Future Generation Computer Systems 86 (2018) 1456–1458

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Editorial

Social networking big data: Opportunities, solutions, and challenges

Sancheng Peng[a,b], Shui Yu[c,d,*], Peter Mueller[e]

[a] School of Cyber Security, Guangdong University of Foreign Studies, Guangzhou, Guangdong Province, 510420, PR China
[b] Laboratory of Language Engineering and Computing, Guangdong University of Foreign Studies, Guangzhou, Guangdong Province, 510420, PR China
[c] School of Computer and Educational Software, Guangzhou University, Guangzhou, Guangdong Province, 510006, PR China
[d] School of Information Technology, Deakin University, Australia
[e] IBM Zurich Research Laboratory, Switzerland

ARTICLE INFO

Keywords:
Social networking big data
Security
Trust
Privacy
Social network analysis

ABSTRACT

Social networking big data is a collection of extremely big data sets with great diversity in social networks. Social networking big data is also a core component for the social influence analysis and the security. However, current work on social networking big data focuses on information processing, such as data mining and analysis. There are two important issues for social networking big data, one is how to conduct social network analysis; the other is how to ensure security. This special issue aims to solicit original research that discuss foundational theories, new technologies, security, trust and privacy of social networking big data; and to provide a review on the progress in opportunities, solutions, and challenges of social networking big data.

1. Introduction

Social networking big data [1] is a collection of very huge data sets with a great diversity of types from social networks (e.g., Facebook, WeChat). The emerging paradigm of social networking and big data provide enormous novel approaches to efficiently adopt advanced networking communications and big data analytic schemas by using the existing mechanism. The rapid development of social networking big data brings revolutionary changes to our daily lives and global business, which has been addressed by recent research. However, attackers are taking advantages of social networks to achieve their malicious goals, making the security issue a critical concern when we use social networking big data in practice.

There are two important aspects of social networking big data due to the complexity and diversity. One is how to conduct social network analysis based on big data; the other is how to use big data analytic technique to ensure security of social networks using various security mechanisms. Current work on social networking big data focuses on information processing, such as data mining and analysis [2,3]. However, security, trust and privacy of social networking big data are remarkably significant for current researchers and practitioners to address and seek efficient methods to different threats. The special issue concentrates on the challenging topic "Social Networking Big Data", and aims to solicit original research papers that discuss foundational theories, new technologies, security, trust and privacy of social networking big data [4].

In fact, social networking big data has become essential components of various distributed services, applications, and systems [5], including viral marketing, influential bloggers finding, information retrieval, online advertising, sentiment analysis or opinion mining, personalized recommendation [6], opinion leader finding, malware propagation containing, etc. In addition, social networking big data focuses on the collection of big data from social networks, big data preprocessing, selection of evaluation metrics, measuring social influence, design of influence maximization algorithm, performance analysis on related algorithm or model [7,8].

The special issue of FGCS is dedicated to the topics of social networking big data: opportunities, solutions, and challenges as follows.

- Fundamentals: Modeling on social influence with big data; social influence analysis with big data; modeling on the characteristics and mechanisms of social networks; influence maximization problem with big data; dynamic social influence analysis in large-scale social networks; social influence analysis in heterogeneous social network; casual relationship in large-scale social networks [9,10].
- Technologies: Recommendations and advertising in social networks with big data; influence propagation in large-scale social networks; user behavior analysis with social influence evaluation; methods for distinguishing the positive, negative, and controversy influence; models, methods, and tools for influence propagation; community detection methods

[*] Corresponding guest editor.
E-mail address: syu@deakin.edu.au (S. Yu).

https://doi.org/10.1016/j.future.2018.05.040
0167-739X/© 2018 Published by Elsevier B.V.

with big data; modeling community influence in social networks; impact of social networks on human social behavior; human behavior analysis in social networks with big data; impact of social networks on human social behavior [5,11].

- Security: Modeling on malicious information propagation with social influence analysis; secure social networking application with social influence analysis; prevention of malware propagation in social networks; modeling on the secure mechanisms of social networks; novel secure solutions for designing; supporting and operating social networks; threat and vulnerability analysis in social networks; secure social network architecture with big data; secure social networking applications with big data; security design for social networks in big data; models, methods, and tools for testing the security of social networks; spam problems in social networks with big data; detection for malicious information propagation in social networks [12–15].
- Trust: Trust evaluation in social networks with big data; trust management in social networks with big data; models, methods, and tools for testing the trust of social networks [16,17].
- Privacy: Privacy in management and analysis of social networking big data; privacy protection in social networks with big data; models, methods, and tools for protecting the privacy of social networks [18–20].

The goal of this special issue is to encourage research and development in social networking big data. In response to the CFP (call for papers), we were pleased to see 35 submissions from 10 countries and areas all over the world, which was far more than we expected. The large number of submissions also reflects the importance of this research field. After a careful review, seven excellent papers have been selected from a good number of quality submissions received. A detailed overview of the selected papers is given as follows.

The first four articles fall in applications for social network analysis with big data. The first paper, *A Novel Context-aware Recommendation Algorithm with Two-level SVD in Social Networks*, by Cui et al. [21], proposes a context-aware recommendation algorithm with two-level SVD, named CTLSVD. The second paper, *An Indicative Opinion Generation Model for Short Texts on Social Networks*, by Zhao et al. [22], develops an indicative opinion generation model utilizing BM25 to identify the important text and using syntactic parsing to obtain the brief opinion representation. The third paper, *Mining of Marital Distress from Microblogging Social Networks: A Case Study on Sina Weibo*, Mao et al. [23], proposes a model, named discovering marital distress (DMD), to discover the crowds with marital distress.

The second category is made up of two papers about social network analysis in big data. The fourth paper, *Maximizing Positive Influence Spread in Online Social Networks via Fluid Dynamics*, by Wang et al. [24], proposes an influence spread model called Fluidspread, to characterize the influence spread process as the fluid update process in three dimensions: the fluid height difference, the fluid temperature and the temperature difference, by using the fluid dynamics theory. This fifth paper, *Incremental Term Representation Learning for Social Network Analysis*, by Peng et al. [25], presents a method that can factorize co-occurrence matrix to query the latest semantic vectors. It divides the streaming social network data into old and updated training tasks respectively, and factorizes the training objective function based on stochastic gradient methods to update vectors.

The third category is about privacy protection in social networks with big data. The sixth paper, *On the Limitations of Existing Notions of Location Privacy*, by Dong et al. [26], illustrates the limitations of existing notions by constructing such scenarios, and introduces a formal definition on location privacy by quantifying the distance between the prior and posterior distribution over the possible locations. Furthermore, a near-optimal obfuscation mechanism is constructed by solving an optimization problem.

The fourth category is about security design for social networks in big data. Last but not least, the seventh paper, *PRECISE: Identity-Based Private Data Sharing with Conditional Proxy Re-encryption in Online Social Networks*, by Huang et al. [27], proposes an identity-based private data sharing scheme with big data for on-line social networks. It adopted attribute-based conditional proxy re-encryption to guarantee that only the data disseminators whose attributes satisfy access policy can disseminate the data to their own social space.

We hope this special issue would provide some in-sight into recent research in social networking big data. This special issue also provides certain guidance for academic and industry advances, and these accomplishments are regarded as a basis toward future research directions, and vital commercial applications. We would like to thank all the authors who submitted their research papers to this special issue. We would also like to thank all the anonymous reviewers who read the papers for their time and effort, and offer good comments and suggestions to the authors to improve their papers. In particular, we would like to express our sincere appreciation to the Editor-in-Chief, Professor Peter Sloot, for his constructive suggestions and timely guidance during the life cycle of this special issue.

Finally, we hope potential readers will be fond of the papers in this special issue, and further explore these promising and uncharted research fields for social networking big data.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China under Grant Nos. 61379041 and 61728201, the Science and Technology Plan Project of Guangzhou under Grant No. 2018-1002-SF-0434, and the Bidding Project of Laboratory of Language Engineering and Computing under Grant No. LEC2017ZBKT001.

References

[1] S. Peng, G. Wang, D. Xie, Social influence analysis in social networking big data: Opportunities and challenges, IEEE Netw. 31 (1) (2017) 11–17.
[2] M. Wang, M. Xiao, S. Peng, G. Liu, A hybrid index for temporal big data, Future Gener. Comput. Syst. 72 (2017) 264–272.
[3] S. Yu, M. Liu, W. Dou, X. Liu, S. Zhou, Networking for big data: A survey, IEEE Commun. Surv. Tutor. 19 (1) (2017) 531–549.
[4] S. Yu, Big privacy: Challenges and opportunities of privacy study in the age of big data, IEEE Access 4 (2016) 2751–2763.
[5] S. Peng, Y. Zhou, S. Yu, L. Cao, J. Niu, Influence analysis in social networks: A survey, J. Netw. Comput. Appl. (2018) in press.
[6] M. Gan, R. Jiang, FLOWER: Fusing global and local associations towards personalized social recommendation, Future Gener. Comput. Syst. 78 (Part 1) (2018) 462–473.
[7] S. Peng, G. Wang, Y. Zhou, C. Wan, C. Wang, S. Yu, J. Niu, An immunization framework for social networks through big data based influence modeling, IEEE Trans. Dependable Secure Comput. (2017) in press.
[8] S. Peng, A. Yang, L. Cao, S. Yu, D. Xie, Social influence modeling using information theory in mobile social networks, Inform. Sci. 379 (2017) 147–159.
[9] S. Peng, S. Jiang, P. Yin, Modeling and propagation analysis on social influence using social big data, in: The 9th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2016), Zhangjiajie, China, November 16–18, 2016, pp. 279–291.
[10] S. Peng, M. Wu, G. Wang, S. Yu, Containing smartphone worm propagation with an influence maximization algorithm, Comput. Netw. 74 (2014) 103–113.
[11] X. Zhou, B. Wu, Q. Jin, User role identification based on social behavior and networking analysis for information dissemination, Future Gener. Comput. Syst. (2017) in press, available online.
[12] S. Peng, M. Wu, G. Wang, S. Yu, Propagation model of smartphone worms based on semi-Markov process and social relationship graph, Comput. Secur. 44 (2014) 92–103.

[13] S. Peng, S. Yu, A. Yang, Smartphone Malware and its propagation modeling: A survey, IEEE Commun. Surv. Tutor. 16 (2) (2014) 925–941.
[14] X. Xiao, R. Yan, R. Ye, S. Peng, Q. Li, S. Xi, Detecting code injection attacks on hybrid apps with machine learning, J. Internet Technol. 18 (4) (2017) 843–854.
[15] S. Peng, G. Wang, S. Yu, Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones, J. Comput. System Sci. 79 (5) (2013) 586–595.
[16] S. Chen, G. Wang, W. Jia, Cluster-group based trusted computing for mobile social networks using implicit social behavioral graph, Future Gener. Comput. Syst. 55 (2016) 391–400.
[17] W. Jiang, G. Wang, J. Wu, Generating trusted graphs for trust evaluation in online social networks, Future Gener. Comput. Syst. 31 (2014) 48–58.
[18] E. Luo, Q. Liu, J.H. Abawajy, G. Wang, Privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks, Future Gener. Comput. Syst. 68 (2017) 222–233.
[19] Q. Liu, G. Wang, F. Li, S. Yang, J. Wu, Preserving privacy with probabilistic indistinguishability in weighted social networks, IEEE Trans. Parallel Distrib. Syst. 28 (5) (2017) 1417–1429.
[20] T. Peng, Q. Liu, D. Meng, G. Wang, Collaborative trajectory privacy preserving scheme in location-based services, Inform. Sci. 387 (2017) 165–179.
[21] L. Cui, W. Huang, Q. Yan, F. Richard Yu, Z. Wen, N. Lu, A novel context-aware recommendation algorithm with two-level SVD in social networks, Future Gener. Comput. Syst. 86 (2018) 1459–1470.
[22] Q. Zhao, J. Niu, H. Chen, L. Wang, M. Atiquzzaman, An indicative opinion generation model for short texts on social networks, Future Gener. Comput. Syst. 86 (2018) 1471–1480.
[23] K. Mao, J. Niu, H. Chen, L. Wang, M. Atiquzzaman, Mining of marital distress from microblogging social networks: A case study on Sina Weibo, Future Gener. Comput. Syst. 86 (2018) 1481–1490.
[24] F. Wang, W. Jiang, X. Li, G. Wang, Maximizing positive influence spread in online social networks via fluid dynamics, Future Gener. Comput. Syst. 86 (2018) 1491–1502.
[25] H. Peng, M. Bao, J. Li, M.Z. Alam Bhuiyan, E. Yang, Incremental term representation learning for social network analysis, Future Gener. Comput. Syst. 86 (2018) 1503–1512.
[26] K. Dong, T. Guo, H. Ye, X. Li, Z. Ling, On the limitations of existing notions of location privacy, Future Gener. Comput. Syst. 86 (2018) 1513–1522.
[27] Q. Huang, Y. Yang, J. Fu, Precise: identity-based private data sharing with conditional proxy re-encryption in online social networks, Future Gener. Comput. Syst. 86 (2018) 1523–1533.

Dr. Sancheng Peng received his Ph.D. degree in computer science from Central South University, Changsha, China, in 2010. Currently, he is a full Professor with School of Cyber Security, and also with Laboratory of Language Engineering and Computing, Guangdong University of Foreign Studies. Dr Peng was the director of Network and Information Security Institute at Zhaoqing University. He has won many research grants, such as National Natural Science Foundation of China, Natural Science Foundation of Guangdong Province, and Postdoctoral Science Foundation of China. He was a Research Associate of City University of Hong Kong from 2008 to 2009. Professor Peng has published around three peer reviewed papers at various venues, such as IEEE Communications Surveys and Tutorials, IEEE Transactions on Dependable and Secure Computing, IEEE Network, Information Sciences, Journal of Network and Computer Applications, Future Generation Computer Systems, Computer & Security, and Computer Networks, Journal of Computer and System Sciences. He has organized or served many international conferences, such as ICYCS 2008, EUC 2011. He has served as TPC member for international conferences, such as TrustCom 2011, ICCVE 2013, EUC 2013, ICC 2014, ICNC 2014, ICA3PP 2015, SpaCCS 2016, and SpaCCS 2017. Dr. Peng is also a reviewer for many prestigious journals, such as IEEE Transactions on Parallel and Distributed Systems, IEEE Network, Information Sciences, Future Generation Computer Sciences, Computer Networks, Journal of Computer and System Sciences, and Journal of Computer Science and Technology.

Dr. Shui Yu is currently a Senior Lecturer (equivalent to Associate Professor in North America) of the School of Information Technology, Deakin University, Australia. Dr. Yu is active in research services in various roles. He services the editor board of the International Journal of Internet Services and Information Sciences. He is a reviewer for a number of prestigious journals, such as IEEE Transactions of Parallel and Distributed Systems, IEEE Transactions on Computer, IEEE Transactions on Wireless Communication. He services as TPC member for international conferences, such as INFOCOM 2013, AINA2012, MobiWac2011, and iCAST2011. Dr. Yu's current research interests include networking theory, network security, privacy and forensics, and mathematical modeling. He targets on narrowing the gap between theory and applications using mathematical tools. He has been publishing papers in high quality journals, such as IEEE Transactions on Information Forensics and Security, IEEE Transactions of Parallel and Distributed Systems, and IEEE Transactions on Mobile Computing. He is a Senior Member of IEEE.

Dr. Peter Mueller joined IBM Research as a Research Staff Member in 1988. His research expertise covers broad areas of distributed computing systems architecture, microwave technology, device physics, nano science and modeling. His current field of research is in the areas of data center storage security and reliability and the high frequency technology. Peter is a founding member and was the Chair of the IEEE ComSoc Communications and Information Systems Security Technical Committee (CIS-TC). In the course of his carrier he authored and co-authored more than 100 papers, 2 books, has been granted 10 patents and served as guest editor for many special issue publications. His affiliations include active society membership in IEEE, where he is Senior Member; the Society for Industrial and Applied Mathematics (SIAM); the Electrochemical Society (ECS); and the Swiss Physical Society (SPS).