

Digital Object Identifier 10.1109/ACCESS.2018.2817858

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: TRUST MANAGEMENT IN PERVASIVE SOCIAL NETWORKING (TruPSN)

With the rapid growth of mobile computing and social networking, social networks have extended their popularity from the Internet to mobile domain. Pervasive Social Networking (PSN) ensures social communications at any time and in any place with a universal manner. It supports online and instant (i.e., pervasive) social activities based on heterogeneous networks, e.g., the Internet, mobile cellular networks or self-organized networks or other networking technologies. It is treated as one of the killer applications in the next generation mobile networks and wireless systems (i.e., 5G). There are various applications over PSN. Typical examples include social chatting, gaming, rescuing, recommending and information sharing. Because group mobility is very common in modern life, PSN has become valuable for mobile users, especially when they are familiar strangers and often appear in the same vicinity. PSN greatly extends our experiences of social communications.

There are quite a number of vivid research activities related to PSN in both academia and industry. However, trust and reputation management has not been extensively considered in existing projects, although trust plays an important role in PSN for reciprocal activities among strangers. It helps people overcome uncertainty, makes wise decisions, avoids unnecessary risks, and engages in trust-related social behaviors. In the literature, trust and reputation mechanisms have been widely studied in various fields. However, traditional online social networking systems (e.g., Facebook) and current PSN research have not fully taken user trust into consideration. They have not comprehensively investigated how to manage trust in PSN in a holistic manner. A number of issues, such as trustworthy identification and authentication, PSN data communication security, user privacy preservation, trust relationship evaluation, evolution and enhancement, unwanted information control, privacy-preserving social data search and mining, user-device trust interaction, etc. have not been extensively studied. Pervasive social networking introduces additional challenges to track and resist malicious social behaviors in practice, especially when user privacy and PSN security should be seriously considered and stringently supported.

This Special Section aims at presenting advanced academic and industrial research results related to trust management

in PSN. We finally selected 11 articles after a rigorous review process for publication in this Special Section. These articles cover wide topics such as malicious social account detection, PSN data access control and protection, privacy preservation, trust evaluation and recommendation, social opinion mining, and so on. In what follows, we briefly introduce each article.

In the article “ProGuard: Detecting malicious accounts in social-network-based online promotions,” Zhou *et al.* proposed a system named ProGuard to detect malicious accounts in a variety of business activities based on online social networks. It achieves its detection goal by considering account general behaviors, recharging patterns, and currency usage. The experiments based on real world data collected from Tencent QQ demonstrated the effectiveness of ProGuard.

In the article “Secure pervasive social communications based on trust in a distributed way”, Huang *et al.* proposed two schemes to secure communication data in PSN purely based on local trust evaluated by PSN nodes in a distributed manner. They aimed to overcome the drawbacks of the data access control solutions based on a centralized server in order to support crucial PSN activities and enhance user privacy. Each node can control its data based on its trust in other nodes by applying Attribute-Based Encryption (ABE).

In the article “A secure system for pervasive social network-based healthcare”, Zhang *et al.* proposed two schemes to securely share health data with other nodes in PSN. The first one is an improved version of the IEEE 802.15.6 display authenticated association for mobile devices and resource-limited sensor nodes. The second one uses blockchain technique to share health data among PSN nodes.

In order to effectively establish key agreement among vehicles, Li *et al.* proposed an efficient physical layer key extraction method by utilizing received signal strength to generate secret keys in the article, “efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks”.

Feng *et al.* proposed a scheme for anonymous authentication on trust in PSN based on group signature in the article “Anonymous authentication on trust in pervasive social networking based on group signature,” for the purpose of secure authentication with anonymity and conditional traceability no

matter whether a trusted authority is available or not. For improving the efficiency of authenticity for a large number of messages, batch signature verification was further utilized to support scalability.

Shen *et al.* proposed a hierarchical evaluation system to support secure and trustworthy PSN in the article “Hierarchical trust level evaluation for pervasive social networking”. The system solves the problem of trust evaluation in PSN and guarantees the secure communications among trusted nodes.

Li *et al.* proposed a recommendation model named RM-UI in the article “A similarity scenario-based recommendation model with small disturbances for unknown items in social networks” for overcoming two issues: “cold start” and “excessively mature recommendation”. The authors derived the recommendation values of items from the probabilities calculated by a similar mature recommendation system during system initiation for solving the “cold start” issue. For overcoming “excessively mature recommendation”, RM-UI also recommends items with low recommendation probabilities to some extent to enable some items that can bring welfare to the recommendation system.

D2D network acts as a practical communication platform for PSN. In order to ensure trustworthy cooperation among D2D communication users, Yan *et al.* proposed a Trust-oriented Partner Selection Mechanism (TPSM) in the article “Trust-oriented partner selection in D2D cooperative communications” to avoid choosing the users with non-cooperative behaviors. Multi-dimensional trust relationships between sending users and cooperative users are evaluated by considering cognition trust, emotion trust, and behavior trust. The users are classified into reliable users, observed users, and unreliable users. With the above trust evaluation and user classification, an optimal partner selection mechanism was further proposed to support different scenarios.

For providing uniform trust management in PSN and reducing computational cost at the same time, Sharma *et al.* presented a pervasive trust management framework that can generate trust values between the users with a low cost of monitoring in the article “computational offloading for efficient trust management in pervasive online social networks using osmotic computing”. The proposed approach uses a flexible mixture model and applies the concept of osmotic computing to perform computational offloading in order to reduce the number of computations and save computational time.

In the article titled “Towards a trust prediction framework for cloud services based on pso-driven neural network”, Mao *et al.* introduced a hybrid prediction algorithm named PSO-NN by using Particle Swarm Optimization (PSO) to enhance Neural network (NN) for predicting the trust rates of cloud services in an accurate way by optimizing its initial settings.

Lv *et al.* studied opinioned posts in Sina Weibo in the article “Opinioned post detection in Sina Weibo” in order to overcome two challenges: short text in Sina Weibo and

the absence of ground-truth data for training models. They proposed a weakly supervised framework named Graph-based Opinioned Post Detector (GOPD) to detect the opinioned posts by utilizing three types of user interactions: reposting, responding, and referring. An Opinioned Similarity Graph (OSG) is constructed to describe the opinion similarity between posts through classification.

During the production of this Special Section, we experienced many interesting and novel ideas and reviewed a number of qualified research results. We would like to thank all authors and reviewers for their contributions to it. We believe trust management in PSN is a vivid and promising research topic worth our further exploration and investigation. We hope this Special Section is valuable for its readers and can benefit their future research and development. We will be very happy if further interests could be stimulated by reading the various perspectives presented herein.

ACKNOWLEDGMENT

This work was supported in part by the NSFC under Grant 61672410 and Grant U1536202, in part by the National Key Foundational Research and Development on Network and Space Security, China, under Grant 2016YFB0800704, in part by the Project Supported by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016ZDJC-06, in part by the 111 Project under Grant B08038 and Grant B16037, and in part by the Academy of Finland under Grant 308087.

ZHENG YAN

*School of Cyber Engineering
State Key Laboratory of Integrated Services Networks
Xidian University
Xi'an 710071, China
and
Department of Communications and Networking
Aalto University
Espoo 02150, Finland*

HONGGANG WANG

*Department of Electrical and Computer Engineering
University of Massachusetts at Dartmouth
Dartmouth, MA 02747-2300, USA*

LAURENCE T. YANG

*St. Francis Xavier University
Antigonish, NS B2G 2W5, Canada*

VALTERI NIEMI

*Department of Computer Science
University of Helsinki
FI 0014 Helsinki, Finland*



ZHENG YAN (M'06–SM'14) received the Ph.D. degree from the Helsinki University of Technology, Espoo, Finland. She is currently a Professor with Xidian University, Xi'an, China, a Visiting Professor with Aalto University, Finland, and a Research Fellow with the Academy of Finland. Her research interests include trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She is a Steering, Organization, and Program Committee Member for over 70 international conferences. She led the organization of the IEEE TrustCom/BigDataSE/ISPA-2015, IEEE CIT 2014, CSS 2014, IEEE CIT2017, ICA3PP2017, and NSS2017 international conferences. She is an Associate Editor of *Information Sciences*, *Information Fusion*, the IEEE INTERNET OF THINGS JOURNAL, the IEEE ACCESS Journal, *JNCA*, *Soft Computing*, *Security and Communication Networks*, and so on. She is a leading Guest Editor of over 20 reputable journals, including ACM TOMM, *Future Generation Computer Systems*, the IEEE SYSTEMS JOURNAL, MONET, and so on.



HONGGANG WANG received the Ph.D. degree in computer engineering from the University of Nebraska–Lincoln in 2009. He is currently an Associate Professor with the University of Massachusetts (UMass) at Dartmouth, where he is the Faculty Member of the Biomedical Engineering and Biotechnology Ph.D. Program, and where he has been a Faculty Member of the Data Science master's Program since 2015. His research was supported by DoT, UMass President Office, and the UMass Healey Grant. His research interests include wireless health, body area networks, and big data in mHealth, cyber and multimedia security, mobile multimedia and cloud, wireless networks, and cyber-physical system. He received the IEEE Multimedia Communications Technical Committee Outstanding Leadership Award in 2015 and the IEEE HEALTHCOM 2015 Outstanding Service Award. He also received the UMass Dartmouth Sponsored Research Recognition Award in 2015 and the Scholar of The Year Award (only one per year) from UMass Dartmouth. He serves as the TPC Chair or Co-Chair for several conferences, such as the TPC Chair for the 8th ICST/ACM International Conference on Body

Area Networks in 2013, a TPC Symposium Co-Chair for the IEEE Conference on Communications in 2015 (Mobile and Wireless Networking symposium), the TPC Chair for the IEEE HEALTHCOM 2015, a TPC Co-Chair for the IEEE ISCC 2015, and a TPC Track Co-Chair for the Cognitive, Cellular and Mobile Networks of the IEEE ICCCN 2014–2015. He also serves as a Steering Committee Co-Chair of the IEEE Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) and a TPC Co-Chair of the IEEE CHASE 2016, which is a leading international conference in the field of connected health. He is the Secretary of the IEEE COMSOC e-Health Committee. He serves as an Associate Editor for the IEEE TRANSACTION ON MULTIMEDIA and the IEEE TRANSACTIONS ON BIG DATA, an Associate Editor-in-Chief for the IEEE INTERNET OF THINGS JOURNAL, an Associate Technical Editor for *IEEE Communication Magazine*, and a Guest Editor for the IEEE IoT Journal special issue on IoT for Smart and Connected Health. His research was reported by media, such as USA ABC 6 TV and Standard Times Newspaper.



LAURENCE T. YANG received the B.E. degree in computer science and engineering from Tsinghua University, China, and the Ph.D. degree in computer science from the University of Victoria, Canada. He is currently a Professor with the School of Computer Science and Technology, Huazhong University of Science and Technology, China, and the Department of Computer Science, St. Francis Xavier University, Canada. His research includes parallel and distributed computing, embedded and ubiquitous/pervasive computing, and big data. He has published around 260 peer-reviewed international journal papers in the above areas of which 45% are on top IEEE/ACM TRANSACTIONS and journals; others are mostly published at Elsevier, Springer, and Wiley. He has been involved actively in conferences and workshops as a program/general/steering conference chair and a program committee member. He served as the Vice-Chair of the IEEE Technical Committee of Supercomputing Applications from 2001 to 2004, the Chair of the IEEE Technical Committee of Scalable Computing from 2008 to 2011, and the Chair of the IEEE Task force on Ubiquitous Computing and Intelligence from 2009 to

2013. In 2014, he was the Vice-Chair of the IEEE Canada Atlantic Section, where he is currently the Chair. He was in the steering committee of the IEEE/ACM Supercomputing conference series from 2008 to 2011, in the National Resource Allocation Committee of Compute Canada from 2009 to 2013, and the Scientific Committee Chair of the Engineering, Mathematics and Computing Science of Compute Canada from 2012 to 2013. He has been acting as an author/co-author or an editor/co-editor of over 25 books from well-known publishers. The book *Mobile Intelligence* (Wiley, 2010) received an Honorable Mention by the American Publishers Awards for Professional and Scholarly Excellence. He received several best paper awards, including the IEEE Best and Outstanding Conference Awards, one Best Paper Nomination, the Distinguished Achievement Award in 2005 and 2011, and the Canada Foundation for Innovation Award in 2003. He is the editor-in-chief of several international journals. He is serving as an Editor for many top international journals, such as the IEEE SYSTEMS, *Information Sciences* (Elsevier), *Information Fusion* (Elsevier), *Future Generation Computer Systems* (Elsevier), and *Big Data Research* (Elsevier). He has been invited to give around 32 keynote talks at various international conferences and symposia.



VALTERI NIEMI is currently a Professor of computer science with the University of Helsinki and leads the Secure Systems Research Group. He is also a Deputy Head of the Department of Computer Science. He has been a Professor of mathematics with the University of Vaasa from 1993 to 1997 and the University of Turku from 2012 to 2015. Between these two academic positions, he served for 15 years in various roles at the Nokia Research Center and was nominated as a Nokia Fellow in 2009. At Nokia, he was involved in wireless and mobile security, including cryptological aspects and privacy-enhancing technologies. He participated in the 3GPP SA3 (security) Standardization Group from its beginning, where he was the Chairman of the group from 2003 to 2009. He has published over 70 scientific articles, and he is a co-author of four books and over 30 patent families.

...