product review spammers using rating behaviors. Proceedings of the 19th ACM international conference on information and knowledge management, 939-948 (2010)
7. Ling, X., Rudd, W.: Combining opinions from several experts. Applied Artificial Intelligence an International Journal, 3 (4), 439-452 (1989)
8. Mukherjee, A., Kumar, A., Liu, B., Wang, J., Hsu, M., Castellanos, M.: Spotting opinion spammers using behavioral footprints. Proceedings of the ACM international conference on knowledge discovery and data mining, 632-640 (2013)
9. Pan, L., Zhenning, X., Jun, A., Fei, W.: Identifying indicators of fake reviews based on spammers behavior features. Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 396-403 (2017)
10. Savage, D., Zhang, X., Yu, X., Chou, P., Wang, Q.: Detection of opinion spam based on anomalous rating deviation. Expert Systems with Applications, 42 (22), 8650-8657 (2015)
11. Shafer, G.: A Mathematical Theory of Evidence, vol. 1. Princeton University Press (1976)
12. Smets, P.: The combination of evidence in the transferable belief model. IEEE Trans. Pattern Anal. Mach. Intell. 12(5), 447-458 (1990)
13. Smets, P.: The transferable belief model for expert judgement and reliability problem. Reliability Engineering and system safety, 38, 59-66 (1992)
14. Smets, P.: The canonical decomposition of a weighted belief. Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence, 1896-1901 (1995)
15. Smets, P.: The transferable belief model for quantified belief representation. In: Smets, P. (ed.) Quantified Representation of Uncertainty and Imprecision, pp. 267-301. Springer, Dordrecht (1998)
16. Wang, G., Xie, S., Liu, B., Yu, P. S.: Review graph based online store review spammer detection. Proceedings of 11th international conference on data mining (icdm), 1242-1247 (2011)