Editorial

Fatos Xhafa*

Department of Languages and Informatics Systems,
Technical University of Catalonia,
Campus Nord, Ed. Omega,
C/Jordi Girona 1-3, 08034 Barcelona, Spain
Email: fatos@lsi.upc.edu
*Corresponding author

Xiaofeng Chen

The State Key Laboratory of Integrated Service Networks (ISN),
School of Telecommunications,
Xidian University,
Taibai South Road 2,
Xi'an City, Shaanxi Province,
710071 Xi'an, China
Email: xfchen@xidian.edu.cn

Biographical notes: Fatos Xhafa received his PhD in Computer Science from the Technical University of Catalonia (UPC), Barcelona, Spain. He was a Visiting Professor at the University of London, UK (2009/2010) and a Research Associate at Drexel University, Philadelphia, USA (2004/2005). He has widely published in peer reviewed international journals, conferences/workshops, book chapters and edited books and proceedings in the field. He is the Editor-in-Chief of the *International Journal of Space-based and Situated Computing*, and of *International Journal of Grid and Utility Computing, Inderscience*. He is actively participating in the organisation of several international conferences. His research interests include parallel and distributed algorithms, combinatorial optimisation, networking, cloud, grid and P2P computing.

Xiaofeng Chen received his BS and MS in Mathematics from Northwest University, China. He received his PhD in Cryptography from Xidian University at 2003. Currently, he works at Xidian University as a Professor. His research interests include applied cryptography and cloud computing security. He has published over 80 research papers in refereed international conferences and journals. His work has been cited more than 1,000 times at Google Scholar. He has served as the Programme/General Chair or programme committee member in over 20 international conferences.

With the fast development of the internet, companies, communities and organisations of practice strongly leverage intelligent networking and collaborative systems by a great variety of formal and informal electronic relations, such as business-to-business, peer-to-peer and many types of online collaborative learning interactions. This has resulted in entangled systems that need to be managed efficiently and in an autonomous way. In addition, latest and powerful technologies based on grid and wireless

Copyright © 2015 Inderscience Enterprises Ltd.

infrastructure as well as cloud computing are currently enhancing collaborative and networking applications a great deal but also facing new issues and challenges. For example, well-known social networks lack of knowledge management and adaptive solutions and the information shared among peers is rather static. Virtual communities of practice also provide poorly interactive solutions and lack of full support for organisation, management, mobility and security.

This special issue on 'Security, management and model for intelligent networking and collaborative systems' attempts to highlight some of the latest research addressing those challenges. It consists of ten papers carefully selected from the contributions of the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS 2013) and 4th International Conference on Emerging Intelligent Data and Web Technologies (EIDWT 2013). More specifically:

- The paper of Wu, Li and Zhang, titled 'Key management scheme based on secret sharing for wireless sensor networks', proposed a key management based on secret sharing scheme to protect the security of the key distribution and management in wireless sensor networks, which is the key challenge for its wide applications.
- The paper of Ren, Tang, Wang and Wong, titled 'Attribute-based signature schemes with accountability', presented a novel notion of accountable attribute-based signature scheme. They also presented two efficient accountable attribute-based signature schemes with formal security proof.
- The paper of Patel, Schubert-Kabban, Baldwin and Montminy, titled 'Statistical analysis and comparison of linear regression attacks on the advanced encryption standard', investigated profiled linear regression-based attacks for extracting the advanced encryption standard secret key. Attack performance showed an order of magnitude improvement when the dimensionality of the distribution estimated in the training phase was increased from 1 to 20, giving greater than 98% success rate with as few as 100 training and test traces.
- The paper of Lin, titled 'On two circuit configurations of non-linear feedback shift registers', proposed the transformation from Galois NLFSRs to their equivalent Fibonacci configuration. By this transformation, the relationship between these two circuit configurations of NLFSRs is derived.
- The paper of Zhang, Zhang and Du, titled 'A real-time data backup model and methods based on peer-to-peer network', presented a real-time disaster recovery backup model based on P2P streaming. This new method can avoid the conflict between fixed bandwidth and dynamic changes of backup data size and the single point failure of leased line.
- The paper of Das, Talukdar and Dutta, titled 'Hidden Markov model-based Assamese vowel phoneme recognition using cepstral features', presented an experiment on how to use linear prediction cepstrum coefficients-based (LPCC) features (namely the weighted LPCC and delta weighted LPCC) to recognise Assamese vowel phonemes employing a discrete hidden Markov model (HMM). The overall recognition rate of their experiment is nearly about 81.5%.

- The paper of Luo and Wang, titled 'New signature schemes in the standard model based on publicly verifiable CCA-secure public key encryption', proposed a new way to construct signature schemes in the standard model. Concretely, this is a new way on how to transform CCA secure publicly verifiable public key encryption schemes into signature schemes.
- The paper of Wang, Liu, Sun and Zhang, titled 'Multi-party concurrent signatures scheme from lattice', proposed a new formal model of multi-party concurrent signatures scheme and a lattice-based multi-party concurrent signatures scheme. The scheme is constructed based on constant-size ring signatures, and thus solved the open problem: how to construct a multi-party concurrent signatures scheme based on constant-size ring signatures, which was introduced by Dongvu Tonien, Willy Susilo and Reihaneh Safavi-Naini in 2006.
- The paper of Deng, Wang and Chang, titled 'Sociality-based comprehensive buffer management for multicast in DTNs', proposed a sociality-based comprehensive buffer management for multicast routing (SCBMR). The nodes with high social centrality are selected in priority as relay nodes. They also design a corresponding buffer management strategy that drops the buffered messages with more replicas and shorter TTL in the network.
- The paper of Wu, Xu and Deng, titled 'Server-aided aggregate verification signature: security definition and construction', introduced a new security model for server-aided aggregate verification signature scheme against collusion attacks. They also proposed a concrete server-aided aggregate verification signature scheme-based BGLS signature scheme, which is secure in their model.

Acknowledgements

The guest editors would like to thank Prof. Srikanta Patnaik (Editor-in-Chief of *IJICT*) for the opportunity to edit this special issue. We would like to thank Ms. Barbara Curran, Inderscience Journal Manager for her attention and support during the special issue editing process. Finally, we appreciate all authors, reviewers and editorial members for their invaluable contribution.