Detecting Suspicious Following Behavior in Multimillion-Node Social Networks

Meng Jiang
Dept. of Computer Science
Tsinghua University
jm06@mails.tsinghua.edu.cn

Peng Cui
Dept. of Computer Science
Tsinghua University
cuip@tsinghua.edu.cn

Alex Beutel
Dept. of Computer Science
Carnegie Mellon University
abeutel@cs.cmu.edu

Christos Faloutsos
Dept. of Computer Science
Carnegie Mellon University
christos@cs.cmu.edu

Shiqiang Yang
Dept. of Computer Science
Tsinghua University
yangshq@tsinghua.edu.cn

ABSTRACT
In a multimillion-node network of who-follows-whom like Twitter, since a high count of followers leads to higher profits, users have the incentive to boost their in-degree. Can we spot the suspicious following behavior, which may indicate zombie followers and suspicious followees? To answer the above question, we propose CatchSync, which exploits two tell-tale signs of the suspicious behavior: (a) synchronized behavior: the zombie followers have extremely similar following behavior pattern; because, say, they are generated by a script; and (b) abnormal behavior: their behavior pattern is very different from the majority. Our CatchSync introduces novel measures to quantify both concepts and catches the suspicious behavior. Moreover, we show it is effective in a real-world social network.

Categories and Subject Descriptors
J.4 [Computer Application]: Social and Behavioral Sciences

Keywords
social graph, zombie follower, synchronized behavior

1. INTRODUCTION
In social networks, the trustworthiness of marketers and the popularity of celebrities is measured by how many followers they have. Branding accounts, celebrities, and even grass-root users need to attract as many followers as they can. Many companies abuse social networks by creating and selling fake accounts that act as “zombie followers”, i.e., accounts who mindlessly follow others. This phenomenon creates distorted images of popularity and trustworthiness, with unpleasant or even dangerous effects to honest users.

To address this problem, instead of trying to understand the behavior that the zombie followers appear to have (e.g., duplicate tweets [2], malicious urls [7]), we propose to study and detect the behavior that they must have (e.g., follow and get followed) to achieve their monetary goals. In more detail, the zombie followers exhibit behavior that is (a) synchronized: they often follow the very same accounts and (b) abnormal: their behavior pattern is very different from the majority. It is exactly these two properties that we propose to exploit, to spot the zombie followers.

In our proposed CatchSync, we give a novel way to measure the synchronicity and the normality of a group of users and spot the outliers. We extensively evaluate the proposed method on Tencent Weibo (one of the largest microblogs in China). The experimental results demonstrated that the proposed CatchSync can spot the suspicious nodes.

2. OUR APPROACH
Here we first give the problem definition of suspicious following behavior detection: given a directed graph of N nodes in the node set U, find a set of zombie followers U_{sync} that have synchronized and abnormal behavior. The word “synchronized” means the followers connect to the very similar users, and “abnormal” means their behavior pattern is very different from the majority of follower nodes.

We define p(u) as the feature vector of node u. In this paper, we choose the degree values (out-degree and in-degree) and HITS scores (hubness and authoritativeness) [3] for two reasons: these features are fast to compute, as well as easy to plot. Figure 1(a) shows a 2D feature space (out-degree vs hubness) of all the follower nodes in Tencent Weibo. As our experiments show, these features work well in pin-pointing suspicious nodes. We denote by F(u) the set of node u’s followees and by d(u) = |F(u)| u’s out-degree. We define the synchronicity of node u as the average similarity of the feature vectors between each pair of u’s followees (v, v’):

\[ \text{sync}(u) = \frac{\sum_{(v,v') \in F(u) \times F(u)} p(v) \cdot p(v')} {d(u) \times d(u)} \]  \hspace{1cm} (1)

Also, we define the normality of u as the average similarity of the feature vectors between each pair of u’s followees and other nodes (v, v’):

\[ \text{norm}(u) = \frac{\sum_{(v,v') \in F(u) \times U} p(v) \cdot p(v')} {d(u) \times N} \] \hspace{1cm} (2)

Figure 1(b) shows the synchronicity-normality plot, in which we can spot outliers over the majority. The outliers have the largest synchronicity scores and smallest normality scores,
indicating that their behavior patterns are synchronized and abnormal. In CATCHSYNC we use a distance-based anomaly detection method to catch the suspicious nodes.

In Figure 2 we compare the precision and recall of CATCHSYNC against that of Graclus [1] and SpokEn [6]. We tuned the number of clusters for Graclus and the number of communities for SpokEn to achieve the best performance. From this experiment, we can clearly see that CATCHSYNC is extremely effective at detecting this suspicious behavior, while successfully catching very few false positives. Both its precision and recall exceed those of its competitors significantly.

Conclusion: CATCHSYNC has a very high recall of over 96% and significantly outperforms all other approaches. Again, CATCHSYNC did not use any of the information that we used to label the nodes.

<table>
<thead>
<tr>
<th></th>
<th>Nodes</th>
<th>Edges</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNTHETIC</td>
<td>1M / 2M / 3M</td>
<td>4M / 8M / 12M</td>
</tr>
<tr>
<td>WEIBO</td>
<td>117,288,075</td>
<td>3,134,074,580</td>
</tr>
</tbody>
</table>

Table 1: The real-world social datasets and synthetic data.

Detection Effectiveness: Synthetic data allows us to have clearly labelled regular “not suspicious” and injected “suspicious” nodes, and is easily reproducible. In Figure 2 we present the precision and recall of CATCHSYNC against that of Graclus [1] and SpokEn [6]. We tuned the number of clusters for Graclus and the number of communities for SpokEn to achieve the best performance. From this experiment, we can clearly see that CATCHSYNC is extremely effective at detecting this suspicious behavior, while successfully catching very few false positives. Both its precision and recall exceed those of its competitors significantly.

**5. REFERENCES**


