UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Misbehaviour Detection Algorithms and Application in Social Networks

by Jun Yin

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

under the supervision of Guandong Xu

University of Technology Sydney
Faculty of Engineering and Information Technology

the September 2021

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, *Jun Yin* declare that this thesis, is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy*, in the *School of Computer Science*, *Faculty of Engineering and Information Technology* at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:

SIGNATURE: Signature removed prior to publication.

[Jun Yin]

DATE: 10th September, 2021

Dedication

To myself . . .

Acknowledgments

First of all, I would like to thank Prof. Guandong Xu, my principal supervisor, for his guidance, suggestion, and support throughout my doctoral program course at the University of Technology Sydney. Without his professional guidance and support, this work would not have been achieved.

I am also grateful to my previous co-supervisor Dr. Shaowu Liu for his constructive suggestions on my research work. I would like to pass my gratitude to my current co-supervisor and friend Dr. Qian Li, for her selfless help and suggestions on my work.

In addition, a thank you to Prof. Zhiang Wu of Nanjing Audit University, who introduced me to social network behaviour analysis, and whose enthusiasm for the research work had lasting effect.

Last but not least, I am thankful to my beloved husband, Wei Yuan, and my baby boy Adam J. Yuan, for their love and encouragement which helps me finish this thesis. I am also thankful to my parents and my parents in law for their support throughout my research studies.

Jun Yin
Sydney, Australia
September, 2021

Abstract

The liberty to contribute content freely has encouraged malicious users to exploit the social platforms (i.e., social networks and e-commerce platforms) for their benefits. Spammers, rumours, and some other unexpected activities are almost an appendage to all social platforms that disrupt the network order. We summarize these unexpected activities as misbehaviours in social platforms. To detect such social platform misbehaviours, machine learning is an expected method where modelling and algorithms are two significant elements. Such an interesting topic that has application prospects and research value has attracted the attention of many researchers, and some results have also been put forward in the literature.

In terms of spammer detection, because of the rich data types of e-commerce platform, such as score, comment content, and comment time, the mainstream detection methods rely on the above data to construct features on e-commerce platforms. For example, text-based features, behaviour features etc. in conjunction with some supervised learning algorithms like Naive Bayes, Decision trees etc. are the most frequently used combinations for spammer detection in e-commerce platforms. However, social networks are based on interaction data and are relatively deficient in data types, thus, spammer detection in social networks requires a detection framework that relies on relational data but is independent of content data. Along this line, the existing research attempts to define complex network features (e.g., degree, K-Core, PageRank, connected component, etc.) and interactive sequence-based features. Nevertheless, the deep semantic information hidden in the multi-relational networks has not been fully utilized.

Furthermore, rumour as another type of misbehaviours in social networks has been run through the whole evolutionary history of mankind. People maliciously disseminate rumours to increase awareness, slander others or cause panic, etc. To eliminate this issue, many researchers resort to detecting rumours in social networks. However, rumour detection is not sufficient to eliminate the negative impact, which also requires official institutions to provide the refutations. In practice, the number of rumours in social networks is too large, there is no need to refute some rumours with little or no concern. Therefore, an evaluation of the impact of the rumours in advance is essential.

To address the aforementioned research problems, a few approaches are proposed in the works introduced in this thesis.

- Based on the non-content data, we fully excavate the deep semantic information hidden in the heterogeneous network and define a series of user behaviour features using relational network data for spammer detection.

- Based on the graph embedding method, we propose a "Send-Receive" Role Separable Graph-Embedding Model (*RS-GEM*) to extract and fuse the hidden features of heterogeneous relations in multi-relational social networks to detect spammers.
- Inspired by deep sequential networks, we propose a "Multi-level Dependency Model" (*MDM*), which exploits user's behaviours in terms of long-term and short-term dependency from both individual-level and union-level to detect multi-relational social spammers.
- Before a rumour has an impact on social networks, we need to assess the possible impact it may have. Therefore, we devise a rumour influence prediction model *RISM* (Rumour Impact on Social Media) based on a popular rumour intensity formula to predict the impact of a newborn rumour.

Last but not least, since the global outbreak of COVID-19 in early 2019, COVID-19-related topics have become hot spots on social networking platforms. At the end of this thesis, we shall also analyze the COVID-19-related tweets on Twitter and get a preliminary understanding of the public's focus and sentiment trends during the pandemic.

Keywords: Multi-relational Social Network; Behaviour Analysis; Spammer Detection; Feature Construction; Rumour Analysis; Sentiment Analysis

List of Publications

Related to the Thesis :

1. Yin, J., Zhou, Z., Liu, S., Wu, Z., & Xu, G. (2018, June). Social Spammer Detection: A Multi-Relational Embedding Approach. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 615-627). Springer, Cham.

2. Yin, J., Liu, S., Li, Q., & Xu, G. (2019, October). Prediction and Analysis of Rumour's Impact on Social Media. In 2019 International Conference on Behavioral, Economic, Socio-cultural Computing (BESC) (pp. 1-6). IEEE.

3. Yin, J., Li, Q., Liu, S., Wu, Z., & Xu, G. (2020, November). Leveraging Multi-level Dependency of Relational Sequences for Social Spammer Detection. Neurocomputing, vol. 428, pp. 130-141.

4. Yin, J., Li, Q., Liu, S., & Xu, G. Social Network Analysis of Twitter User's Behaviour during COVID-19 Pandemic. Prepared to be submitted as a Journal Paper.

Others :

5. Zhou, Z., Liu S., Xu, G., Xie, X., Yin, J., Li, Y., & Zhang, W. (2018, June).Knowledge-Based Recommendation with Hierarchical Collaborative Embedding. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 222-234). Springer, Cham.

Table of Contents

List of Figures

List of Tables