Editorial

Ilsun You*

School of Information Science,
Korean Bible University,
16 Danghyun 2-gil, Nowon-gu, Seoul, 139-791, South Korea
Email: ilsunu@gmail.com
*Corresponding author

Jinshu Su

School of Computer Science,
National University of Defense Technology,
Deya Road #109, Changsha, Hunan, China
Email: sjs@nudt.edu.cn

Qin Xin

Faculty of Science and Technology,
University of the Faroe Islands,
Noatun 3, FO 100 Torshavn, Faroe Islands, Denmark
Email: qinx@setur.fo

Baokang Zhao

School of Computer Science,
National University of Defense Technology,
Deya Road #109, Changsha, Hunan, China
Email: bkzhao@nudt.edu.cn
Email: zhaobaokang@gmail.com

Biographical notes: Ilsun You received his MS and PhD in Computer Science from Dankook University, Seoul, Korea in 1997 and 2002, respectively. Also, he received his second PhD from Kyushu University, Japan in 2012. In 2005, he joined Korean Bible University, South Korea as a Full Time Lecturer, and he is currently working as an Associate Professor. He has served or is currently serving as main organiser of international conferences and workshops such as IMIS, MobiWorld, AsiaARES and so forth. He is currently the Editor-in-Chief of *Journal of Wireless Mobile Networks*, *Ubiquitous Computing, and Dependable Applications* (*JoWUA*), and belongs to the editorial board for *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC*), *Journal of Network and Computer Applications* (*JNCA*), and so forth. His main research interests include internet security, authentication, access control, and formal security analysis. He is an IET Fellow and an IEEE senior member.

Jinshu Su received his BSc in Mathematics from Nankai University, Tianjin, China in 1983, MS in Computer Science from National University of Defense Technology, Changsha, China in 1989, and PhD in Computer Science from National University of Defense Technology, Changsha, China in 1999. He is a Full Professor at the School of Computer Science, National University of Defense Technology, and serves as the Head of the Institute of Network and Information Security, NUDT. He is the Academic Leader of the State Innovative Research Team in University ('Network Technology' Innovative Team) awarded by the Ministry of Education, China. He has lead several national key projects of China, including national 973 projects, 863 projects and NSFC key projects. His research interests include high performance routers, internet routing, high performance computing, wireless networks and information security. He is a member of the ACM and IEEE.

Qin Xin graduated with his PhD (2002–2004) in the Department of Computer Science at the University of Liverpool, UK in 2004. Currently, he is working in the Department of Science and Technology at the University of the Faroe Islands (UoFI), Faroe Islands as a Full Professor of ICT. Prior to joining UoFI, he held various research positions in world leading universities and research laboratory including Senior Research Fellowship at the Universite Catholique de Louvain, Belgium, Research Scientist/Postdoctoral Research Fellowship at Simula Research Laboratory, Norway and Postdoctoral Research Fellowship at the University of Bergen, Norway.

His main research focuses are on design and analysis of sequential, parallel and distributed algorithms for various communication and optimisation problems in wireless networks and information management systems. Moreover, he also investigates the combinatorial optimisation problems with applications in bioinformatics, data mining and space research.

Baokang Zhao is an Assistant Professor with the School of Computer Science, National University of Defense Technology. He received his BS and PhD from the National University of Defense Technology, both in Computer Science. He served as a programme committee member for several international conferences and a reviewer for several international journals (including *TC*, *TCAD*, etc.). He serves on the editorial board of *Journal of Internet Services and Information Security* (*JISIS*). His current research interests include protocols, algorithms, and security issues in computer networks and quantum communication. He is a committee member of CCF internet committee.

The recent proliferation and adoption of information technology are having a huge impact on many areas of society. Privacy security and trust is about understanding how information technology impacts the privacy of individuals and developing new privacy-preserving and secure technologies to protect their privacy. This special issue comprises of 11 extended version of selected papers presented at the 7th International Conference on Frontier of Computer Science and Technology (FCST 2012 was held at the University of Soochow in Suzhou, China, November 21–23, 2012), and provides the reader with the current status, trends and the latest results in this area.

The first article 'A data flow-oriented specification method for analysing network security configurations' by Hicham El-Khoury, Romain Laborde, François Barrère, Abdelmalek Benzekri and Maroun Chamoun extends their previous work with a generic model of equipment configuration built based on their attribute-based approach. Network security services are represented by specific atomic abstract functions called 'basic commands' that can modify the data flow. Based on this representation, they define an abstract model of configuration.

The second article 'Intrusion detection method based on nonlinear correlation measure' by Mohammed A. Ambusaidi, Zhiyuan Tan, Xiangjian He, Priyadarsi Nanda, Liang Fu Lu and Aruna Jamdagni proposed an effective nonlinear correlation coefficient-based (NCC) measure which can accurately extract both linear and nonlinear correlations between network traffic records for intrusion detection.

In the third article 'An efficient quantum anonymous communication with hybrid entanglement swapping', Xiaoping Lou, Jun Dai, Zhigang Chen and Moon Ho Lee proposed an efficient information-theoretically secure protocol which is built for the anonymous transmission of quantum information.

The fourth article 'Efficient constructions of certificate-based key encapsulation mechanism' by Yang Lu and Jiguo Li extended the concept of key encapsulation mechanism to the primitive of certificate-based encryption and proposed two provably secure certificate-based key encapsulation mechanism schemes.

The fifth article 'Efficient identity-based threshold signature scheme from bilinear pairings in standard model' by Fei Li, Wei Gao, Guilin Wang, Kefei Chen and Xueli Wang proposed a new identity-based threshold signature (IBTHS) scheme from bilinear pairings resulting in several benefits in terms of efficiency, security and functionality.

In the sixth article 'High-efficient quantum secret sharing with arrangements of lines on two-dimensional planes', Li Zhang, Ying Guo and Dazu Huang investigate a simple (2, 2)-threshold scheme and its generalised (n, n)-threshold scheme for the quantum secret sharing (QSS) based on fundamental laws of analytic geometry.

In the seventh article 'LIFE: a lightweight and flexible key management scheme for securely and pervasively file editing in mobile cloud computing', Wei Ren, Jiahua Lin, Qiang Cao and Liangli Ma proposed a lightweight and flexible scheme – LIFE – to address the key management problem without relying on any trusted third party or trusted computing module.

In the eighth article 'Modelling, analysis and containment of passive worms in P2P networks', Wei Yang, Yong-peng Gao, Zhi-liang Zhu, Gui-ran Chang and Yu Yao address the major threats caused by passive worms by modelling and analysing passive worm propagation. The analysis is useful in understanding how particular factors can affect worm propagation and the authors design effective containment strategies within P2P networks to suppress the worm propagation.

In the ninth article 'Quantum states sharing in the relay system with teleportation of non-maximally entanglement', Jinjing Shi, Ronghua Shi, Yin Li, Ye Kang and Xiaoqi Peng proposed a novel scheme for multi quantum states sharing. The scheme is based on the relay system with teleportation in the non-maximally-entangled channel in order to improve the efficiency of secure distribution of quantum states for communications.

The tenth article ‘The algorithm model for cumulative vulnerability risk assessment’ by Yong Yan Chen and Hong Chun Shu develops a new method to count cumulative multi-risk which uses vulnerabilities in attack graph and reverse iteration tracing algorithm based on rough sets.

We would like to thank for Sherali Zeadally and Liz Harris for guiding us through the editorial process for during the preparation of this special issue, and Sherali Zeadally, Han-Chieh Chao and Jiann-Liang Chen for providing us this special issue opportunity. We are also indebted to all the reviewers who provided valuable comments to the authors to help them strengthen and improve their papers.