Spotting Collective Behaviour of Online Frauds in Customer Reviews

Sarthika Dhawan¹, Siva Charan Reddy Gangireddy¹, Shiv Kumar² and Tanmoy Chakraborty¹*

¹Indraprastha Institute of Information Technology Delhi (IIITD), India
²Netaji Subhas University of Technology (NSUT), Delhi, India
{sarthika15170, sivag}@iiitd.ac.in, shivk.it.16@nsit.net.in, tanmoy@iiitd.ac.in

Abstract

Online reviews play a crucial role in deciding the quality of products before purchasing any product. Unfortunately, spammers often take advantage of online review forums by writing fraud reviews to promote/demote certain products. It may turn out to be more detrimental when such spammers collude and collectively inject spam reviews as they can take complete control of users’ sentiment due to the volume of spam reviews they inject. Group spam detection is thus more challenging than individual-level fraud detection due to unclear definition of a group, variation of inter-group dynamics, scarcity of labeled group-level spam data, etc. Here, we propose DeFrauder, an unsupervised method to detect online fraud reviewer groups. It first detects candidate fraud groups by leveraging the underlying product review graph and incorporating several behavioral signals which model multi-faceted collaboration among reviewers. It then maps reviewers into an embedding space and assigns a spam score to each group such that groups comprising spammers with highly similar behavioral traits achieve high spam score. While comparing with five baselines on four real-world datasets (two of them were curated by us), DeFrauder shows superior performance by outperforming the best baseline with 17.11% higher NDCG@50 (on average) across datasets.

1 Introduction

Nowadays, online reviews are becoming highly important for customers to take any purchase-related decisions. Driven by the immense financial profits from product reviews, several blackmarket syndicates facilitate to post deceptive reviews to promote/demote certain products. Groups of such fraud reviewers are hired to take complete control of the sentiment about products. Collective behaviour is therefore more subtle than individual behaviour. At individual level, activities might be normal; however, at the group level they might be substantively different from the normal behavior. Moreover, it is not possible to understand the actual dynamics of a group by aggregating the behaviour of its members due to the complicated, multi-faceted, and evolving nature of inter-personal dynamics. Spammers in such collusive groups also adopt intelligent strategies (such as paraphrasing reviews of each other, employing a subset of their resources to one product, etc.) to evade detection.

Previous studies mostly focused on individual-level fraud detection [Lim et al.2010, Fei et al.2013, Akoglu et al.2013]. Few other studies which realized the detrimental effect of such collective activities detected groups simply based on Frequent Itemset Mining (FIM) [Mukherjee et al.2012, Xu et al.2013, Allahbakhsh et al.2013]. They thus focused more on ranking fraud groups, paying less attention to judge the quality of the detected groups.

[Wang et al.2016] pointed out several limitations of FIM for group detection – high computational complexity at low minimum support, absence of temporal information, unable to capture overlapping groups, prone to detect small and tighter groups, etc.

In this paper, we propose DeFrauder¹, a novel architecture for fraud reviewer group detection. DeFrauder contributes equally to (i) the detection of potential fraud groups by incorporating several coherent behavioral signals of reviewers, and (ii) the ranking of groups based on their degree of spamicity by proposing a novel ranking strategy. Experiments on four real-world labeled datasets (two of them were prepared by us) show that DeFrauder significantly outperforms five baselines – it beats the best baseline by 11.35% higher accuracy for detecting groups, and 17.11% higher NDCG@50 for ranking groups (averaged over all datasets).

In short, our contributions are fourfold: (i) two novel datasets, (ii) novel method for reviewer group detection, (iii) novel method for ranking groups, and (iv) a comprehensive evaluation to show the superiority of DeFrauder.

2 Related Work

Due to the abundance of literature [Kou et al.2004] on online fraud detection, we restrict our discussion to fraud user detection on product review sites, which we deem as pertinent to this paper.

¹DeFrauder: Detecting Fraud Reviewer Groups, Code is available in [Dhawan et al.2019].
In user-level fraud detection, notable studies include [Lim et al.2010] which proposed scoring methods to measure the degree of spamicity of a reviewer based on rating behaviors; [Wang et al.2011] which developed a graph-based fraud reviewer detection model; [Fei et al.2013] which exploited burstiness in reviews to detect fake reviewers. SpEagle [Akoglu et al.2013] utilizes clues from all metadata as well as relational data and harnesses them collectively under a unified framework. ASM [Mukherjee et al.2013a] facilitates modeling spamicity as latent factor and allows to exploit various behavioral footprints of reviewers. [Wang et al.2012] argued that the dynamic behavioral signals can be captured through a heterogeneous reviewer graph by considering reviewers, reviews and products together. FraudEagle [Akoglu et al.2013] spots fraudsters and fake reviews simultaneously. [Dutta et al.2018, Chetan et al.2019] discussed about collusion in social media.

Few studies attempted to detect group-level fraud reviewer groups. GSRank [Mukherjee et al.2012] was the first method of this kind, which identifies spam reviewer groups using FIM, and ranks groups based on the relationship among groups, products, and individual reviewers. [Mukherjee et al.2012] argued that due to the scarcity of data, unsupervised method should be used to tackle this problem. Other studies largely focused on improving the ranking algorithm, ignoring the performance of the group detection method (they also used FIM for detecting groups) [Xu et al.2013, Allahbakhsh et al.2013, Mukherjee et al.2013b, Ott et al.2011]. [Xu and Zhang2015] proposed an Expectation Maximization algorithm to compute the collocative score of each group detected using FIM. [Wang et al.2016] argued that FIM tends to detect small-size and tighter groups. They proposed GSBP, a divide-and-conquer algorithm which emphasizes on the topological structure of the reviewer graph. GGSspam [Wang et al.2018b] directly generates spammer groups consisting of group members, target products, and spam reviews.

We propose DeFrauder that leverages temporal pattern, content similarity and underlying graph structure to detect collusive fraud groups in review forums (see Table 1 for a comparison). Unlike others, DeFrauder contributes equally to both the components – group detection and ranking.

### Table 1: DeFrauder captures all three signals obtained from users attributes and underlying graph structure.

<table>
<thead>
<tr>
<th>Temporal</th>
<th>GSBP</th>
<th>GGSspam</th>
<th>GSRank</th>
<th>DeFrauder</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 3 Proposed DeFrauder Framework

In this section, we explain DeFrauder which is a three-stage algorithm – detecting candidate fraud groups, measuring different fraud indicators of candidate groups, and ranking groups based on the group spam score.

#### 3.1 Group Fraud Indicators

Here we present six fraud indicators which measure the spamicity of a group [Mukherjee et al.2012, Wang et al.2018b, Wang et al.2016] by taking into account linguistic, behavioral, structural and temporal signals. All indicators are normalized to $[0, 1]$ – larger value indicates more spamming activity. Let $R$ and $P$ be the entire set of reviewers and products. Let $R(g)$ be the set of reviewers in a group $g$, and $P(g)$ be the set of target products reviewed by the reviewers in $R(g)$. Each reviewer $i$ reviewed a set of products $P_i$.

To reduce the contingency of small groups, we use a penalty function $L(g)$ which is a logistic function [Wang et al.2016]: $L(g) = 1/(1 + e^{-(\gamma|R(g)|+\gamma|P(g)|)^3})$. We subtract 3 from the sum since we consider minimum number of reviewers and products within a group to be 2 and 1, respectively; therefore $L(g) \in [0.5, 1]$ [Wang et al.2018a].

#### Review tightness ($RT$).

It is the ratio of the number of reviews in $g$ (assuming each reviewer is allowed to write one review to each product) to the product of the size of reviewer set and product set in $g$.

$$RT(g) = \frac{\sum_{i \in R(g)}|P_i|}{|R(g)||P(g)|} \cdot L(g)$$

(1)

If significant proportion of people co-reviewed several products, then it may imply a spam group activity.
Neighbor tightness (NT). It is defined as the average value of the Jaccard similarity (JS) of the product sets of each reviewer pair.

\[ NT(g) = \frac{\sum_{i,j \in R(g)} JS(P_i, P_j)}{|R(g)|^2} \cdot L(g) \]  

(2)

If the product sets are highly similar, both the reviewers are then highly likely to be together in a collusive group.

Product tightness (PT). It is the ratio of the number of common products to the number of products reviewed by all the members in \( g \) [Wang et al. 2016].

\[ PT(g) = \frac{|\bigcap_{i \in R(g)} P_i|}{\bigcup_{i \in R(g)} P_i} \cdot L(g) \]  

(3)

Group members reviewing certain number of products and not reviewing any other products are more likely to indulge in fraud activities.

Rating variance (RV). Group spammers tend to give similar ratings while reviewing any product. Let \( SD^2(p, g) \) be the variance of the rating scores of product \( p \) by reviewers in \( g \). We take the average variance for all target products. The variance degree \([0, 1]\) is converted into spam score between \([0, 1]\).

\[ RV(g) = 2L(g) \left( 1 - \frac{1}{1 + e^{-\frac{\sum_{p \in P(g)} SD^2(p, g)}{|P(g)|}}} \right) \]  

(4)

Product reviewer ratio (RR). It is defined as the maximum value of the ratio of the number of reviewers in \( R(g) \) who reviewed product \( p \in P(g) \) to the number of all the reviewers of \( p \), denoted by \( |Rev(p)| \):

\[ RR(g) = \max_{p \in P(g)} \frac{\sum_{i \in R(g)} |\{ 1 : p \in P_i \}|}{|Rev(p)|} \]  

(5)

If a product is mainly reviewed by the reviewers in \( g \), then the group is highly likely to be a spammer group.

Time window (TW). Fraudsters in a group are likely to post fake reviews during a short-time interval. Given a group \( g \), and a product \( p \in P_g \), we define the time-window based spamnicity as

\[ TW(g, p) = \begin{cases} \frac{1 - SD_p}{T}, & \text{if } SD_p \leq T \\ 0, & \text{if } SD_p > T \end{cases} \]

(6)

where \( SD_p \) is the standard deviation of review time for a product \( p \) reviewed by reviewers in group \( g \). \( T \) is a time threshold (set to 30 days in our experiments as suggested in [Wang et al. 2018b]).

### Algorithm 1: Extract Groups

```plaintext
1: Initialize:
2: \( CCgroups \leftarrow \text{set}() \) \quad \triangleright \text{Set of candidate groups}
3: \( G(V, E) \leftarrow \text{Edge attributed graph} \)
4: \( CSet \leftarrow \{ \} \) \quad \triangleright \text{Potential merged groups}
5: \( G, CCgroups \leftarrow \text{GroupDetector}(G, CCgroups) \)
6: Iterate:
7: \( G'(V', E') \leftarrow \text{Attributed line graph of } G \)
8: \( G', CCgroups = \text{GroupDetector}(G', CCgroups) \)
9: \( G \leftarrow G' \)
10: until \( |E| > 1 \)
11: return \( CCgroups \)
12: function \( \text{GroupDetector}(G, CCgroups) \)
13: \( \text{for each isolated node } v_i \text{ in } G \) do
14: \( CCgroups.add(v_i) \) and remove \( v_i \) from \( G \)
15: \( \text{for each pair } (e_i, e_j) \text{ in } E \times E \) do
16: \( \text{if } a^e_i \subset a^e_j \text{ then} \)
17: \( \text{if } \sum_{m \in e_j} p_m > 0.5 \text{ then} \)
18: \( CSet(a^e_i) = CSet(a^e_i) \cup a^e_j \)
19: \( \text{else} \)
20: \( \text{if } \sum_{m \in (a^e_i \cup a^e_j)} p_m > 0.5 \text{ then} \)
21: \( CCgroups.add(a^e_j - a^e_i) \)
22: \( \text{for each } e_i \in E \) do
23: \( k = CSet(e^a_i) \)
24: \( CCgroups.add(k) \) and remove \( k \) from \( G \)
25: \( \text{for each connected component } c \text{ with } |c| > 2 \) do
26: \( CCgroups.add(c) \) and remove \( c \) from \( G \)
27: \( \text{for each group } g \in CCgroups \) do
28: \( \text{if } \text{CollectiveScore}(g) \leq \tau_{spam} \text{ then} \)
29: \( CCgroups.remove(g) \)
30: \( \text{return } G, CCgroups \)
31: \end function
```

### 3.2 Detection of Candidate Fraud Groups

We propose a novel graph-based candidate group detection method based on the “coherence principle”.

**Hypothesis 1 (Coherence Principle)** Fraudsters in a group are coherent in terms of – (a) the products they review, (b) the ratings they give to the products, and (c) the time of reviewing the products.

We show that each component of this hypothesis is statistically significant (see Sec. 5). We incorporate these three factors into a novel **attributed product-product graph** construction – \( G(V, E) \) such that each \( v_{ij} \in V \) indicates a product-rating pair \( (p_i, r_j) \) and its attribute \( a^p_{ij} \) consists of the set of reviewers who rated \( p_i \) with \( r_j \). An edge \( e_{(i,j,mn)} = (u_{ij}, v_{mn}) \in E \) indicates the co-reviewing and co-rating patterns of two products \( p_i \) and \( p_m \) with rating \( r_j \) and \( r_n \), respectively. The edge attribute \( a^e_{(i,j,mn)} \) indicates the set of co-reviewers \( R_{(i,j,mn)} \) who reviewed both \( p_i \) and \( p_m \) and gave same ratings \( r_j \) and \( r_n \) respectively within the same time \( \tau_i \) (defined in Sec. 3.3). Note that edge \( e_{(i,j,mn)} \) connecting same product with different ratings wont exist in \( G \) as we assume
that a reviewer is not allowed to give multiple reviews/ratings to a single product.

We then propose \textbf{ExtractGroups} (pseudocode in Algo 1, a toy example in Supplementary [Dhawan et al.2019]), a novel group detection algorithm that takes \( G \) as an input and executes a series of operations through \textbf{GroupDetector()} (Line 12) – isolated nodes are first removed (Lines 13-14), edge attributes are then merged and removed if Jaccard similarity (JS) of product sets that the corresponding reviewers reviewed is greater than a threshold (set as 0.5). Any group of reviewers eliminated due to the consideration of only common reviewers during the creation of edges is also checked through JS in order to avoid loosing any potential candidate groups (Lines 15-24). Before proceeding to the next iteration, connected components containing more than two nodes are removed (Lines 25-26). We define \textbf{CollectiveScore} as the average of six group level indicators defined in Sec. 3.1, and consider those as potential groups whose \textbf{CollectiveScore} exceeds \( \tau_{spam} \) (Lines 27-29, defined in Sec. 5.2).

It then converts the remaining structure of \( G \) into an attributed line graph (edges converted into vertices and vice versa) \( G'(V',E') \) as follows: \( v'_{(ij,nn)} \in V' \) corresponds to \( e_{(ij,nn)} \) in \( G \) and \( a'_{(ij,nn)}=a_{(ij,nn)} \) an edge \( e_{(ij,nn,ab)}=(v'_{(ij,nn)},v'_{(ij,ab)}) \) represents co-reviewing and co-rating patterns of products \( p_i, p_m \) and \( p_a \); the corresponding edge attribute is \( a_{(ij,nn,ab)}=a_{(ij,nn)} \land a_{(ij,ab)} \). \( G' \) is again fed into \textbf{GroupDetector} in the next iteration. Essentially, in each iteration, we keep clubbing reviewers together, who exhibit coherent reviewing patterns. The iteration continues until none of the edges remain in the resultant graph, and a set of candidate fraud groups are returned.

The worst case \textbf{time complexity} of \textbf{ExtractGroups} is \( O(k|E|^2) \), where \( k \) is the number of iterations, and \( |E| \) is the number of edges in \( G \) (see Supplementary [Dhawan et al.2019] for more details).

\textbf{Theorem 3.1 (Theorem of convergence)}

\textbf{ExtractGroups will converge within a finite number of iterations.}

See Supplementary [Dhawan et al.2019] for the proof.

3.3 Ranking of Candidate Fraud Groups

Once candidate fraud groups are detected, DeFraudr ranks these groups based on their spamicity. It involves two steps – mapping reviewers into an embedding space based on their co-reviewing patterns, and ranking groups based on how close the constituent reviewers are in the embedding space.

\textbf{Reviewer2Vec: Embedding Reviewers}

Our proposed embedding method, \textbf{Reviewer2Vec} is motivated by [Wang et al.2018b]. Given two reviewers \( i \) and \( j \) co-reviewing a product \( p \) in \( P \) by writing reviews \( c^i_p \) and \( c^j_p \) with the rating \( r^i_p \) and \( r^j_p \) at time \( t^i_p \) and \( t^j_p \) respectively, we define the \textit{collusive spamicity} of \( i, j \) w.r.t. \( p \) as:

\[
\text{Coll}(i,j,p) = \begin{cases} 
0, & |t^i_p - t^j_p| > \tau_t \vee |r^i_p - r^j_p| \geq \tau_r \\
\zeta(i,j,p), & \text{otherwise}
\end{cases}
\]

where,

\[
\zeta(i,j,p) = s^p \left[ \alpha \left( 1 - \frac{|t^i_p - t^j_p|}{\tau_t} \right) + \beta \left( 1 - \frac{|r^i_p - r^j_p|}{\tau_r} \right) + \gamma \cdot \text{Cosine}(c^i_p,c^j_p) \right]
\]

Where \( s^p \) is the degree of suspicion of product \( p \). \( \tau_t, \tau_r \) and \( \theta \) are the parameters of the model. If the posting time difference among reviewers \( i \) and \( j \) on \( p \) is beyond \( \tau_t \) or their rating on \( p \) deviates beyond \( \tau_r \) (where \( \tau_r = (\max - \min)x\% \)), where \( \max \) and \( \min \) are the maximum and minimum ratings that a product can achieve respectively, we do not consider this co-reviewing pattern. \textbf{ExtractGroups} achieves best results with \( \tau_t = 20 \) and \( \tau_r = (\max - \min)20\% \) (see Sec. 5.3).

\(
\zeta(i,j,p) = \text{the collusiveness between two reviewers w.r.t. product } p \text{ they co-reviewed; however there might be other reviewers who reviewed } p \text{ as well.}
\)

Lesser the number of reviewers of \( p \), more is the probability that \( i \) and \( j \) colluded. This factor is handled by \( s^p \) after passing it through a sigmoid function. \( \theta \) is a normalizing factor which ranges between \([0, 1]\) (set as 0.4 [Wang et al.2018b]). We take the cosine similarly of two reviews \( c^i_p \) and \( c^j_p \) after mapping them into embedding space using Word2Vec [Mikolov et al.2013]. Combining the collusive spamicity of a pair of reviewers across all the products they co-reviewed, we obtain the overall collusive spamicity between two reviewers:

\[
\Phi(i,j) = \frac{2}{1 + e^{-\sigma(i,j)}} - 1
\]

where \( \sigma(i,j) = \sum_{p \in \{P \cap P_i\}} \text{Coll}(i,j,p) |P_i \cap P_j| / |P_i \cup P_j| \)

We then create a reviewer-reviewer spammer graph [Wang et al.2018b] which is a bi-connected and weighted graph \( G_s = (V_s, E_s) \), where \( V_s \) corresponds to the set of reviewers \( R \), and two reviewers \( i \) and \( j \) are connected by an edge \( e_{ij} \in E_s \) with the weight \( W_{ij} = \Phi(i,j) \). Once \( G_s \) is created, we use state-of-the-art node embedding method to generate node (reviewer) embeddings (see Sec. 5.3).

\textbf{Ranking Groups}

For each detected group, we calculate the density of the group based on (Euclidean) distance of each reviewer in the group with the group’s centroid in the embedding space. An average of all distances is taken as a measure of spamicity of the group. Let \( i \) be the vector representation of reviewer \( i \) in the embedding space. The group spam score \( \text{Spam}(g) \) of group \( g \) is measured as:

\[
\text{Spam}(g) = \frac{1}{|R(g)|} \sum_{i \in R(g)} \left[ i - \frac{1}{|R(g)|} \sum_{i \in R(g)} i \right]^2
\]
### Table 2: Statistics of four datasets.

<table>
<thead>
<tr>
<th>Dataset</th>
<th># Reviews</th>
<th># Reviewers</th>
<th># Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>YelpNYC</td>
<td>359052</td>
<td>160225</td>
<td>923</td>
</tr>
<tr>
<td>YelpZIP</td>
<td>608598</td>
<td>260227</td>
<td>5044</td>
</tr>
<tr>
<td>Amazon</td>
<td>10261</td>
<td>1429</td>
<td>900</td>
</tr>
<tr>
<td>Playstore</td>
<td>325424</td>
<td>321436</td>
<td>192</td>
</tr>
</tbody>
</table>

### 5 Experimental Results

#### Statistical validation.
To measure the statistical significance of each component (say, products reviewed by the group members) of Hypothesis 1 (Sec. 3.2), we randomly generate pairs of reviewers (irrespective of the groups they belong to) and measure how their co-reviewing patterns (cumulative distribution) are different from the case if a pair of reviewers co-occur together in the same group. We hypothesize that both these patterns are different (whereas null hypothesis rejects our hypothesis). We observe that the difference is statistically significant as $p < 0.01$ (Kolmogorov-Smirnov test). See Supplementary [Dhawan et al. 2019] for more discussion. We then perform evaluation in two stages – quality of the detected groups, and quality of the ranking algorithms.

#### 5.1 Baseline Methods

We consider three existing methods (see Sec. 2 for their details) as baselines for both the evaluations – (i) GSBP [Wang et al. 2016], (ii) GGSPam [Wang et al. 2018b], and (iii) GSRank [Mukherjee et al. 2012].

#### 5.2 Evaluating Candidate Groups

Along with the three baselines mentioned above, we also consider two variations of DeFrauder as baselines for group detection: $\text{DeFrauder}_G$ constructs the attributed product-product graph $G$ based only on co-rating without considering the time of reviewing; and $\text{DeFrauder}_T$ constructs $G$

2. They were social media experts, and their age ranged between 25-35.


![Figure 2: CDF of (a) GS and (b) RCS for YelpNYC. The more the distance of a CDF (corresponding to a method) from y-axis, the better the performance of the method.](image-url)
Table 3: Performance of the competing methods: GGSpam [Wang et al. 2018b], GSBP [Wang et al. 2016], GSRank [Mukherjee et al. 2012], DeFrauderR, DeFrauderT, and DeFrauder. Number of groups detected ($|G|$) are mentioned after removing groups of size less than 2 (cyan regions). Accuracy for the group detection (white regions) and ranking (gray regions) is reported in terms of EMD (the higher, the better), and NDCG@50 (ND) respectively. DeFrauderR and DeFrauderT are used only for group detection. The ranking methods of all baselines are run on the groups detection by DeFrauder.

![Figure 3: Performance on YelpNYC. Baselines are run with their detected groups as well as with the groups (+D) detected by DeFrauder (same naming convention as in Table 3).](image1)

Figure 3: Performance on YelpNYC. Baselines are run with their detected groups as well as with the groups (+D) detected by DeFrauder (same naming convention as in Table 3).

![Figure 4: Parameter selection on YelpNYC. We vary each parameter keeping others as default. Since $\tau_l = 20$ produces best results for group detection, we kept this value for ranking as well.](image2)

Figure 4: Parameter selection on YelpNYC. We vary each parameter keeping others as default. Since $\tau_l = 20$ produces best results for group detection, we kept this value for ranking as well.

6 Conclusion

In this paper, we studied the problem of fraud reviewer group detection in customer reviews. We established the principle of coherence among fraud reviewers in a group in terms of their co-reviewing patterns. This paper contributed in four directions: Datasets: We collected and annotated two new datasets which would be useful to the cybersecurity community; Characterization: We explored several group-level behavioral traits to model inter-personal collusive dynamics in a group; Method: We proposed DeFrauder, a novel method to detect and rank fraud reviewer groups; Evaluation: Exhaustive experiments were performed on four datasets to show the superiority of DeFrauder compared to five baselines.

Acknowledgements

The work was partially funded by Google Pvt. Ltd., DST (ECR/2017/001691) and Ramanujan Fellowship. The authors also acknowledge the support of the Infosys Centre of AI, IIIT-Delhi, India.
References


