Accepted Manuscript

A multi-criteria detection scheme of collusive fraud organization for reputation aggregation in social networks

Bo Zhang, Qian Zhang, Zhenhua Huang, Meizi Li, Luqun Li

PII: S0167-739X(16)30836-6
DOI: https://doi.org/10.1016/j.future.2017.09.027
Reference: FUTURE 3682

To appear in: *Future Generation Computer Systems*

Received date : 23 December 2016
Revised date : 6 August 2017
Accepted date : 10 September 2017

Please cite this article as: B. Zhang, Q. Zhang, Z. Huang, M. Li, L. Li, A multi-criteria detection scheme of collusive fraud organization for reputation aggregation in social networks, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.09.027

A Multi-Criteria Detection Scheme of Collusive Fraud Organization for Reputation Aggregation in Social Networks

Bo Zhang[1], Qian Zhang[1], Zhenhua Huang[2], Meizi Li[1,2], Luqun Li[1]

[1]College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, PR China
[2]College of Electronics and Information Engineering, Tongji University, Shanghai, 201804, PR China

Corresponding author: Bo Zhang, Tel: +8613524186012, E-mail address: zhangbo@shnu.edu.cn

Abstract In social networks, reputation aggregation is an effective approach for recognizing malicious behaviors and individuals. However, organized collusive fraud to obtain a high reputation is the most common and most harmful type of widespread network attack. Therefore, countering the collusion in reputation aggregation systems and further detecting the collusive fraud organizations (CFO) is a significant challenge. In this study, we propose a multi-criteria detection scheme of collusive fraud organization, named MD-CFO, to identify CFO in social networks. This scheme is based on a new universal reputation aggregation method, which includes the calculation of a reputation score and a universal factor. Moreover, five detection criteria and their corresponding factors, i.e., the rating difference fraud factor, rating frequency fraud factor, collaborative behavior fraud factor, suspicious relationship fraud factor, and CFO factor, are used to evaluate the likelihood of being a colluder. Furthermore, we propose three algorithms for detecting CFO and colluders. To prevent false-positive detection results, a correction mechanism called time slice verification (TSV) is used to certify a node's likelihood of suspicion or fraud in a series of time slices, thereby excluding honest nodes from CFO detection. Finally, empirical simulations are used to test the feasibility and effectiveness of our scheme.

Keywords: social network; reputation aggregation; collusive fraud organization detection; multi-criteria; false positive

1. Introduction

The rapid explosion in social networking services (SNSs) has facilitated communication with friends and strangers, such as the sharing of feelings, items, or experiences, and SNSs have become highly popular [1, 2]. In most cases, people experience happiness during social interactions, and they can ignore the potential risks of SNS. Unfortunately, not everyone is honest on SNSs. Malicious users can employ anonymous attacks for their own benefits, and deception is an unavoidable threat in SNS management.

Reputation is used to reflect past trustworthiness and predict the future likelihood of an individual remaining reliable, and it has been utilized as an effective and feasible solution for security management in online networks [3, 4, 36, 37, 38]. A reliable reputation system can determine whether each member of a community is trustworthy. In reputation-based systems, deciding whether an individual is trustworthy can be assessed using applications that consider the context of future decisions. However, the benefits of high reputation, such as attracting more potential buyers to business websites or acquiring more fans for micro-blog websites with a higher impact, may tempt immoral people to engage in fraud, i.e., slandering, self-inflation, and collusive cheating, thereby obtaining high reputation for themselves or slandering their rivals [7-8]. Furthermore, organized collusive fraud, rather than individual deception, is used widely in SNS reputation aggregation because organized collusion can cause more damage than independent deception [5, 6, 7, 9, 40, 41]. Therefore, how to accurately recognize collusive fraud organizations (CFOs), which organize and launch collusions in social networks during reputation aggregation, for reputation aggregation in the large-scale application of SNSs is the main issue to be addressed in this present study.

The general consensus is that reputation systems are essential for security management because risks are unavoidable in network environments. Due to the authentic and common sharable nature of reputation, users can acquire trustworthiness in terms of a specific target according to their reputation rates. Traditional studies of reputation aggregation in SNSs have focused on the development of computation models based on peer-to-peer (P2P) connections among users [10, 11, 12, 13]. A significant feature of these proposed approaches for reputation aggregation is that the computational method is based on public and common explicit expressions by users regarding who can be trusted and how much they can be trusted. From this perspective of global trustworthiness, reputation can be regarded as a collective judgment result based on the topological features of an SNS [1, 14, 15]. However, this type of aggregation method is vulnerable to fraud because all judgments are given equal weighting during reputation aggregation. For example, if unfair and malicious collusive attacks occur against individuals, the loss would be irreversible. Recently, many studies have addressed fraud detection, including methods based on neural networks, support vector machines, and decision trees.