Evidential Spammers and Group Spammers Detection

Malika Ben Khalifa, Zied Elouedi, Eric Lefevre

Evidential Spammers and Group Spammers Detection

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, UR 3926, Laboratoire de Génie Informatique et d'Automatique de l'Artois (LGI2A), Béthune, F-62400, France
eric.lefevre@univ-artois.fr

Abstract. The online success of the brands, products or services depends upon the online reviews written by the consumers to share their experiences. These reviews deeply affect the buying decision of the new customers. For the purpose of performing their e-reputation, some companies rely on spammers to involve fraud reviews with the aim of gaining more profit. They can work individually or collaborate together to post various fake reviews trying to promote or demote target companies or product. These spammers and the group of spammers mislead the readers which make the e-commerce unsafe domain. To deal with this issue, we propose a new method having the objective to detect the spammers while taking into account both the group spammers and the individual spammers indicators. Our proposed method relies on the K-nearest neighbors algorithm under the belief function theory in order to handle the uncertainty in both the spammers and the group spammers indicators. Experiments are conducted on two labeled real datasets extracted from Yelp.com where our method achieves significant results.

Keywords: Fake reviews, Spammers, Group spammers, Uncertainty, Belief Function Theory, EK-NN, E-commerce.

1 Introduction

In recent years, e-commerce has become one of the most important sources that manipulate the economy of the world. Furthermore, with the COVID-19 epidemic and with the successive confinements, the online purchase has become the only solution to buy the different products due to the closure of the stores. Since the products and services are represented only by a description and photos, the customers rely mainly on both the rating score and the reviews representing the opinion of the consumers regarding the products or services. Thus, brands and companies aim to improve the quality of the reviews by posting positive fake reviews and also negative ones to destruct their competitors. Therefore, they rely on the spammers to practise these misleading activities. These spammers are considered as the most harmful generator source of fake reviews. Hence, detecting spammers becomes pivotal to save e-commerce and to ensure fair competition

between brands and companies [7]. This challenging problem attracts significant researchers who have proposed different methods to spot fake reviews. These contributions can be grouped in three categories [11]: review spam detection based on the reviews contents and linguistic features, spammer detection and group spammer detection. The spammer detection methods can be classified in two global categories: methods based on graph and others based on behavioral indicators. The main graph based methods were proposed in [8, 20]. These methods do not achieve a very good performance.
Moreover, another approach introduced in [15] relies also on the rating behavior of each reviewer. One of the most preferment studies was proposed in [9] to detect the burst pattern in reviews given to some specific products or services. This approach generates five new spammer behavior indicators to ameliorate the review spammer detection. This method achieves 83.7% of precision thanks to the spammers behaviors indicators. Since then, behavioral indicators have become an important basis for spammer detection task. In this way, Rayana and Akoglu [16] proposed a novel framework called SpEagle that relies on conjointly relational data and the spammers indicators to identify deceptive reviewers and reviews, as well as the spam target products. The SpEagle framework significantly outperforms various baselines and state-of-the-art approaches. Moreover, Fontanarava et al. [10] proposed and evaluated some new features.
Furthermore, spammers work individually or more they can also collaborate together to create the group spammers in order to magnify the effect of review manipulation. The group spammers can even be more dangerous than the individual spammer thanks to their potential to deviate the overall rating and representing the majority of the reviews in a short time. Thus, recently there were increasingly research interests in group spamming detection aspects. The first study, in this aspect, was proposed by Mukherjee et al. [12]. This method relies on the Frequent Itemset Mining (FIM) technique in order to generate review spammers groups. It models the reviewers as items and the products as transactions. By applying the FIM and initializing the minimum support count to 3, they can spot at least 2 reviewers, while each reviewer reviews at least 3 common products. The majority of the group spammer methods [13, 21] relies on the FIM technique and proposes different frameworks to evaluate the spamming of each candidate spammer groups. Some other recent works, in this aspect, do not rely on the FIM techniques such in [22] but on the structure of the reviewer graph. This work also achieves significant results.
The fake reviews detection problem can be considered as one of the uncertain challenging issues due to the ambiguity provided by the spammers and the group spammers to mislead the detection systems. Nevertheless, the previous proposed methods did not take into consideration the uncertain aspect while trying to detect the spammers or the group spammers. The negligence of this uncertainty can severely affect the detection quality. That's why, we have proposed different methods that deal with uncertainty while distinguishing between fake and genuine reviews [1, 2]. Among these methods, we have proposed a method to detect spammers, in which we use the Evidential K-Nearest Neighbors classifier

(EK-NN) while taking into account the spammers' indicators [3]. Another one to detect group spammers basing on the group spammers' indicators and the EK-NN as well [4]. These methods achieve good results. Since, we think that the reviewer can be classified as not spammer through the spammers' indicators for lack of historical information. In this case, the spammer behavior cannot be significant. However, this reviewer can belong to a suspicious group thus he can be spotted through the group spammers' indicators. Aims at this, a reviewer can be classified as not spammer since he does not belong to any group of spammers but he can be detected as spammer thanks to the spammers' indicators. Thus and with the aim of improving detection, we propose a novel approach to spot fake reviewers which takes into account both the spammers and the group spammers' indicators while managing the uncertainty. To the best of our knowledge, this method will be the first which combines both the spammers and the group spammers aspects to perform the detection.
This paper is organised as follows. We present the fundamentals of the belief function framework in section 2. In section 3, we detail our proposed approach and we consecrate section 4 from the experimental study, then we end up with a conclusion and some future work.

2 Belief function theory

In section, we present the fundamentals of the belief function theory used in our method.

2.1 Basic concepts

The belief function theory, one of the powerful theories handling uncertainty, was introduced by Shafer [17] as a model to manage beliefs. In this theory, a given problem is represented by a finite and exhaustive set of different events called the frame of discernment Ω. 2^Ω is the power set of Ω that includes all possible hypotheses and it is defined by: $2^\Omega = \{A|A \subseteq \Omega\}$.
A basic belief assignment (*bba*) named also a belief mass represents the degree of belief given to an element A. It is defined as a function m^Ω from 2^Ω to $[0, 1]$ such that:

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

A focal element A is a set of events having a strictly positive mass value $m^\Omega(A) > 0$.

2.2 Dempster's rule of combination

Let m_1^Ω and m_2^Ω two *bba*'s modeling two distinct sources of information defined on the same frame of discernment Ω.
The Dempster combination rule is introduced in [5], denoted by $\oplus$ and defined as:

$$m_1^\Omega \oplus m_2^\Omega(C) = \begin{cases} \frac{\sum_{A \cap B = C} m_1^\Omega(A) m_2^\Omega(B)}{1 - \sum_{A \cap B = \emptyset} m_1^\Omega(A) m_2^\Omega(B)} & \text{if} \quad C \neq \emptyset, \forall C \subseteq \Omega, \\ 0 & otherwise. \end{cases} \tag{2}$$

2.3 Vacuous extension

Frequently, we need to aggregate two $bba's$ $m_1^{\Omega_1}$ and $m_2^{\Omega_2}$ that have different frames of discernment. Thus, we rely on the vacuous extension which extends the frames of discernment Ω_1 and Ω_2, corresponding to the mass functions $m_1^{\Omega_1}$ and $m_2^{\Omega_2}$, to the product space $\Omega = \Omega_1 \times \Omega_2$. The vacuous extension operation denoted by $\uparrow$ and defined such that:

$$m^{\Omega_1 \uparrow \Omega_1 \times \Omega_2}(B) = m^{\Omega_1}(A) \quad if \quad B = A \times \Omega_2 \tag{3}$$

where $A \subseteq \Omega_1$, $B \subseteq \Omega_1 \times \Omega_2$. It transforms each mass to the cylindrical extension B to $\Omega_1 \times \Omega_2$.

2.4 Decision process

The belief function framework proposes various solutions to make decision. Within the Transferable Belief Model (TBM) [19], the decision process is performed at the pignistic level where $bba's$ are transformed into the pignistic probabilities denoted by $BetP$ and defined as:

$$BetP(B) = \sum_{A \subseteq \Omega} \frac{|A \cap B|}{|A|} \frac{m^{\Omega}(A)}{(1 - m^{\Omega}(\emptyset))} \quad \forall\ B \in \Omega \tag{4}$$

3 Evidential Spammers and Group Spammers Detection (ESGSD) Method

In the following section, we elucidate a novel proposed hybrid method named Evidential Spammers and Group Spammers Detection (ESGSD) which aims to classify reviewers into spammer or genuine ones while taking into account both the group spammer and single spammer detection aspects.
Our proposal is composed from three parts. In the first one, we rely on the spammers' indicators extracted from each reviewer historic and used as features in the Evidential K-Nearest Neighbors classifier (EK-NN) [6] to model the reviewer spamicity according the single spammer indicators, which is inspired from our contribution in [3]. In the second part, we propose to model the reviewer spamicity while taking into account the group spammers' indicators which are modeled basing on the candidate groups and used as features in the EK-NN classifier which takes into account the pairwise group to define the distance choosing the K-nearest neighbors [4]. Once the reviewer spamicity basing on the spammer indicators and that based on the group spammers indicators are represented into two mass functions. Then, we combine them, in the third part, in order to make more suitable decision basing on the two aspects.
We detail these three parts in depth. In the following section, the reviewer is denoted by R_i where $i = 1, \ldots, n$ is the id of the corresponding one.

3.1 Modeling the reviewer spamicity using the spammer detection indicators

In this part, we propose to model the reviewer spamicity through a *bba* when relying on the spammer's indicators extracted from each reviewer behavior based on its historical data. Then, we handle the problem as binary classification one in order to model each reviewer spamicity under the frame of discernment $\Omega_S = \{S, \overline{S}\}$ where S represents the class of the reviewer considered as spammer and $\overline{S}$ is the class of the innocent reviewers.

3.1.1 Step 1: Pre-processing phase As well known in the fake reviews fields, the attitudes and the behaviors of the reviewer are considered as the most important points in the detection process. These behaviors may be extracted from the historic data of each reviewer. In ESGSD, we propose to use the spammers' indicators as features to train our algorithm. Thus, we rely on nine significant ones used in our method in [3]. Four features have the values into an interval of [0,1], where those closed to the 1 indicate the high spamicity degree. These features are Content Similarity (CS), Maximum Number of Reviews (MNR), Reviewing Burstiness (BST) and Ratio of First Reviews (RFR). Moreover, we rely on also on five other binary features where the 1 value indicates the spamming and the 0 value presents the non spamming behavior. These are named: Duplicate/Near Duplicate Reviews (DUP), Extreme Rating (EXT), Rating Deviation (RD), Early Time Frame (ETF) and Rating Abuse (RA). All the definitions and the calculation details are presented in our previous work [3].

3.1.2 Step 2: EK-NN application After extracting the spammers indicators, we propose to use them as features to train the EK-NN [6] in order to model the reviewer spamicity while taking into account the uncertain aspect. We apply the EK-NN classifier in which we initialize the parameters, we measure the distance between each reviewer R and the target one R_i using $d(R, R_i)$ and select K most similar neighbors to each target reviewer. After that, we generate bbas for each reviewer and we combine them through the Dempster combination rule. Thus, the obtained *bba* represents the reviewer spamicity while taking into account the uncertain aspect and the spammers' indicators. It is obtained as follows: $m_R^{\Omega_S} = m_{R,R_1}^{\Omega_S} \oplus m_{R,R_2}^{\Omega_S} \oplus .... \oplus m_{R,R_K}^{\Omega_S}$.

3.2 Modeling the reviewer spamicity using group spammer detection indicators

3.2.1 Step 1: Pre-processing phase Group Spammers usually attack the brands together where posting multiple reviews in order to promote or demote any target products. Thus, in order to build candidate spammers groups, we use frequent pattern mining which catch the spammers working together on multiple products. After that, we enumerate the group spammers indicators which can control the behaviors of the candidate spammers and to find out if these groups are behaving strangely. In order to construct sufficient groups for evaluation from

the data, we use the Frequent Itemset Mining (FIM). Since, we aim to focus on the worst spamming activities in our dataset, we apply the Maximal Frequent Itemset Mining (MFIM) to discover groups with maximal size. The different group spammers' indicators used in this part are Time Window (TW), Group Deviation (GD), Group Content Similarity (GCS), Member Content Similarity (MCS), Early Time Frame (ETF), Ratio of Group Size (RGS), Group Size (GS) and Support Count (SC) [4].

3.2.2 Step 2: EK-NN application After applying the FIM algorithm with fixed parameters, we find that the suspect clusters turn out to be very similar to each other in terms of members, examined products and similar evaluations. These small clusters can be favorable for detecting groups in novel ways. Thus, we apply the EK-NN based method to detect groups when relying on the similarities between such groups. We model our detection problem as a binary classification problem in order to assign each reviewer R to a class $\Omega_{GS} = \{MGS, \overline{MGS}\}$ where MGS represents the class of the members of the group spammer and $\overline{MGS}$ is the class of the reviewers who did not belong to the group spammer (innocent ones). The idea is that given a set of groups, the reviewers who belong to "similar" groups may be more likely to have the same class labels. Thus the class label of a reviewer R can be determined commonly by a set of K reviewers R_i who belong to groups most "similar" to the groups R belongs to.

After applying EK-NN classifier, the whole *bba* that models the evidence of the K-nearest Neighbors regarding the class of the reviewer is measured as such: $m_R^{\Omega_{GS}} = m_{R,R_1}^{\Omega_{GS}} \oplus m_{R,R_2}^{\Omega_{GS}} \oplus .... \oplus m_{R,R_K}^{\Omega_{GS}}$. It is considered as the mass function which represents the reviewer spamicity while relying on the group spammer indicators. The details are given in our previous work [4].

3.3 Distinguishing between spammers and genuine reviewers

In this part, we aim to combine the two *bbas* that model the reviewer spamicity once when taking into account the individual spammer behaviors and the other while taking into account the group spammer's indicators and in order to construct a global *bba* representing the reviewer spamicity. For this, we must model the *bbas* under a global frame and transfer them to the decision frame to make the final decision. These steps are detailed above.

3.3.1 Modeling the reviewer spamicity basing on both the spammers and the group spammers aspects

- Define Ω_{GSS} as the global frame of discernment relative to the reviewer spamicity according the group spammers and the spammers indicators. It defines the cross product of the two different frames Ω_{GS} and Ω_S denoted by: $\Omega_{GSS} = \Omega_{GS} \times \Omega_S$
- Extend all the review trustworthiness and the reviewer spamicity *bbas*, respectively $m_R^{\Omega_{GS}}$ and $m_R^{\Omega_S}$, to the global frame of discernment Ω_{GSS} to get new *bbas* $m_R^{\Omega_{GS}\uparrow\Omega_{GSS}}$ and $m_R^{\Omega_S\uparrow\Omega_{GSS}}$ using the vacuous extension (Eq. 3).

– Combine different extended *bbas* using the Dempster rule of combination. $m_R^{\Omega_{GSS}} = m_R^{\Omega_{GS}\uparrow\Omega_{GSS}} \oplus m_R^{\Omega_S\uparrow\Omega_{GSS}}$

Finally, $m_R^{\Omega_{GSS}}$ represents the reviewer spamicity relying on both the group spammers and the spammers indicators.

3.3.2 The reviewer spamicity transfer The next step is to transfer the combined $m_R^{\Omega_{GSS}}$ under the product space Ω_{GSS} to the frame of discernment $\Theta_D = \{RS, \overline{RS}\}$, where RS represents the class of the reviewers confirmed as spammers, and $\overline{RS}$ is the class of the genuine reviewers, in order to make the final decision by modeling the reviewer into a spammer or not. For that, a multi-valued operation [5], denoted τ is applied. The function τ: $\Omega_{GSS} \rightarrow 2^{\Theta_D}$ rounds up event pairs as follows:

– Masses of event couples with at least an element in $\{GS, S\}$ and not in $\{\overline{GS}, \overline{S}\}$ are transferred to Reviewer Spammer $RS \subseteq \Theta_D$ as:

$$m_\tau(\{RS\}) = \sum_{\tau(SR)=RS} m_R^{\Omega_{GSS}}(SR),\ SR \subseteq \Omega_{GSS} \tag{5}$$

– Masses of event couples with at least an element in $\{\overline{GS}, \overline{S}\}$ and not in $\{GS, S\}$ are transferred to Reviewer not Spammer $\overline{RS} \subseteq \Theta_D$ as:

$$m_\tau(\{\overline{RS}\}) = \sum_{\tau(SR)=\overline{RS}} m_R^{\Omega_{GSS}}(SR),\ SR \subseteq \Omega_{GSS} \tag{6}$$

– Masses of event couples with no element in $\{GS, S\}$ and not in $\{\overline{GS}, \overline{S}\}$ are transferred to Θ_D as:

$$m_\tau(\Theta_D) = \sum_{\tau(SR)=\Theta_D} m_R^{\Omega_{GSS}}(SR),\ SR_i \subseteq \Omega_{GSS} \tag{7}$$

3.3.3 Decision Making Now that we transferred all *bbas* modeling both the whole reviewer spamicity to the decision fame of discernment Θ_D in order to differentiate between the spammer and the genuine reviewers. Thus, we apply the pignistic probability $BetP$ using (Eq. 4). We select the hypothesis with the greater value of $BetP$ and we considered it as the final decision.

4 Experimentation and Results

Data description
We use two real labeled datasets collected from Yelp.com in order to evaluate our ESGSD method effectiveness. These datasets are considered as the most complete. They are labeled through the yelp filter which has been used in different related works [2, 3, 10, 14, 16] as a fundamental truth in favor of its effective

Table 1. Datasets description

Datasets	Reviews (filtered %)	Reviewers (Spammer %)	Services (Restaurant or hotel)
YelpZip	608,598 (13.22%)	260,277 (23.91%)	5,044
YelpNYC	359,052 (10.27%)	160,225 (17.79%)	923

detection algorithm based on both experts judgment and several behavioral features. Table 1 represents the datasets content where the percentages indicate the filtered fake reviews (not recommended) also the spammers reviewers.
In order to evaluate the ESGSD method, we rely on 3 evaluation criteria mentioned in the following: Accuracy, precision and recall.

Experimental results
In our datasets extracted from Yelp.com, we find that the number of genuine reviews is much larger than the number of fraudulent reviews, which can lead to an over-fitting. For the purpose of avoiding this problem, we extract a balanced data (50% of spam reviews and 50% of trustful ones). After that, we divided the datasets into 70% of training set and 30% of testing set. In addition, we average 10 trials values using the 10 cross-validation technique to obtain the final estimation of evaluation criterion. In the first part, we extract the spammers indicators through the historical of each reviewer (in our two datasets) to create our features in order to apply the EK-NN algorithm, we choose $k = 3$. In the second part, we apply the frequent itemset mining FIM, where I is the set of all reviewer ids in our two datasets. Each transaction is the set of the reviewer ids who have reviewed a particular hotel or restaurant. Thus, each hotel or restaurant generates a transaction of reviewer ids. By mining frequent itemsets, we find groups of reviewers who have reviewed multiple restaurants or hotels together. Then, we rely on the Maximal Frequent Itemset Mining (MFIM) to spot groups with maximal size in order to focus on the worst spamming activities. In the YelpZip dataset, we found 74,364 candidate groups and 50,050 candidate groups for the YelpNYC dataset.
Since, there is no methods which deal with both the spammer and the group spammers aspects. We propose to compare our ESGSD method with two methods from the group spammer detection field which is based on the FIM named: Detecting Group Review Spam **(DGRS)** proposed in [12] and Ranking Group Spam algorithm **(GSRank)** introduced in [13]. We compare also with two methods from the spammers detection field: **SpEagle** framework proposed by Rayana and Akoglu [16] and the method proposed by Fontanarava et al. [10] we denoted **FAFR**. We add to the comparison study our two previous methods: Evidential Group Spammers Detection (**EGSD**) introduced in [4] and Evidential Spammer Detection (**ESD**) proposed in [3].

The evaluation results are elucidated in Table 2. We observe that our ESGSD method continuously outperforms almost all compared baselines in most of evaluation criteria. We obtain the best results in terms of accuracy, precision, and

Table 2. Comparative results

	YelpZip			YelpNYC		
Evaluation criteria	Precision	Recall	Accuracy	Precision	Recall	Accuracy
SpEagle [16]	75.3%	65.2%	79%	73.5%	67.3%	76.9%
FAFR [10]	77.6%	86.1%	80.6%	74.8%	85%	81.6%
DGRS [12]	70%	71%	65%	62%	61.3%	60%
GSRank [13]	76%	74%	78%	76.5%	77.2%	74%
ESD [3]	85%	**86%**	84%	86%	83.6%	85%
EGSD [4]	83.5%	**86%**	85%	83.55%	85%	84.3%
ESGSD	**86%**	85%	**86.9%**	**87%**	**85.2%**	**85.9%**

a competitive ones in term of recall while using YelpZip dataset. For the YelpNYC database, we get the best results for all three considered criteria. We record at best an accuracy of 86.9% with the YelpZip dataset. We note an improvement which almost reaches 2% comparing with ESD method and 3% comparing with EGSD method. The precision criterion reaches at best 87%. The performance improvements recorded prove the importance of the use of both the group spammers and the spammers indicators while taking into account the uncertain aspects which allowed us to detect more particular cases.

5 Conclusion

In this paper, we tackle for the first time both the group spammer and the spammer review detection problem in order to perform the detection quality. This detection allows the different review systems to block suspicious reviewers in order to stop the emergence of fake reviews. Our ESGSD method succeeds in distinguishing between the spammers and the innocent even in the special cases. It proves its performance and effectiveness against various state-of-the-art approaches from the spammer and the group spammer fields. As future work, we aim to create a platform that deals with the all aspects of fake reviews detection problem to detect different types of spammers and deceptive reviews.

References

1. Ben Khalifa, M., Elouedi, Z., Lefèvre, E. Fake reviews detection based on both the review and the reviewer features under belief function theory. In proceedings of the 16th international conference Applied Computing (AC'2019), 123-130 (2019)
2. Ben Khalifa, M., Elouedi, Z., Lefèvre, E.: Spammers detection based on reviewers' behaviors under belief function theory. In proceedings of the 32nd International Conference on Industrial, Engineering Other Applications of Applied Intelligent Systems (IEA/AIE'2019). Springer International Publishing, 642-653 (2019)
3. Ben Khalifa, M., Elouedi, Z., Lefèvre, E., An Evidential Spammer Detection based on the Suspicious Behaviors' Indicators. In proceedings of the international Multi-Conference on: "Organization of Knowledge and Advanced Technologies" (OCTA), Tunis, Tunisia, 1-8 (2020)

4. Ben Khalifa, M., Elouedi, Z., Lefèvre, E. (2020) Evidential Group Spammers Detection. In proceeding of information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU' 2020). Springer International publishing, 341-353 (2020)
5. Dempster, A.P.: Upper and lower probabilities induced by a multivalued mapping. Ann. Math. Stat.38, 325-339 (1967)
6. Denoeux, T.: A K-nearest neighbor classification rule based on Dempster-Shafer theory. IEEE Trans. Syst. Man Cybern. 25(5), 804–813 (1995)
7. Elmogy, A., Usman. T., Atef, I., Ammar, M.: Fake Reviews Detection using Supervised Machine Learning. International Journal of Advanced Computer Science and Applications. 12 (1), 601-606 (2021).
8. Fayazbakhsh, S., Sinha, J.: Review spam detection: A network-based approach. Final Project Report: CSE 590 (Data Mining and Networks) (2012)
9. Fei, G., Mukherjee, A., Liu, B., Hsu, M., Castellanos, M., Ghosh, R.: Exploiting burstiness in reviews for review spammer detection. In proceedings of the Seventh International Conference on Weblogs and Social Media, ICWSM, 13, 175-184 (2013)
10. Fontanarava, J., Pasi, G., Viviani, M.: Feature Analysis for Fake Review Detection through Supervised Classification. In proceedings of the International Conference on Data Science and Advanced Analytics, 658-666 (2017).
11. Heydari, A., Tavakoli, M., Ismail, Z., Salim, N.: Leveraging quality metrics in voting model based thread retrieval.International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10 (1), 117-123 (2016)
12. Mukherjee, A., Liu, B., Wang, J., Glance, N., Jindal, N. Detecting Group Review Spam. In proceedings of the 20th International Conference on World Wide Web, WWW 2011, Hyderabad, India, ACM 978-1-4503-0637-9/11/03 (2011)
13. Mukherjee, A., Liu, B., Glance, N.: Spotting fake reviewer groups in consumer reviews. In proceedings of the 21st international conference on world wide web, ACM, New York, 191–200 (2012)
14. Mukherjee, A., Venkataraman, V., Liu, B., Glance, N.: What Yelp Fake Review Filter Might Be Doing. In proceedings of the Seventh International Conference on Weblogs and Social Media, ICWSM, 409-418 (2013)
15. 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)
16. Rayana, S., Akoglu, L.: Collective opinion spam detection: Bridging review networks and metadata. In proceedings of the 21th International Conference on Knowledge Discovery and Data Mining, ACM SIGKDD, 985-994 (2015)
17. Shafer, G.: A Mathematical Theory of Evidence, vol. 1. Princeton University Press (1976)
18. Smets, P.: The transferable belief model for expert judgement and reliability problem. Reliability Engineering and system safety, 38, 59-66 (1992)
19. Smets, P.: The transferable belief model for quantified belief representation. In: Smets, P. (ed.) Quantified Representation of Uncertainty and Imprecision, 267-301. Springer, Dordrecht (1998)
20. Wang, G., Xie, S., Liu, B., Yu, P. S.: Review graph based online store review spammer detection. In proceedings of the 11th international conference on data mining, ICDM, 1242-1247 (2011)
21. Wang, Z., Hou, T., Song, D., Li, Z., Kong, T.: Detecting review spammer groups via bipartite graph projection. Comput J 59(6):861–874 (2016)
22. Wang, Z., Gu, S., Xu, X.: GSLDA: LDA-based group spamming detection in product reviews. Appl Intell 48, 3094–3107 (2018).