The Computer Journal Advance Access published December 23, 2014

doi:10.1093/comjnl/bxu151

Guest Editorial
Security, Trust and Risk in Multimedia Social Networks

Zhiyong Zhang*

Department of Computer Science, Henan University of Science and Technology,
Luoyang 471023, P. R. China
**Corresponding author: z.zhang@ieee.org*

Received 26 November 2014; revised 28 November 2014; accepted 29 November 2014
Handling editor: Chris Mitchell

With the rapid development of network socialization, multimedia social networks (MSNs) have increasingly emerged. These MSNs offer network tools, services and applications for multimedia content (e.g. electronic book, digital image, audio and video) that can be shared among users in the same group or between different groups within social networks. Many MSNs, such as video Youtube and audio SongTaste sharing networks, are increasingly widely used. However, easy digital content reproduction, convenient distribution and sharing of such content facilitated by open MSNs environments have enabled people to share and distribute valuable copyrighted digital content within social networks. Copyright infringement behaviour, such as illicit copying, malicious distribution, unauthorized usage and free sharing of copyright-protected digital content, will also become a much more common phenomenon. Some research frontiers on media content security in social networks applications have been in progress, including enhanced security mechanisms, methods and algorithms, trust assessment and risk management in social network applications, as well as social factors and soft computing in social media distributions. The special issue attempts to bring together researchers, content industry engineers and administrators resorting to the state-of-the-art technologies and ideas to protect valuable media content and services against security attacks and piracy exposure in the emerging social networks.

In the first section of the special issue, there are five original articles in the field of MSNs security, privacy and forensics. First, Patsakis *et al.* made a survey on the most significant security and privacy issues related to the exposure of multimedia content in online social network (OSN), and then discussed possible countermeasures and methods. In the second paper, Hui Zhu *et al.* attempted to explore privacy setting policies in OSN, and proposed a general stochastic model called diffusion model based on privacy setting with multiple diffusion mechanisms for OSN services. By a series of experimental simulations and analysis, the paper shows that the novel model can precisely describe the diffusion process. Next, Hong Zhu *et al.* highlighted an independent ℓ-Diversity principle, based on which a privacy-preserving data publication model is presented to prevent individual sensitive information disclosure in the corruption attack. The proposed model could prevent attacks from attackers who have known data publishing algorithms and have the corruption abilities. Followed by media content security and forensics in the section, Weitao Song *et al*. paid more attention to the type-flaw attacks detection and security protocol formalism. They introduced a multi-branch tag tree to establish a three-level model for detecting type-flaw attacks on security protocols. In the final fifth paper, considering an effective forensic analysis on digital images, the authors, Bin Yang *et al*., represented a novel shadow-based method, by which the fake shadow of the composites can be detected.

The special issue's second section focuses on MSNs trust and reputation issues, and also includes the following five selected papers. Ayesha Kanwal *et al*. have performed in-depth analyses of the existing trust models in the cloud environment, and presented panoramic taxonomies covering the state-of-the-art features. Furthermore, they have applied the proposed taxonomies as assessment criteria for the analysis of various trust models in the cloud domain. In addition, the emerging MSNs services and tools, in recent years, have generally facilitated convenient platforms for users to share multimedia content based on cloud. At the same time, some security-related burning issues, for instance deliberate and unintentional spreads of the copyrighted or negative digital content, have become very serious. Qingqi Pei *et al*. represented a strong and weak ties feedback-based trust model on the basis of the Weak Ties Theory of sociology. With regarding to the negative information in MSNs, Zhen Yang *et al*. provided a normalized cross entropy metric to determine whether a headline is sensational or not, by the literal consistency between the headline and its corresponding documents. Besides, as one of essential infrastructures of social networking, multi-hop wireless networks are facing with the internal multi-layer security threats. This is right the research motivation of the forth paper. For this, Hui Lin *et al*. put forward to a dynamic cross-layer reputation computation model named as CRM to dynamically characterize and quantify the actions of nodes in multi-hop wireless networks. Further, Prof. Kanliang Wang and I have explored the potential paths on the propagation of copyrighted content, and proposed an approach to mining credible potential paths in MSNs.

At last but not least, there are three research works involved with MSNs architecture, networking and disaster recovery. Natarajan V *et al*., in the first paper, made a systematic research on Stegobot, which is a special-purpose botnet for social networks. The authors presented an effective method to detect Stegobot hosts within a monitored social network, as well as a classification model constructed by using the profile level and content level analysis to improve the detection ability. As to the routing in MSNs, Guowei Wu *et al*. found that some nodes tend to be selfish or malicious. In order to address the issue, they proposed a fuzzy-based trust management technique for the context-based routing, and incorporated social trust metrics and quality of services metrics into the trust model. As a result, the proposed trust routing would balance the message overhead and delivery ratio as a lightweight protocol. More interestingly, in the last paper of the special issue, Danmei Niu considered how to quickly and efficiently conduct the service composition and recovery policy among mobile devices used for safe experiences of mobile social network services. The paper presented a comprehensive strategy applied to MSNs when natural disasters happen.

The above 13 papers were selected by strict several rounds of peer reviewing based on their originality, relevance, technical clarity and presentation, by at least two anonymous reviewers. Here, I show gratitude to Assoc. Prof. Muthucumaru Maheswaran from School of Computer Science, McGill University, for his collaboration of the successful special issue on the very interesting and challenging security-centric topic of MSNs. Besides, all invited reviewers are appreciated for their reviews, comments and suggestions for authors. Finally, I give special thanks to Editor-in-Chief Prof. Fionn Murtagh and Dr Jutta Mackwell as Editor of *The Computer Journal*, for their great helps and efforts so as to the special issue publication on time and successfully.

FUNDING

The work was sponsored by National Natural Science Foundation of China Grant No. 61370220, Plan For Scientific Innovation Talent of Henan Province Grant No. 134100510006, Program for Henan Province Science and Technology Grant No. 142102210425, Key Program for Basic Research of The Education Department of Henan Province Grant No. 13A520240 and No. 14A520048.

Z. Zhang, born in 1975, at Xinxiang City, Henan, China, and received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, respectively. He was ever postdoctoral fellowship at Xi'an Jiaotong University, China. Nowadays, he is a full-time Distinguished Professor with Department of Computer Science, College of Information Engineering, Henan University of Science and Technology. He is also ACM Senior Member, IEEE Senior Member, IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee.

Prof. Zhang and research interests include MSNs and digital rights management, trusted computing and access control, as well as security risk management and soft computing. He has published over 80 scientific papers on the above research fields, and held 8 authorized patents. Besides, he is Editorial Board of Neural Network World, Associate Editor of Social Network Analysis and Mining and Guest Editor of *The Computer Journal*, EURASIP Journal on Information Security, Journal of Multimedia. And also, he is Chair/Co-Chair and TPC Member for numerous international workshops/sessions on Digital Rights Management and content security.

PS: LIST OF SPECIAL ISSUE ACCEPTED PAPERS

Section 1: MSN Security, Privacy and Forensics

COMPJ-2013-09-0592: Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures

COMPJ-2013-09-0570: Information Diffusion Model Based on Privacy Setting in Online Social Networking Services

COMPJ-2013-09-0587: Privacy Preserving Data Publication with Features of Independent ℓ-Diversity

COMPJ-2013-09-0541: Approach to Detecting Type Flaw Attacks Based on Extended Strand Spaces

COMPJ-2013-09-0539: Exposing Photographic Splicing by Detecting the Inconsistencies in Shadows

Section 2: MSN Trust and Reputation

COMPJ-2013-09-0590: Taxonomy for Trust Models in Cloud Computing

COMPJ-2013-09-0588: A Strong and Weak Ties Feedback-Based Trust Model in Multimedia Social Networks

COMPJ-2013-09-0581: Sensational Headline Identification by Normalized Cross Entropy Based Metric

COMPJ-2013-09-0593: CRM: A New Dynamic Cross-Layer Reputation Computation Model in Wireless Networks

COMPJ-2013-09-0578: A Formal Analytic Approach to Credible Potential Path and Mining Algorithms for Multimedia Social Networks

Section 3: MSN Architecture, Networking and Disaster

COMPJ-2013-09-0589: Multilevel Analysis to Detect Covert Social Botnet in Multimedia Social Networks

COMPJ-2013-09-0577: A trust routing for Multimedia Social Networks

COMPJ-2013-09-0576: A Composition and Recovery Strategy for Mobile Social Network Service in Disaster