Spotting Suspicious Reviews via (Quasi-)clique Extraction

Paras Jain, Shang-Tse Chen, Mozhgan Azimpourkivi†, Duen Horng Chau, Bogdan Carbunar†
Georgia Tech, †Florida International University
{paras, schen351, polo}@gatech.edu, †{mazim003, carbunar}@cs.fiu.edu

Abstract—How to tell if a review is real or fake? What does the underworld of fraudulent reviewing look like? Detecting suspicious reviews has become a major issue for many online services. We propose the use of a clique-finding approach to discover well-organized suspicious reviewers. From a Yelp dataset with over one million reviews, we construct multiple Reviewer Similarity graphs to link users that have unusually similar behavior: two reviewers are connected in the graph if they have reviewed the same set of venues within a few days. From these graphs, our algorithms extracted many large cliques and quasi-cliques, the largest one containing a striking 11 users who coordinated their review activities in identical ways. Among the detected cliques, a large portion contain Yelp Scouts who are paid by Yelp to review venues in new areas. Our work sheds light on their little-known operation.

I. INTRODUCTION

Review-centric online services like Yelp and TripAdvisor crowdsource the job of reviewing businesses. The popularity and influence of reviews make such sites ideal targets for malicious behaviors: businesses commission fraudulent reviews to artificially boost their ratings. An estimated 16% of Yelp restaurant reviews are fraudulent [1].

Identifying suspicious review behaviors is critical to maintaining the integrity of online services and protecting their users. However, this task is challenging, as fraudsters’ strategies can change rapidly. Crowdsourcing services such as Freelancer, Fiverr and Amazon Mechanical Turk are exploited for recruiting experienced review writers at a massive scale for nefarious purposes [2].

Recent research started to investigate network-based techniques for uncovering organized fraud by analyzing the link structures among potential fraudsters. For example, NetProbe uses an inference algorithm to find “near bipartite cores” formed among fraudsters and their accomplices on eBay [3].

More recently, Vlasselaer et al. find rectangles in bipartite graphs to detect social security fraud [4].

Interestingly, even though clique [5] and quasi-clique [6] have long been hinted as one of the strongest tell-tale signs of fraud, no prior work has studied if they indeed exist in online review websites like Yelp, where we can create a graph where each node represents a user, and an edge connects two users if they have reviewed common venues.

Fig. 1: Example suspicious clique formed among reviewers, found in a (6,5)-graph extracted from the Yelp data. Two reviewers are linked when they have reviewed the same 6 venues (or more) within 5 days.

II. EXTRACTING (QUASI-)CLIQES

The Yelp Review Dataset. We use the dataset from the Yelp Dataset Challenge which contains 42,153 venues and 1,125,458 reviews. Yelp did not specify whether they filtered the dataset but it would be reasonable to assume that they have only included publicly listed reviews in the dataset.

Building K-D Graphs to Uncover Suspicious Links. We extract a set of (k, d)-graphs from the raw Yelp data, originally formatted as a list of JSON objects, varying the k and d parameters. We define a (k, d)-graph to be an undirected
graph, where vertices represent users, and an edge exists between two vertices if the corresponding users reviewed at least \( k \) venues in common, and the reviews for each venue were posted at most \( d \) days apart (see Table I).

**Quasi-clique extraction.** We extract cliques and quasi-cliques from the set of \((k,d)\)-graphs. Cliques are complete sub-graphs of undirected graphs. Quasi-cliques are sub-graphs with edge densities no less than a fixed threshold [5].

Identifying cliques is NP-hard. The Bron-Kerbosch algorithm finds maximal cliques and is based on the Branch-and-Bound technique. Most real-world datasets produce sparse graphs, allowing Bron-Kerbosch to find maximal cliques faster and with lower time bounds. Larger cliques with higher \( k \) (more venues) and lower \( d \) values (tighter time bound) are more suspicious.

To extract quasi-cliques, we utilize the method proposed in [5], which uses a greedy way to grow a quasi-clique, along with a clever pruning technique. Quasi-cliques of size 11 and 12 were found in the Yelp dataset (see Table II). Larger cliques with higher \( k \) (more venues) and lower \( d \) values (tighter time bound) are more suspicious.

We manually inspected some flagged users, and were surprised that they are *Yelp Scouts* who are paid by Yelp to review venues in new areas. In the \((6,5)\)-graph, 31% of users were Yelp Scouts.

This is a significant discovery; no prior study has revealed how these Scouts operate, how they choose which venues to visit, and what kinds of reviews they write (positive or negative)? Our work sheds light on these little-known activities, which are highly organized both in timing and in venue selection. While they may not be suspicious, they are certainly unnatural, and possibly controversial!

**III. Conclusions & Next Steps**

It is alarming to find large cliques from the Yelp data, which are likely suspicious. But it is also critical to devise methods that reduce the false alarm rates to the minimum possible.

We plan to incorporate other rich signals from the Yelp data to help with this, such as by analyzing review text, and the spatial and temporal relationships among reviewed venues (e.g., it would be impossible for a user to visit a venue in the US and another in Asia on the same day).

**Acknowledgment**

This work was supported in part by NSF grant CCF-1101283.

**References**

[1] M. Luca and G. Zervas. “Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud,” *Harvard Business School NOM*, vol. 56, no. 1, pp. 3–16, 2010.

[2] G. Lubin, “The Illegal Way To Improve Your Rating On Yelp. Business Insider,” 2012. [Online]. Available: http://www.businessinsider.com/the-illegal-way-to-improve-your-rating-on-yelp-2012-2

[3] S. Pandit, D. H. Chau, S. Wang, and C. Faloutsos, “Netprobe: a fast and scalable system for fraud detection in online auction networks,” in *WWW*, 2007, pp. 201–210.

[4] V. Van Vlasselaer, L. Akoglu, T. Eliassi-Rad, M. Snoeck, and B. Baesens, “Guilt-by-constellation: Fraud detection by suspicious clique memberships,” in *HICSS*, 2015.

[5] T. Uno, “An efficient algorithm for solving pseudo clique enumeration problem,” *Algorithmica*, vol. 56, no. 1, pp. 3–16, 2010.

[6] C. Bron and J. Kerbosch, “Algorithm 457: finding all cliques of an undirected graph,” *Commun ACM*, vol. 16, no. 9, pp. 575–577, 1973.

A user’s Yelp Scout status is determined from a badge on their profile.