Journal of Artificial Intelligence and Data Mining (JAIDM), Vol. 10, No. 2, 2022, 269-283.

Shahrood University of Technology

Journal of Artificial Intelligence and Data Mining (JAIDM)
Journal homepage: http://jad.shahroodut.ac.ir

Research paper

Detecting Group Review Spammers in Social Media

Zeinab Teimoori[1], Mostafa Salehi[1,4]*, Vahid Ranjbar[2], Saeedreza Shehnepoor[3], and Shaghayegh Najari[1]

1. Faculty of New Sciences and Technology, University of Tehran, Tehran, Iran.
2. Department of Computer Engineering, Yazd University, Yazd, Iran.
3. Department of Electrical, Electronic, and Computer Engineering, University of Western Australia, Perth, Australia.
4. School of Computer Science, Institute for Research in Fundamental Science (IPM), Tehran, Iran.

Article Info

Article History:
Received 10 July 2021
Revised 07 September 2021
Accepted 25 January 2022

DOI:
10.22044/jadm.2022.10981.2245

Keywords:
Social Media, Spam Reviews, Group Review Spammers, Heterogeneous Information Networks.

**Corresponding author: mostafa_salehi@ut.ac.ir (M. Salehi).*

Abstract

Nowadays, some e-advice websites and social media like e-commerce businesses provide not only their goods but a new way that their customers can give their opinions about the products. Meanwhile, there are some review spammers who try to promote or demote some specific products by writing fraud reviews. There have been several types of research works and studies toward detecting these review spammers but most studies are based on the individual review spammers, and few of them have studied the group review spammers; nevertheless, it should be mentioned that the review spammers can increase their effects by cooperating and working together. There have been many features introduced in order to detect the review spammers, and it is better to use the efficient ones. In this paper, we propose a novel framework, named network-based group review spammers, which tries to identify and classify the group review spammers with the usage of the heterogeneous information network. In addition to the eight basic features for detecting the group review spammers, three efficient new features from the previous studies are modified and added to improve detecting the group review spammers. Then with the definition of meta-path, the features are ranked. The results obtained show that using the importance of features and adding three new features in the suggested framework, the group review spammer detection is improved on the Amazon dataset.

5.1 Introduction

Nowadays, the growth of social media, e-advice, and e-commerce websites and the ability to share information, news, and opinions of the users with each other has become one of the inseparable parts of the people's social life. Social media such as online stores and social networks play a big role in both the people's social and commercial life. The online stores and manufacturers use the customers' reviews in order to evaluate the customers' needs and also defects of the products. On the other side, the reviews written by other users about the quality of services is more trusted for the customers rather than advertisements that try to exaggerate about the positive aspects. If most reviews are positive, they will buy them, and if most reviews are negative, they opt to buy other products. This can lead to hiring [1] review spammers by the companies to sell their product better in this competitive market by promoting their products and demoting other companies' products. The review spammers can easily lead the customers to purchase a specific product or to choose another product.

There are many methods introduced based on different approaches with various datasets. These methods based on features, can be categorized in these four categories: some of them can detect the review spammers and spam reviews using the

information provided by metadata; features extracted from the users' behavior [2]-[9], [10]. The linguistic-based methods use the information extracted from the text in reviews. They also use the context process techniques like N-gram [11]-[13] in order to analyze the behavioral features of reviews. There are other methods that extract the features using Deep Neural Networks (DNNs); they recently are more popular in the fake detection research such as spam detection [14], [15], anomaly detection [16], and bot detection tasks [17]. One of the interesting kinds of these methods known as auto-encoder uses the automatic feature extraction manner [18]. These methods extract the features from a text with no need to pre-process the textual data. Finally, there are some methods detecting the review spammers by graphs and correlation between the entities and network concepts [19]-[27], or in a new branch of research to measure trust in group [28], [29]. A review spammer approaches his/her goals by either writing a review individually or in a group. As [30] has indicated, most of the algorithms fail to spot the review spammers with a high accuracy since they will not consider group nature of spam writing, so lots of research works are now investigating the collective spam detection. There are three types of group review spammers: first, the users can work as a group, and each one of them tries to promote the other mates' reviews by replying or tagging or liking them [31]. The group review spammers also write reviews on the specific products using the common and pre-determined features like putting exclamation/question mark in their review more than usual or posting their reviews in a specific time [1], [32]-[34]. The last type is the review spammers with many accounts with different usernames in the producers' websites or online stores [35].

The main aim of this paper is to propose a graph-based method in a heterogeneous information network in order to find groups of review spammers with common features. Generally, the review datasets consist of the users (customers, reviewers), products (commodities, hotels, and restaurants), and reviews. The importance of graph-based methods is the unity of data and showing internal correlations by checking different paths [19].

In this work, we tried to extend our base framework proposed in [36] to spot the group review spammers (NGS). In fact, in addition to the features of the individual users, we engaged the information of the created connections between them in a network. Furthermore, we first modified the three practical features from the previous research works to be applicable for group spam detection, and used them along with eight other basic features from the previous [32]. On the other hand, we investigated the weight of all these eleven features on a graph in order to capture the information of connection between the entities using the meta-path. In short, in our proposed framework, we have a heterogeneous information network, in which each group maps into a node labeled using a semi-supervised learning method and connects these nodes by different features whose values indicate the connection weight. Our results show that not only does our proposed method outperform the state-of-the-art works but also our proposed features are able to outperform the results again.

Two different datasets from the Amazon website was used to evaluate the proposed method. After extracting every feature weight for identifying the features with good performance, these features were divided into four groups: behavioral-user-based, behavioral-item-based, linguistic-user-based, and linguistic-item-based. The results in each group for distinguishing the best performance and accuracy of the proposed method in both datasets were checked. To sum up, we can summarize our contribution as follows:

(i) In addition to eight existing features, three practical features from the previous research works were modified and introduced in the field of detecting group review spammers, resulting in a better performance.

(ii) A novel method called Network based Group Review Spammer (NGS) is introduced uses a meta-path based method for finding the weights and importance of the features, and finally, spotting the group review spammers and spam reviews with a semi-supervised learning method.

(iii) Finally, NGS could improve the applied criteria in identifying the group review spammers using the feature weights and their performance in labeling the group review spammers in comparison with the past studies.

The rest of the paper is organized as what follows. First, we mention the previous studies on different review spammer detection categories including the individual and group review spammer detection in Sec. 2 as the relate works. In Sec. 3, we give the preliminaries on our work including primary definitions of the network, and also the features used for the review spammer detection purpose. In Sec. 4, the proposed framework is discussed, and the pseudo-code of our algorithm is also presented. The results and evaluations of the algorithm and the proposed solution are

analyzed in Sec. 5, and finally, Sec. 6 concludes this work.

2. Related Works

There has been a noticeable growth in studying spam detection since 2008. In the recent years, many methods have been introduced to detect the individual or group review spammers. Yet, this problem is far from solving. Different researchers have focused on finding an acceptable way with a high performance in order to solve this problem. Thus the previous research works are introduced based on their engaged approaches.

2.1. Linguistic-based method

The linguistic-based method tries to extract the features from the reviews to detect the spam reviews and review spammers. Although there have been lots of studies in this field, the linguistic-based method is one of the oldest and basic methods, i.e. for individual spam detection [12], [37], cosine similarity, as a feature for demonstrating the similarity between two reviews, show that as much as similarity between the reviews increases, their probability being spam increases as well. Mukherjee *et al.* [5] have also claimed that by using the length of the review, they have found out that if the reviewer's texts are shorter, s/he is probably a review spammer. For the group review spammer detection [1], [32], [33], they have used some text features like the length of reviews or similarities of reviews or number of capital letters in a group in order to detect the group review spammers.

2.2. Behavioural-based method

In order to improve the linguistic-based method, the behavioral features are engaged, which require a dataset with meta-data. Some studies could detect the review spammers using some features like burstiness [5], more precise. Also in Lim *et al.* [6], using the average rate of reviews, have shown that more deviation from the average can increase the probability of spamicity. In the field of detecting the group review spammers, [32] and [33] have shown that with using the features like group time window, they can conclude that the members in a spam group are likely to work together in posting reviews for the target products during a short time interval. A couple of studies focus on some special social networks or media for targeting the spams and review spammers. There are several studies on Twitter as one of the most targeted media by the review spammers [38]. In [38], the effectiveness of 24 features such as the number of tweets, number of followers, and tweet rate is examined on Twitter. Similar to our case study in [27], these features are finally ranked by three measurements: Information Gain, Chi-Square, and AUC. In [39], the researchers have claimed that the extracted features can change over time, and this results in an accuracy decrement. This study addressed this problem by means of 1 million spam and 1 million non-spam tweets and incorporating feature variation in the training process. In [40], a hybrid approach has been proposed by incorporating both the meta-data and content-centric features on Twitter. This study claims that a user can evade the features related to her/his activities but it is difficult for him/her to evade the followers' activities. 27 features are engaged in this study, and three different classifiers including random forest, decision tree, and Bayesian network are used to classify the twitters.

2.3. Graph-based method

The graph-based method makes a graph between the users, reviews, and items, and usethe connections in the graph and also some network-based algorithms to rank or label the reviews and the users. In 2015, Akoglu *et al.* [19], introduced a graph-based method using the extracted network-based features for the individual review spammer detection. In this method, some features of the nearest neighbors for a node such as the number of triangles and the total weight of edges were used, and after studying these features, they determined a specific pattern in order to find the abnormal nodes/edges. Before 2011, due to the time/space complexity issue, the researchers had used small graphs but in 2011, Henderson *et al.* [21] extracted some nodes and their neighbors' features using a recursive algorithm, and they could obtain an acceptable behavioral information in a big graph. According to our knowledge, the first study on the group review spammer detection has been done in 2012 [32], and they have pre-processed an Amazon dataset, and extracted eight behavioral and linguistic features related to the group review spammers, and then introduced three models by combining the groups, members, and products for ranking and labeling the groups. After that, in 2016, a method was proposed for detecting the group review spammers using an Arabic dataset [33], which used the support vector machine (SVM) and k-nearest neighbor algorithms as a classification method. Another approach for detecting the group review spammers was done in 2019 with a new method to create the groups [34]. In the proposed method, they created a group that consisted of just one

member and focused on how a member behaved. Using this method, they showed that a review spammer behaved in the same way. In 2017, a new approach was proposed for detecting the individual review spammers using the meta-path in heterogeneous networks, and then the prominence of eight individual features for detecting the review spammers was studied [36], [33].

3. Preliminarie

In order to better understand the proposed framework, an overview of some of the concepts and definitions in the heterogeneous information networks are presented. In this section, we introduce the definitions related to the approach in the sub-section 3.1. The sub-section 3.2 introduces the feature types used for the group review spammer detection.

3.1. Definitions

Definition 1 (Heterogeneous information network). Suppose that we have $r(>1)$ types of nodes and $s(>1)$ types of relation links between the nodes, and then a heterogeneous information network is defined as a graph $G=(V.E)$, where each node $v \in V$ and link $e \in E$ belong to one particular node type and link type, respectively. If the two links belong to the same type, the types of starting node and an ending node of those links are the same [32], [36].

Definition 2 (Meta-path). Given a network $T_G=(A.R)$, a meta-path P is defined by a sequence of relations in the network, denoted in the form of $A_1(R_1)A_2(R_2)\ldots(R_{l-1})A_l$, which defines a composite relation $P=R_1 o R_2 o \ldots o R_{l-1}$ between two nodes, where o is the composition operator on the relations. For convenience, a meta-path can be represented by a sequence of node types when there is no ambiguity, *i.e.* $P=A_1.A_2.\ldots.A_l$. Then the meta-path extends the concept of link types to the path types, and describes the different relations among the node types through indirect links, *i.e.* paths, and also implies diverse semantics [32], [36].

3.2. Features types

The features used for detecting the review spammers are classified into the individual and group features. The group features are employed in this work.

Inputs: *group review dataset–group spam features–pre-labeled review groups*

Outputs: *features importance(W)–groups spamicity probability (Pr)*

%Prior knowledge

$$prior_u^{spam} = \frac{1}{L}\sum_{l=1}^{L}\left(f(x_{l_u})\right)$$

%Meta-path definition and creation

$$m_u^{p_l} = \frac{s \times f\left(x_{l_u}\right)}{s}$$

$$m_v^{p_l} = \frac{s \times f\left(x_{l_v}\right)}{s}$$

if

$= m_u^{p_l} \quad m_v^{p_l}$

$$m_{u,v}^{p_l} = m_v^{p_l}$$

else

$$m_{u,v}^{prior_l} = 0$$

%Classification–Weight calculation

$$Wp_l = \frac{\sum_{u=1}^{n}\sum_{v=1}^{n} m_{uv}^{p_l} \times prior_u^{spam} \times prior_v^{spam}}{\sum_{u=1}^{n}\sum_{v=1}^{n} m_{uv}^{p_l}}$$

%Classification–Labeling

$$Pr_{uv}^{spam} = 1 - \left(\prod_{l=1}^{L} m_{uv}^{p_l} \times \left(1 - W_{p_l}\right)\right)$$

$$Pr_u^{spam} = avg\left(Pr_{u1}^{spam}, Pr_{u2}^{spam}, \ldots, Pr_{ul}^{spam}\right)$$

return (W, Pr)

Algorithm 1. Detecting the group review spammers using a graph-based method with meta-path, and calculating the weights of each feature.

3.2.1. Group content similarity

The probability of being a group review spammer increases if the reviews in a group look the same. The *Group Content Similarity (GCS)* models this behavior [32]:

$$GCSD(g) = max_{p \in P_g}\left(CS_G(g.p)\right). \quad (1)$$

$$CS_G(g.p) = avg_{m_i.\, m_j \in g.i<j}\left(cosine\left(c(m_i.p).c(m_j.p)\right)\right) \quad (2)$$

Where $c(m_i.p)$ is the content of the review written by a group member $m_i \in g$, for product p from product group p_g. $CG_G(g.p)$ captures the average pairwise similarity of the review contents among the group members for a product p by computing the cosine similarity [32].

3.2.2. Group member content similarity

Normally, a review spammer posts the same comment on similar or different products in order to emphasize on his/her comment, and also to

save time and money. Thus the probability of a group review spammer increases if the users post the same comments on the same products or even the different ones. This behavior can be expressed by *Group Member Content Similarity (GMCS)*, as follows [32]:

$$GMCS(g) = \frac{\sum_{m \in g} CS_M(g.m)}{|g|} \quad (3)$$

$$CS_M(g.m) = avg_{p_i.p_j \in P_g, i<j}\left(cosine\left(c(m.p_i).c(m.p_j)\right)\right) \quad (4)$$

The group attains a value ≈ 1 on GMCS when all of its members entirely copy their own reviews across different products. In the P_g. $CS_M(g.m)$ models, the average pairwise content similarity of member $m \in g$ over all products in P_g. $|g|$ is the number of reviewers in a group g [32].

3.2.3. Group time window

The group members have a tendency to post a review in a short window time. Accordingly, the time gap between posting reviews can help to detect the group review spammers. The degree of active involvement of a group is modeled as *Group Time Window (GTW)* [32]:

$$GTW(g) = max_{p \in P_g}\left(GTW_p(g.p)\right) \quad (5)$$

$$\begin{cases} 0 & if\ L(g.p) - F(g.p) > \tau \\ 1 - \frac{L(g.p) - F(g.p)}{\tau} & otherwise \end{cases} \quad (6)$$

Where $L(g.p)$ and $F(g.p)$ are the latest and earliest dates of reviews posted for product $p \in P_g$ by the reviewers of group g, respectively. P_g is the set of all products reviewed by group g. Thus $GTW_p(g.p)$ gives the time window information of group g on a single product p. This definition says that a group g of reviewers posting reviews on a product p within a short burst of time is more prone to be spamming (attaining a value close to 1). A group working over a longer time interval than τ get a value of 0 as they are unlikely to have worked together. τ is a parameter, which as it is estimated [32], it is about to 86 days. The *Group Time Window GTW(g)* considers all the products reviewed by the group taking max over $p \in P_g$ so as to capture the worst behavior of the group. For the subsequent behaviors, max is taken for the same reason [32].

3.2.4. Group deviation

The average rating given by the users is in a certain range. Therefore, if the rates given by the users in a group is more or less than the average rate, the probability of being a group review spammer increases. This behavior is modeled by *Group Deviation (GD)* on a 5-star rating scale (with 4 being the maximum possible deviation) [32]:

$$GD(g) = max_{p \in P_g}(D(g, p)) \quad (7)$$

$$D(g.p) = \frac{\left| r_{p.g} - \overline{r_{p.g}} \right|}{4}, \quad (8)$$

Where $r_{p.g}$ and $\overline{r_{p.g}}$ are the average ratings for product p given by the members of group g and by other reviewers not in g, respectively. $D(g.p)$ is the deviation of the group on a single product p. If there are no other reviewers who have reviewed the product p, $\overline{r_{p.g}} = 0$ [32].

3.2.5. Group early time frame

Normally, the users pay more attention to the earlier reviews for a product, and most of the users do not have time to read all reviews for a product. Thus the review spammers try to be the first reviewer. The *Group Early Time Frame (GETF)* models have this behavior [32]:

$$GETF(g) = max_{p \in P_g}(GTF(g, p)) \quad (9)$$

$$GTF(g.p) = \begin{cases} 0 & if\ L(g.p) - A(p) > \beta \\ 1 - \frac{L(g.p) - A(p)}{\beta} & otherwise \end{cases} \quad (10)$$

Where $GTF(g.p)$ captures the time frame as to how early a group g reviews a product p. $L(g.p)$ and $A(p)$ are the latest dates of a review posted for product $p \in P_g$ by the group members and the date when p was made available for reviewing, respectively. β is the threshold (say 260 days), which means that after β days, GTF attains a value of 0 as the reviews posted then are not considered to be early anymore. Since our experimental datasets [1], [32] have no exact date for launching product, A(p) is a good indicator for estimating this date $A(p)$ [32].

3.2.6. Group size ratio

The number of reviews in a group for a product compared to all reviews on that product in a

dataset plays a role in defining a group as a group review spammer. According to this, if the number of group reviews to the total number of reviews for a product increases, it means that there are fewer reviews posted by the other users. Thus they have more control over this product, and it seems that the group members are the only reviewers of the product, and as a result, the probability of a group reviewers of being spammer increases. The *Group Size Ratio (GSR)* models this behavior [32]:

$$\mathrm{GSR}(g)=Ave_{p\in P_g}(\mathrm{GSR}_p(g,p)) \quad (11)$$

$$\mathrm{GSR}_p(g,p)=\frac{|g|}{|M_p|} \quad (12)$$

Where $GSR_p(g.p)$ is the ratio of group size to M_p (the set of all reviewers of product (p) for product p [32].

3.2.7. Group size

The group size or in other words, the number of all reviewers in a group is one of the features that can be used for detecting the group review spammers. It means that the big groups with lots of reviewers is more likely to be a spammer group. GS is easy to model. We normalized it to [0, 1]. $max(|g_i|)$ is the largest group size of all discovered groups [32].

3.2.8. Group support count

The support count of a group is the total number of products in each group. The groups with high support counts have higher possibilities, and are more likely to be the group review spammers, as the probability of a group of random people happens to have reviewed many products together is small. GSUP is modeled as follows. We normalized it to [0, 1], with $max(|P_{g_i}|)$ being the largest support count of all the discovered groups [32]:

$$\mathrm{GS}(g)=\frac{|g|}{max(|g_i|)} \quad (13)$$

3.2.9. Group support count

The support count of a group is the total number of products in each group. The groups with high support counts have higher possibilities, and are more likely to be the group review spammers, as the probability of a group of random people happens to have reviewed many products together is small. GSUP is modeled as follows. We normalized it to [0, 1], with $max(|P_{g_i}|)$ being the largest support count of all the discovered groups [32]:

$$\mathrm{GSUP}(g)=\frac{|P_g|}{max(|P_{g_i}|)} \quad (14)$$

4. NGS: Proposed Solution

In this section, we provide the details of the proposed solution, which is shown in *Algorithm 1*. The proposed method has four main phases. In the following, we will discuss about these phases.

4.1. Frequent item-set mining

This phase is actually a machine learning algorithm that firstly imports the dataset and exports a new dataset including the groups of different users who post reviews on the products. In this part, due to studying the group review spammers, the groups of users and products are created to apply the group features on them. Using the proposed algorithm in [42], FIM (Frequent Item-set Mining) is used to create the groups of users who have posted on at least three common products. This algorithm examines the number of products, and each is common in the users who tried to share their opinion with the other users. Thus if the users have at least 3 products in common for the reviews they had written, they will be considered as groups. Then these groups will be engaged on the computations used for calculating spamicity for each one of them.

4.2. Extracting features

This phase can extract the mentioned features in Sec. 3. and three modified features in order to detect the group review spammers. After introducing eight basic features, three new features are proposed as follow:

4.2.1. Group review size ratio

A reviewer who posts a lot of reviews is called an active reviewer. An active reviewer is more likely to be a spammer since s/he spends more time and posts more reviews in order to earn more money; thus if the number of active reviewers in a group is more than 0.715 (that is the threshold), this group has a higher possibility to be a group review spammers. *Group Review Size Ratio (GRS)* is modeled as follows:

$$\mathrm{GRS}(g)=1-Ave_{m\in M_g}(\mathrm{RS}(g,\mathrm{m})) \quad (15)$$

$$\mathrm{RS}(g,\mathrm{m})=\frac{|r(g.m)|}{|M_r|} \quad (16)$$

Where $r(g.m)$ is the number of reviews given by a member m in a group g, and M_r is the total number of reviews given by m on all products.

4.2.2. Group capital words

In a text, if there are too many words written in capital letters, this means that a user wants to emphasize on a matter; hence, s/he can attract attentions of different visiting users to himself/herself. If the number of capital words is higher than the threshold 0.75 in a group, then the group is more likely to be a group review spammer. We normalized it to [0, 1], with $max(GCW(g))$ being the largest number of capital words of all discovered groups. The *Group Capital Words (GCWs) is* modeled as bellow:

$$GCW(g) = \frac{ave_{p \in P_g}\left(CW_G(g.p)\right)}{Max_{p \in P_g}\left(GCW(g_i)\right)} \quad (17)$$

$$CW_G(g.p) = \sum_{p \in P_g}\left(cw(c(p))\right) \quad (18)$$

Where $cw(c(p))$ indicates the number of capital words in the content of reviews on a product p in group g.

4.2.3. Group review length

As mentioned earlier, the real users tend to write a detailed review, while the review spammers try to write a brief review instead of going through details. Thus if the average length of reviews in a group is less than the set threshold of 0.35, the probability of being a spam group increases. We normalized it to [0, 1], with $Max_{g \in G} Max_{p \in P_g}\left(RL(p.g)\right)$ being the largest review length of all the discovered groups. *Group Review Length (GRL)* is modeled as below:

$$GRL(g) = 1 - \frac{ave_{p \in P_g}\left(RL(g.p)\right)}{Max_{g \in G} Max_{p \in P_g}\left(RL(\mathrm{p.g})\right)} \quad (19)$$

$$RL(g.p) = \sum_{p \in P_g}\left(L(R(p.g))\right) \quad (20)$$

Where $L(R(p.g))$ is the length of reviews from each user on a product p in a group g.

4.1. Mata-path definition and creation

This phase creates the network regarding feature values extracted in the previous phase. After extracting all the features values, the next step is to compute prior knowledge, *i.e.* the initial probability of a group of users u being spam is indicated as $prior_u^{spam}$. In our method, the prior knowledge is formalized using $prior_u^{spam} = \frac{1}{L}\sum_{l=1}^{L}\left(f(x_{l_u})\right)$, where $f(x_{l_u})$ is the probability of group *u* being the review spammers according to feature l, and L is the number of all the used features (in this work, eleven features). After computing the prior knowledge for each group, we define an extended version of the meta-path concept considering different levels of spam certainty. In other words, two groups are connected to each other if they share the same value. We use a step function in order to determine the levels of spam certainty that are used to assign values to each meta-path, so we can have meta-path between each two reviews. For this purpose, given a group u, the levels of spam certainty for meta-path p_l is computed as $m_u^{p_l} = \frac{s \times f\left(x_{l_u}\right)}{s}$, where s denotes the number of levels. After computing $m_u^{p_l}$ for all groups and meta-path, two groups u and v with the same values are connected to each other through meta-path, and create one link of group network. The meta-path value between these groups is denoted as $m_{uv}^{p_l} = m_u^{p_l} = m_v^{p_l}$. Using s with higher values will increase the number of each feature's meta-path. In other hands, using lower values for s (e.g. 2) makes the groups to take the value 0 or 1. In the proposed framework, we considered $s = 20,$ which is $m_u^{p_l} \in \{0.0.5.0.10.\ldots.0.85.0.90.0.95\}$ [37].

4.2. Classification

As the final step for this framework, we need to classify the reviews and group review spammers. In this part, two important outputs of this framework (feature weights and group spamicity) will be obtained. This phase is made of two steps: the weight calculating step that computes the weight of each feature regarding their produced network, and the labeling step that can calculate the spamicity value for each group. In the following, each step is explained separately.

4.4.1. Weight calculation

In this step, the weight of each feature is computed using the values obtained from the mentioned meta-paths. Each feature weight indicates the priority and importance of those features.

Table 1. Different datasets used in this work.

Dataset name	Released date	Dataset types	Number of users	Number of reviews	Number of products	Number of groups	Number of labelled groups
Amazon	Early in 2010	Main	2476785	5845126	1231018	7052	2431
		Review-based	171845	584513	192976	2333	2333
		User-based	166108	355325	130083	866	866
		Item-based	94547	181293	45769	733	733
Amazon	2012	Main	560277	1582125	489124	8925	5846
		Review-based	48034	158213	39856	6258	3458
		User-Based	14786	132732	17946	5853	2869
		Item-Based	12865	117208	11269	2698	1895

Considering the graph, edges, and their relationship in this work, as much as the number of meta-paths between two reviews increases, they are more likely to have the same label. For computing the weight of meta-path p_l, we propose the following equation:

$$Wp_l = \frac{\sum_{r=1}^{n}\sum_{s=1}^{n} m_{rs}^{p_l} \times prior_r^{spam} \times prior_s^{spam}}{\sum_{r=1}^{n}\sum_{s=1}^{n} m_{rs}^{p_l}} \quad (21)$$

Where n is the number of all groups, $m_{rs}^{p_l}$ is a meta-path value between *the* groups r, and s, $l = 1.....11$, *and* $prior_r^{spam}$. $prior_s^{spam}$ are the prior knowledge of the groups r and s, respectively. As the equation shows, there is a multiplication of the meta-path value between two nodes and our prior knowledge on them to be spam, normalized by summation on meta-path values. Thus as much as the prior knowledge increases for a specific feature, it shows that the mentioned meta-path is more contributed in finding the spam reviews, and vise-versa.

4.4.2. Labelling

In this part, the feature weights are calculated using meta-path, and then the spamicity of each review is obtained using these weights. Let $Pr_{u.v}^{spam}$ be the probability of unlabeled group u being spam by considering its relations with group v. In order to compute Pr_u^{spam}, the following equations are modeled:

$$Pr_{uv}^{spam} = 1 - \left(\prod_{i=1}^{n} m_{uv}^{p_l} \times \left(1 - W_{p_l}\right) \right) \quad (22)$$

$$Pr_u^{spam} = avg\left(Pr_{u1}^{spam}.Pr_{u2}^{spam}.... . Pr_{un}^{spam} \right) \quad (23)$$

Where n is the number of groups connected to group u, and W_{p_i} is the calculated weight for feature i. As much as the number of links between a group and other groups increases, its possibility to have the same label increases as well.

4.2. Experimental evaluation

In this section, firstly, the datasets used in this work and also three other extracted datasets are studied, and then we explain how to extract the other datasets using the first original datasets. Next, we introduce the evaluation metrics regarding the performance of the proposed framework. After obtaining the desired values for each metrics, these values will be compared with the state-of-the-art method, and finally, the importance of weight extraction and features will be studied.

Table 2. Distributions of spam/non-spam groups with a different threshold.

	Median	0	0.5	0.7
Spam	48%	41%	39%	30%
Non-spam	52%	59%	61%	70%

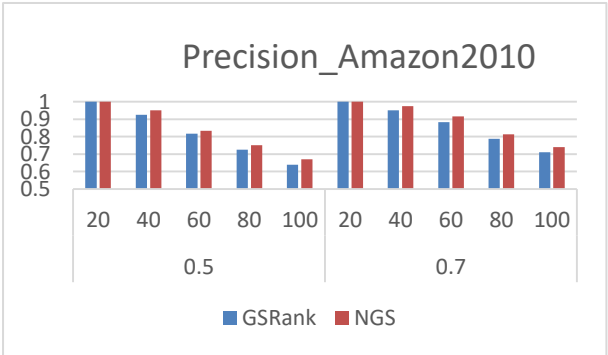
Table 3. Different feature categories of eleven features used in this work.

Feature categories	Item-based	User-based
Behavioral-based	GS-GSUP-GRS	GTW-GD-GETF-GSR
Linguistic-based	GCS-GRL-GCW	GMCS

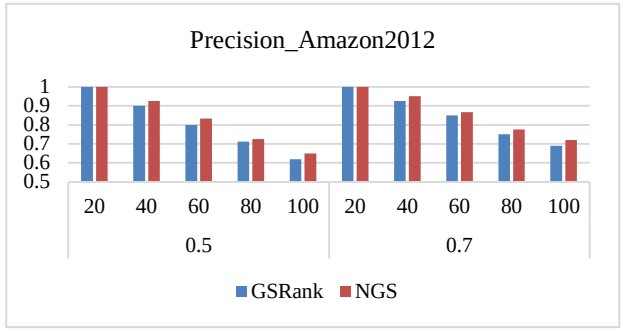
4.3. Dataset

In order to evaluate our framework, we need a dataset with fake/real reviews. In addition, this dataset should contain labels indicating the users that are in spam groups or not. Two different datasets were chosen from Amazon for

evaluation. The first dataset belongs to book and CDs



(a)



(b)

Fig. 1. Precision metric analysis for two different datasets using TH=0.5, 0.7, (a). Precision at different position @n=20, 40, 60, 80, 100 using the spamicity threshold of TH=0.5, 0.7 for Amazon-2010 dataset. (b). Precision at different position @n=20, 40, 60, 80, 100 using the spamicity threshold of TH=0.5, 0.7 for Amazon-2012 dataset.

categories of Amazon, which was collected in 2010 and contains 5,845,126 reviews, 1,231,018 products, 2,476,785 reviewers, and 7052 groups of users who posted reviews on at least three common products using frequent item-set minding algorithm. These reviews contain information about the quality and other aspects of the products of Amazon. In addition to reviews, this dataset contains 2431 labeled groups as near ground-truth, which determined whether a group is spam or not. These labels were made using human judges. Eight experts were hired, and in almost two months, they labeled all the groups by the values of 0, 0.5, and 1. Then as the final label for a group, the average values of all eight experts were calculated [33], and the other unlabeled groups were excluded. The second dataset is also from Amazon, which was collected in 2012 from the electronics devices category. This dataset is labeled using deleting algorithm in amazon that removes reviews in seven-month period, and determines if a review is spam or not. Thus they first crawl the dataset, and then after seven months, they will examine the dataset to see whether a review is deleted or not, and then they delete the reviews. This dataset consists of 1,582,125 reviews, 560,277 reviewers, 489,124 products, and 8925 groups that like the other dataset contains 5846 labeled groups as near ground-truth [1] and the other unlabeled groups were excluded. In this dataset, other attributes are the user id, product id, user name, rate of reviewers, date of the written review, and the review.

We created three other datasets from the main dataset as follow:

- The review-based dataset, including (containing) 10% of the reviews from the main dataset that was selected randomly by a uniform distribution.
- The item-based dataset includes 10% of the selected reviews for each item randomly, also by a uniform distribution.
- The user-based dataset includes 10% reviews for each user that was selected randomly using a uniform distribution.

Further information about the datasets is shown in Table 1.

4.4. Evaluation metrics

In order to detect the group review spammers, we need to calculate the probability of spamicity for each group using some metrics like Precision and Area Under Curve (AUC).

AUC measures the accuracy of ranking of the groups based on False Positive Ratio (FPR) as the x-axis and True Positive Ratio (TPR) as the y-axis, and integrate the values based on these two measured values. The value of these metrics increases as the proposed method performs well in ranking. The AUC value is obtained by the following equations:

$$TPR(i) = \frac{n_i}{q} \tag{24}$$

$$FPR(i) = \frac{n_i}{m} \tag{25}$$

$$AUC = \sum_{i=2}^{m} \left(FPR(i) - FPR(i-1)\right) \times \left(TPR(i)\right) \tag{26}$$

Where n_i is the number of spam groups, n_i is the number of non-spam groups before the index, q is the total number of spam groups, and m is the total number of groups.

In order to compute the Precision metric, first, we indicate a rank position n, which shows the precision values in $n = 20.40.60.80.100$ top ranked in the list, and it rewards ranking with the most relevant results at the top positions. This metric is calculated by the following equation:

$$P = TP / \left(\mathrm{TP} + \mathrm{FP}\right) \tag{27}$$

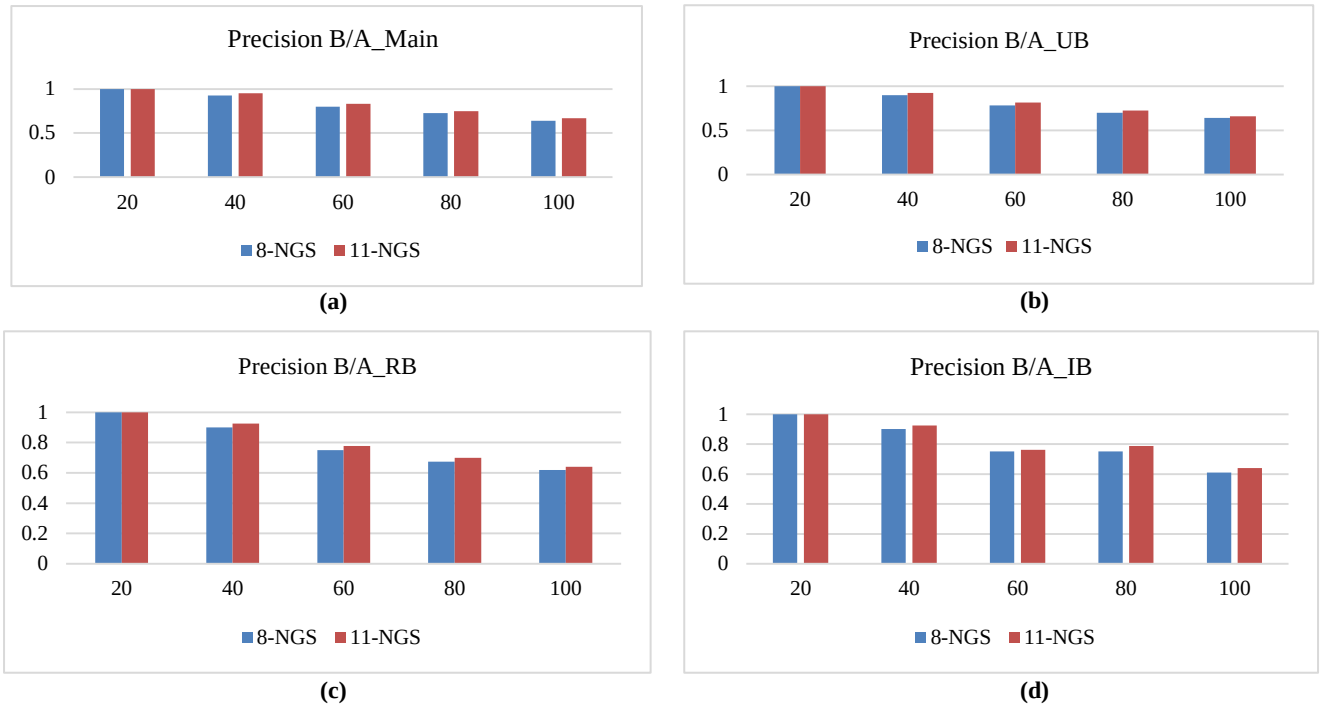
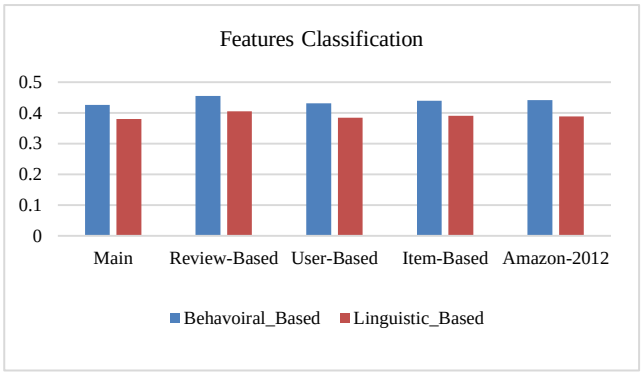


Figure 2. Precision metric analyis sbefore and after adding three new features for different Amazon-2010 dataset categories. (a). Precision at different rank position @n = 20, 40, 60, 80, 100 before and after adding three new proposed features for Amazon-2010-Main dataset. (b). Precision at different rank position @n = 20, 40, 60, 80, 100 before and after adding three new proposed features for Amazon-2010-user-based dataset. (c). Precision at different rank position @n = 20, 40, 60, 80, 100 before and after adding three new proposed features for Amazon-2010-review-based dataset. (d). Precision at different rank position @n = 20, 40, 60, 80, 100 before and after adding three new proposed features for Amazon-2010-Item-based dataset.

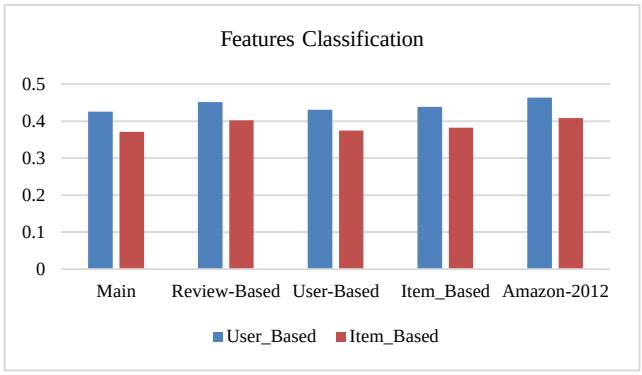
Where TP is the number of true detected spam groups and FP is the number of groups that are not actually spam but labeled as spam. As a result, when we sort the spam probabilities for the groups, all the groups with spam labels are on top of the ranked list.

4.5. Main results

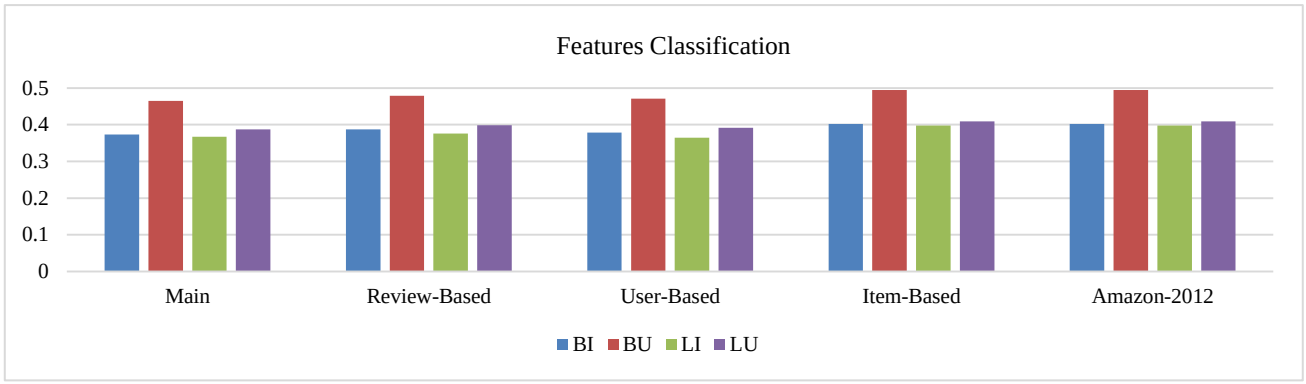
In this sub-section, the proposed method (NGS) is evaluated from a different perspective, and compared with other approaches, GSRank [32].
Due to the fact that NGS uses the meta-path approach, the observations show that NGS outperforms the GSRank. In fact, the meta-path major purposes are to increase the number of observations and the statistical power, and to improve the estimates of the effect size of an intervention or an association. In order to analyze the results obtained, two different thresholds on the groups' spamicity were used. These thresholds were chosen by their data distributions of group review spammers, as presented in *Table II*. Realistically, the spam reviews are small part of the Amazon data that we try to detect, so the set threshold is chosen by observing how much each threshold can show this partitioning.



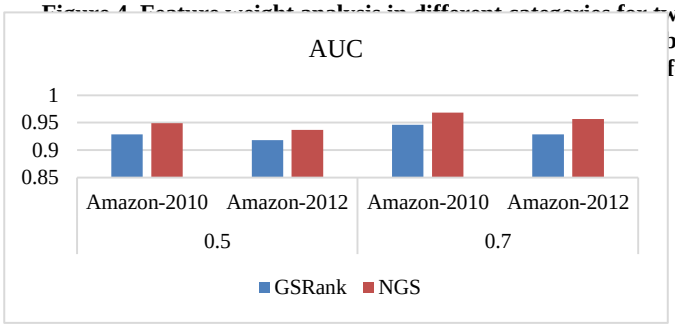
(a)



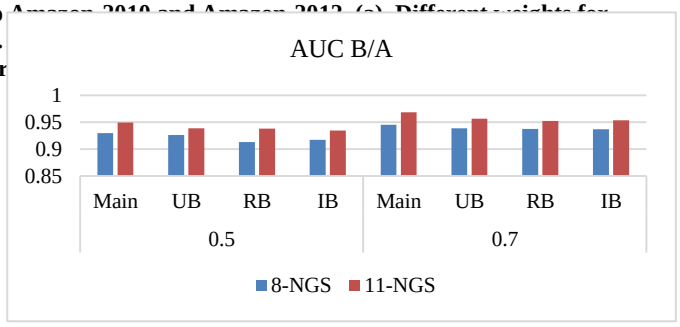
(b)



(c)



(a)



(b)

Figure 3. Area under curve metric analysis for different datasets and before/after adding three new features for different Amazon-2010 dataset categories. (a). Area under curve using spamicity threshold of TH = 0.5, 0.7 for two different datasets. (b). Area Under Curve using the spamicity threshold of TH=0.5, 0.7 before and after adding three new proposed features for different Amazon-2010 dataset categories.

Accuracy: Figure 1 presents the performance of precision for the proposed method (NGS) in 2 different Amazon datasets using the two thresholds 0.5 and 0.7 in the n rank positions. As shown in the first 20 groups, the accuracy is almost near to 1, and then it decreases as we go down the list since the groups are most likely to be the non-spam review groups. By increasing the number of groups, the precision values for both the 0.5 and 0.7 thresholds in NGS are getting higher and better than GSRank. In order to evaluate the performance of the three new features (GCW, GRL, and GRS), Figure 2 presents the precision values before and after adding the three new features in all four categories of the Amazon 2010 dataset (main, user-based, item-based, and review-based). It is observed that these features can improve the performance of detecting the group review spammers. In Figure 3(a), the AUC metrics is analyzed in two different datasets using two thresholds 0.5 and 0.7, and as it is shown, NGS has better values than GSRank with a higher rank positions of n. Figure 3(b) represents the AUC values in all the four different categories of

Amazon 2010 dataset (main, user-based, item-based, and review-based) before and after adding three new features, respectively. Feature weights Analysis: One of the achievements is calculating the weight and importance of the features.
Thus for comparing the features based on their weights, they are divided into different categories that are shown in table III. We are going to explain them in more details.
Behavioral-item-based features: These features do not use the content of reviews in the groups and its main focus is on a review that shows the users behavior. This category includes the GSUP, GS, and GSR features.
Linguistic-item-based features: This group of features constraints on the content of reviews regarding specific product and no supplementary information is needed. This category includes GCW, GRL, and GCS features.
Behavioral-User based features: These features do not use the content of reviews in groups and their main focus is on users' behavior. This category includes the GTW, GD, GETF, and GRS features.

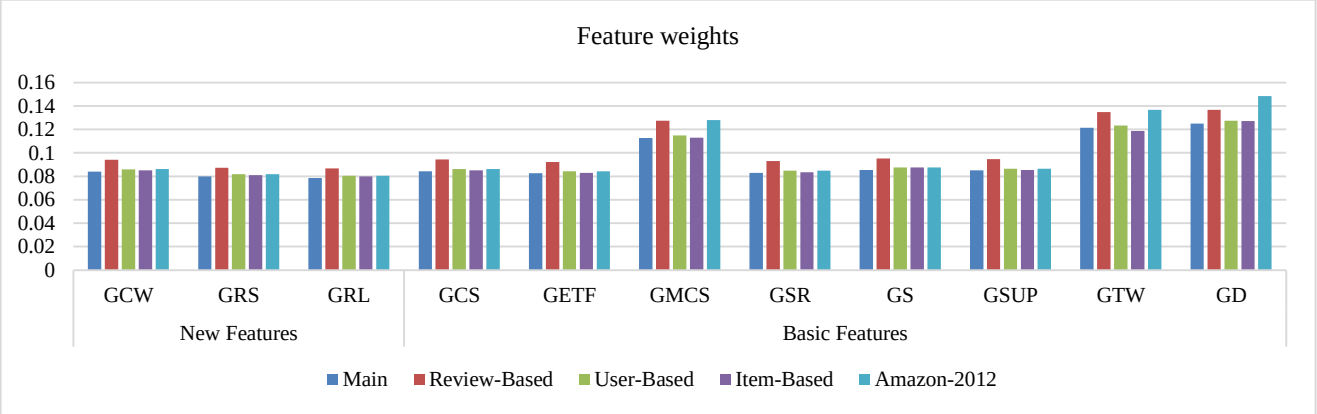


Figure 5. Weights of all new proposed features and basic features for different Amazon-2010 dataset categories and Amazon-2012 dataset.

Linguistic-user-based features: This group of features concentrates on the content of reviews according to the specific users in the groups, and does not use other information. This category includes the GMCS feature.

Next, the feature weights and their involvement for detecting the group review spammers are discussed. As mentioned earlier, the features were categorized into four categories (main, user-based, item-based, and review-based). Figure 4 shows the average weights of the features in each category, and it can be observed that the behavioral-user-based features can perform better, and can increase detecting the group review spammers functionality. As one can see, three new features yield the same performance as the other features do. As an analysis for this observation, the spamicity is more user-based rather than item-based, and as a result, lots of users tend to maintain their spammer nature rather than focus on their own specific set of items to attack, in a process called camouflage [19, 20].

If this process happened to be reverse, the users could write amouflage reviews to escape the detector algorithm, while they tend to strike complete and on different items.
Figure 5 shows the weights of all the used features in different datasets, and as shown, for all datasets and most weighted features, there is a certain sequence for the feature weights. The features like GD, GTW, and GMCS have better and higher weights, which means that they can detect more group review spammers than the other features, and on the other hand, GRL is not very efficient, which means that this feature cannot play an essential role to detect the spam review groups. It can be observed that these three new proposed features can perform like the other proposed features in the previous studies, and their weights are nearly the same so they can be considered as the new features in detecting the groups of review spammers.

4.6. Time complexity

Similar to the previous works, the time complexity of this framework is based on the main dataset as an input, which is $O(e^2 m)$, where e is the number of links in a created network or the number of reviews, and m is the number of features. This means that we need to check if there is a meta-path between a specific node (group) with other nodes that is $O(e^2)$, and

this process is repeated for all the features. Thus the time complexity for the offline mode, in which we gave the dataset to the framework and calculated the spamicity of groups, is $O(e^2)$. In the online mode, when a group is given to NGS to see whether it is a spam group or not, it needs to check if there is a meta-path between a given group with the other groups, which is $O(e)$, and like the offline mode, it has to be repeated for all features (11 features, in this case). Thus the time complexity is $O(em)$.

6. Conclusion

In this work, we introduced a novel group review spammer detection framework, named network-based group review spammer based on a network-based method and the meta-path concept with adding three practical new features that had been modified in the term of group review spammers for improving the detection process. With all the features in the field of detecting group review spammers, our framework could propose a way to calculate the weight of each feature used in the framework in order to determine the importance and priority of the features as an optimizer for the performance of proposed method.

The main results showed that by categorizing the features, we could choose the features with a high weight and a better performance in order to detect the group review spammers faster in an easier way. The proposed method was evaluated with the precision and AUC metrics, and compared with the state-of-the-art framework. The AUC results obtained showed that the NGS method could outperform the other method (GSRank) by about 3% improvement in detecting the group review spammers. The improvement is due to using the defined features alongside the concept of meta-path (explained in Section 4.3).

The key criterion for the proposed method's time complexity was to maintain the linear relationship between the number of reviews and the group spamicity detection in an online mode.

For the future works, at first, the Persian dataset can be selected and pre-processed in order to employ spam detection and some linguistic features based on the Persian language. In addition, as mentioned earlier, there are some groups of review spammers that one user has many user IDs in these groups and with different user IDs works in the websites. Therefore, in order to improve the group review spammer detection, it is possible to focus on the multiple-user-id entities and study the users' behavior by extracting useful information from the multiple-user-id members. Also we intend to apply some automatic text feature extraction methods including filtration and mapping in order to gain more valuable information from the reviews in order to increase the accuracy of the group spam detection.

Acknowledgment

Mostafa Salehi was supported by a grant from IPM, Iran (No. CS1400-4-268).

References

[1] M. Hu, G. Xu, C. Ma., and M. Daneshmand, "Detecting review spammer groups in dynamic review networks", In *Proceedings of the ACM Turing Celebration Conference-China*, 2019.

[2] Y. Ren, D. Ji., "Learning to Detect Deceptive Opinion Spam: A Survey", *IEEE Access* 7, pp. 42934-42945, 2019.

[3] F. Gillani, E. Al-Shaer, and B. AsSadhan, "Economic metric to improve spam detectors", *Journal of Network and Computer Applications, 65*, pp. 131-143, 2016.

[4] H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao, "Spotting Fake Reviews via Collective Positive-Unlabeled Learning", In *International Conference on Data Mining, IEEE*, pp. 894-904, 2014.

[5] A. Mukherjee, V. Venkataraman, B. Liu, and N. Glance, "What Yelp Fake Review Filter Might be Doing?", In *17th International AAAI Conference on Weblogs and Social Media*, pp. 1-10, 2013.

[6] R. Kaur, S. Singh, and H. Kumar, "Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches", *Journal of Network and Computer Applications, 112*, pp. 53-88, 2018.

[7] A. Mukherjee, A. Kumar, B. Liu, J. Wang, M. Hsu, and M. Castellanos, "Spotting Opinion Spammers using Behavioral Footprints", In *19th SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM*, pp. 632-640, 2013.

[8] B. Viswanath, M. A. Bashir, and M. C. Guha, "Towards Detecting Anomalous User Behavior in Online Social Networks", In *23rd USENIX Security Symposium*, pp. 223-238, 2014.

[9] J. Fu, P. Lin, and S. Lee, "Detecting spamming activities in a campus network using incremental learning", *Journal of Network and Computer Applications, 43* , pp. 56-65, 2014.

[10] A. Ala'M., J. Alqatawna, H. Faris, and M. A. Hassonah. "Spam profiles detection on social networks

using computational intelligence methods: the effect of the lingual context." Journal of Information Science 47, No. 1 (2021): 58-81.

[11] C. Chen, H. Zhao, and Y. Yang, "Deceptive Opinion Spam Detection using Deep Level Linguistic Features", In *National CCF Conference on Natural Language Processing and Chinese Computing*, pp. 465-474, 2015.

[12] R. Ghai, S. Kumar, and A. C. Pandey, "Spam Detection using Rating and Review Processing Method", In *Smart Innovations in Communication and Computational Sciences*. *Springer, Singapore*, pp. 189-198, 2019.

[13] P. P. Chan, C. Yang, D. S. Yeung, and W. W. Ng, "Spam filtering for short messages in adversarial environment", *Neurocomputing*, *155*, pp. 167-176, 2015.

[14] A. Zulfikar, B. Carminati, and E. Ferrari. "A deep learning model for Twitter spam detection." Online Social Networks and Media 18 (2020): 100079.

[15] E. Elakkiya, S. Selvakumar, and RL. Velusamy. "TextSpamDetector: textual content-based deep learning framework for social spam detection using conjoint attention mechanism." Journal of Ambient Intelligence and Humanized Computing (2020): 1-16.

[16] M. Ghanbari, M. Salehi, and V. Ranjbar: Anomaly Detection in Heterogeneous Information Networks. in Proc. Second National Informatics Conference of Iran, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran, 23-24 December 2020. (Persian).

[17] Shaghayegh Najari, Mostafa Salehi, and Reza Farahbakhsh: GANBOT: A GAN-based Framework for Social Bot Detection, 2021.

[18] A. D. Manqing, L. Yao, X. Wang, B. Benatallah, Ch. Huang, and X. Ning. "Opinion fraud detection via neural auto-encoder decision forest." Pattern Recognition Letters 132 (2020): 21-29.

[19] L. Akoglu, H. Tong, and D. Koutra, "Graph-based anomaly detection and description: a survey", In *21th International Conference on Information and Knowledge Management, ACM*, pp. 626-689, 2015.

[20] S. Rayana and L. Akoglu, "Collective Opinion Spam Detection: Bridging Review Networks and Metadata", In *21st SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM*, pp. 985-994, 2015.

[21] K. Henderson, B. Gallagher, L. Li, and L. Akoglu, "It is Who You Know: Graph Mining using Recursive Structural Features", In *17th SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM*, pp. 663-671, 2011.

[22] R. S. Wu, C. Ou, H. Y. Lin, S. I. Chang, and D. C. Yen, "Using a data mining technique to enhance tax evasion detection performance", *Expert Systems with Applications. 39(10)*, pp. 8769-8777, 2011.

[23] H. Li, A. Mukherjee, B. Liu, R. Kornfieldz, and S. Emeryz, "Detecting Campaign Promoters on Twitter using Markov Random Field", In *International Conference on Data Mining, IEEE*, pp. 290-299, 2015.

[24] Q. Meng, S. Tafavogh, and P. Kennedy, "Community Detection on Heterogeneous Networks by Multiple Semantic-Path Clustering", In *6th International Conference on Computational Aspects of Social Networks, IEEE*, pp. 7-12, 2014.

[25] Z. Wang, T. Hou, D. Song, Z. Li, and T. Kong, "Detecting Review Spammer groups via Bipartite Graph Projection", *The Computer Journal, 59(6)*, pp.861-874, 2017.

[26] A. N, Shirin, Nb. Salim, and N. Hawaniah Zakaria. "Opinion spam detection: using multi-iterative graph-based model." Information Processing and Management 57, No. 1 (2020): 102140.

[27] A. Hashemi and Z. Chahooki, "GroupRank: Ranking Online Social Groups Based on User Membership Records." *Journal of AI and Data Mining* 9, no. 1 : 45-57 (2021).

[28] Yanhong Li, Gang Kou, Guangxu Li, and Haomin Wang: Multi-attribute group decision making with opinion dynamics based on social trust network. Information Fusion 75: 102-115 (2021).

[29] Pasquale De Meo, Emilio Ferrara, Domenico Rosaci, and Giuseppe M. L. Sarnè: Trust and Compactness in Social Network Groups. IEEE Transactions on Cybernetics 45(2): 205-216 (2015).

[30] S. Cresci, R. D. Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "The paradigm-shift of social spambots: evidence, theories, and tools for the arms race", In *Proceedings of the 26th International Conference on World Wide Web Companion*, pp. 963-972, 2017.

[31] E. Choo, T. Yu, and M. Chi, "Detecting Opinion Spammer Groups through Community Discovery and Sentiment Analysis", In *International Federation for Information Processing*, pp.170-188, 2015.

[32] C, Chao, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Statistical features-based real-time detection of drifted Twitter spam", *IEEE Transactions on Information Forensics and Security* 12, No. 4, pp. 914-925, 2017.

[33] N. Aloshban and N. Aloshban, "A new approach for group spam detection in social media for Arabic language", In *8th International Conference on Latest Trends in Engineering and Technology*, pp.130-137, 2016.

[34] G. Xu, M. Hu, C. Ma, and M. Daneshmand, "GSCPM: CPM-based Group Spamming Detection in Online Product Reviews", In *IEEE International Conference on Communications (ICC)*, pp. 1-6, 2019.

[35] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. B. Razak, "Malicious accounts: dark

of the social networks", *Journal of Network and Computer Applications* 79, pp. 41-67, 2017.

[36] S. Shehnepoor, M. Salehi, R. Farahbakhsh, and N. Crespi, "NetSpam: a Network-based Spam Detection Framework for Reviews in Online Social Media", *Transactions on Information Forensics and Security, IEEE. 12(7),* pp.1585-1595, 2017.

[37] B. Manaskasemsak, C. Chanmakho, J. Klainongsuang, and A. Rungsawang, "Opinion Spam Detection through User Behavioral Graph Partitioning Approach", *Proceedings of the 3rd International Conference on Intelligent Systems, Metaheuristics and Swarm Intelligence, ACM,* pp. 73-77, 2019.

[38] Y. Chao, R. Harkreader, and G. Gu, "Empirical evaluation and a new design for fighting evolving twitter spammers", *IEEE Transactions on Information Forensics and Security* 8, No. 8, pp. 1280-1293, 2018.

[39] C, Chao, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Statistical features-based real-time detection of drifted Twitter spam", *IEEE Transactions on Information Forensics and Security* 12, No. 4, pp. 914-925, 2017.

[40] M. Fazil and M. Abulaish, "A Hybrid Approach for Detecting Automated Spammers in Twitter", *IEEE Transactions on Information Forensics and Security*, 2018.

[41] Z. Chensu, Y. Xin, X. Li, Y. Yang, and Y. Chen. "A heterogeneous ensemble learning framework for spam detection in social networks with imbalanced data." *Applied Sciences* 10, No. 3 936. (2020).

[42] R. Agrawal and R. Srikant, "Fastalgorithms for mining associationrules", *VLDB,* 1994.

شناسایی گروهی کاربران هرزنامه‌نگار در شبکه‌های اجتماعی

زینب تیموری[۱]، مصطفی صالحی[۱،۴*] ، وحید رنجبر[۲]، سعیدرضا شهنه‌پور[۳]و شقایق نجاری[۱]

[۱] دانشکده علوم و فنون نوین، دانشگاه تهران، تهران، ایران.

[۲] دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.

[۳] دانشکده مهندسی برق و کامپیوتر، دانشگاه وسترن استرالیا، پرت، استرالیا.

[۴] دانشکده علوم کامپیوتر، پژوهشگاه دانش‌های بنیادین، تهران، ایران.

ارسال ۲۰۲۱/۰۷/۱۰؛ بازنگری ۲۰۲۱/۰۹/۰۷؛ پذیرش ۲۰۲۲/۰۱/۲۵

چکیده:

امروزه اکثر شبکه‌های اجتماعی و وبسایت‌های تجاری فعال در حوزه تجارت الکترونیک، علاوه بر فروش محصولات امکانی برای تبادل نظر برای کاربران فراهم می‌آورند. در این میان کاربرانی که به آن‌ها هرزنامه‌نگار نیز گفته می‌شود وجود دارند که با نظرات متقلبانه تلاش دارند محصولی را بهتر و یا بدتر از حالت طبیعی آن جلوه دهند. در این خصوص، پژوهشگران زیادی تلاش نموده‌اند تا روش‌هایی برای شناسایی این گروه از افراد ارائه نمایند. علی‌رغم موفقیت‌های زیاد اما اکثر این روش‌ها مبتنی بر اطلاعات فقط یک کاربر است و اطلاعات گروهی کاربران را نادیده می‌گیرند در حالی‌که گروه‌های اسپمر می‌توانند تاثیر بیشتری بر سایر کاربران عادی بگذارند. در این مقاله ما تلاش داریم این گروه از هرزنامه‌نگاران را با استفاده از روش‌های مبتنی بر شبکه‌های اطلاعاتی ناهمگن استفاده کنیم. علاوه بر ۶ ویژگی پایه‌ای موجود مختص این شبکه‌ها ما ۳ ویژگی جدید را مبتنی بر ویژگی‌های قبلی برای بهبود روش شناسایی کاربران متقلب گروهی استفاده کرده‌ایم و در نهایت با استفاده از ویژگی فرامسیر ویژگی‌ها را مرتب میکنیم. نتایج ما بر روی یک دیتاست شناخته شده آمازون از اهمیت روش پیشنهادی و ویژگی‌های پیشنهاد شده در بهبود کارهای قبلی حکایت دارد.

کلمات کلیدی: شبکه‌های اجتماعی، کاربران متقلب، اسپمرها، شبکه‌های اطلاعاتی ناهمگن.