Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 556 – 562

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Novel Graph Centrality Based Approach to Analyze Anomalous Nodes with Negative Behavior

Ravneet Kaur[a*], Mankirat Kaur[a*], Sarbjeet Singh[a]

[a]*Computer Science Engineering, University Institute of Engineering and Technology, Panjab University, Chandigarh, India*

Abstract

Detection of different kinds of anomalous behaviors originating from negative ties among actors in online social networks is an unexplored area requiring extensive research. Due to increase in social crimes such as masquerading, bullying, etc., identification and analysis of these activities has become need of the hour. Approaches from two separate, yet, similar research areas, i.e. anomaly detection and negative tie analysis, can be clubbed together to identify negative anomalous nodes. Use of best measures from centrality based (negative ties) and structure based approaches (anomaly detection) can help us identify and analyze the negative ties more efficiently. A comparative analysis has been performed to detect the negative behaviors in online networks using different centrality measures and their relationship in curve fitting anomaly detection techniques. From results it is observed that curve fitting analysis of centrality measures relationship performs better than independent analysis of centrality measures for detecting negative anomalous nodes.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Anomaly; Centrality; Negative Ties; Social Networks.

1. Introduction

In recent years, Online Social Networks have attracted a lot of population owing to its basic feature of bringing

* Corresponding author. Tel.: +91-977-999-1701;
E-mail address: ravneets48@gmail.com
* Corresponding author. Tel.: +91-946-354-3880;
E-mail address: mannsunshine09@gmail.com

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.102

together the people from different cultures at a common platform. But their growing popularity not only influenced different domains positively but also led to their extensive misuse like, sending spam emails, creating fake profiles, sending of unnecessary friend requests, etc. Similarly, the presence of negative ties among different users due to the existence of frequent set of negative social behavior towards other users is also on the rise. Nowadays, a lot of research is being focused on detection and analysis of these types of anomalous and negative activities[1-6].

Different centrality based measures like, degree, status[7], PN centrality[8], etc. were proposed by many researchers to identify the negative nodes and ties. The existence of negative nodes in online networks represents an unusual activity which as per the definition of anomaly[9,10] could be categorized as abnormal. Therefore, a number of anomaly detection techniques can also be applied for identifying such negative nodes. A better approach could also be developed by merging the techniques from two domains.

In this paper, a novel graph based approach has been proposed which uses degree and PN centrality as graph metrics in fitting curves to spot and rank the negative anomalous nodes.

The remaining paper is structured into different sections. Section 2 discusses the related work already performed in the respective domains of negative tie analysis and anomaly detection. Section 3 describes the novel approach followed to detect negative anomalous nodes followed by the Experimental analysis in Section 4. Finally, the paper has been concluded in Section 5 with few future directions.

2. Related Work

2.1. Centrality measures to Analyze negative ties

The term centrality refers to the central element or actor in any domain of knowledge. Likewise, in social networks, concept of centrality defines the most central and influential node in the network through which most of the information flows. Various centrality measures were proposed to analyze ties in networks such as, degree, betweenness and closeness centrality given by Freeman[11], and eigenvector centrality given by Bonacich[12].

Due to the difference in characteristics of flow in positive and negative tie networks, some of these measures are not applicable in identifying negative nodes. Hence, many new measures such as degree, status[7], PII[13] and PN[8] centrality were developed to analyze both types of ties simultaneously.

Degree measure calculates the overall degree of the node by summing the number of positive and negative ties of actor whereas status measure calculates the status of an actor by assigning the elements of eigenvector of adjacency matrix as the scores of actors[7]. PII measure calculates the power possessed by actor by analyzing its dependence of resources and information on other actors in political network of allies and adversaries[13]. PN measure calculates the centrality of actor contributed by direct as well as indirect positive and negative links. Out of these four measures PN centrality was able to identify maximum outsiders in different networks[8].

2.2. Structure based Techniques to detect anomalies

For detecting unusual activities in social networks, different anomaly detection approaches categorized under behavior based[14-16] or structure based scenario have been proposed by various researchers. Out of these, structure based approaches[17-19] seems to be more beneficial as they work on the structural characteristics of the network which a user cannot manipulate. The structural properties in a network like, the number and type of connections among nodes, centrality values etc. are those which cannot be fabricated and denied by a user hence, becomes important and significant to be worked upon.

A number of researchers have incorporated different metrics in curve fitting approaches using regression to detect various anomalies. For instance, Akoglu et. al.[18] proposed an Oddball algorithm which used various power laws to detect different type of anomalies. Likewise, Reza et. al.[19] introduced the use of average betweenness centrality (ABC) and community cohesiveness to predict the anomalous nodes and it was shown that the relation between ABC and number of edges was able to identify anomalies more accurately. Rezai et. al.[20] also evaluated the results of N vs. E on Twitter data set. Similarly, Henderson et al.[21] studied a number of already existing node-based and egonet-based characteristics recursively by calculating some aggregate values over the already existing features.